DERECHO Y TECNOLOGÍAS

María Emilia Casas Baamonde
(Directora)
Daniel Pérez del Prado
(Coordinador)

HAND books

FUNDACIÓN RAMÓN ARECES

DERECHO Y TECNOLOGÍAS

María Emilia Casas Baamonde
(Directora)
Daniel Pérez del Prado
(Coordinador)

DERECHO Y TECNOLOGÍAS

FUNDACIÓN
RAMÓN ARECES

Reservados todos los derechos.

Ni la totalidad ni parte de los libros pueden reproducirse o transmitirse por ningún procedimiento electrónico o mecánico, incluyendo fotocopia, grabación magnética o cualquier almacenamiento de información y sistema de recuperación, sin permiso escrito de Editorial Centro de Estudios Ramón Areces, S.A.

El contenido expuesto en este libro es responsabilidad exclusiva de sus autores.

© EDITORIAL CENTRO DE ESTUDIOS RAMÓN ARECES, S.A.
Tomás Bretón, 21 – 28045 Madrid
Teléfono: 915 398 659
cerasa@cerasa.es
www.cerasa.es

© FUNDACIÓN RAMÓN ARECES
Vitruvio, 5 – 28006 MADRID
www.fundacionareces.es

ISBN-13: 978-84-9961-466-3
Depósito legal: M-643-2025

Impreso por:
Campillo Nevado, S.A.
Desierto de Tabernas, 8
28320 Pinto (Madrid)

Impreso en España / Printed in Spain

ÍNDICE

PRÓLOGO 17

Introducción. TECNOLOGÍAS, CIENCIA, ECONOMÍA Y DERECHO (María Emilia Casas Baamonde) 19

1. Los avances imparables de la tecnociencia 19
2. La digitalización como imperativo económico y político (de política económica) de la Unión Europea y de sus Estados 25
3. Las tecnologías digitales y el Derecho; la reforma de la Constitución, la democracia y el Estado de Derecho 31
   - 3.1. La innovación jurídica con causa tecnológica, derechos fundamentales, reformas legislativas e interpretativas. ¿Reformas de las Constituciones? Sobre la reforma de la Constitución española.... 32
   - 3.2. Los sistemas de fuentes de producción normativa; la principalidad de la ley (su dignidad democrática) 36
   - 3.3. Reformas legislativas tecnológicas y técnica normativa 37
   - 3.4. El Derecho de la sociedad digital; y sobre el Estado de Derecho legislado y judicial en la democracia constitucional..... 38

Primera Parte
ESTUDIO INTRODUCTORIO

Capítulo 1. JUEZ CON ROBOT, MÁS QUE ROBOT JUEZ (Andrés Ortega Klein) 45

1. Introducción 45
2. Inducción, deducción, abducción 48
3. ¿Justicia algorítmica? 52
4. Transparencia y explicabilidad 60
5. Neurociencia, libre albedrío y responsabilidad 64
6. Conclusiones: eficiencia y rapidez. ¿Hacia un transjuez? 70

Bibliografía 73

Segunda Parte
ESTUDIOS SOBRE ROBÓTICA E INTELIGENCIA ARTIFICIAL

Capítulo 2. DERECHOS FUNDAMENTALES EN LA SOCIEDAD DIGITAL Y DE LA INTELIGENCIA ARTIFICIAL (Tomás de la Quadra-Salcedo Fernández del Castillo) 79
1. Introducción 79
2. Dislocación de espacios de relación y trastrocamiento de reglas de conducta 82
3. La permanencia de informaciones ciertas sobre las personas: el derecho al olvido como primer ejemplo de reconstrucción de límites y reglas en espacios digitales 83
4. Alteración asimétrica de la posición de oferentes y demandantes en mercados en línea: discriminación algorítmica de precios y precios dinámicos. El síndrome Robin Hood en mercados a distancia 88
4.1. Derecho a la igualdad 93
4.2. Derecho a la protección de datos (art. 18.4 CE) y Derecho a la información (art. 20 CE) 95
4.3. La garantía de los derechos de consumidores y usuarios (art. 51 CE). 99
4.4. La libertad de empresa en el marco de una economía de mercado (art. 38 CE) y los precios algorítmicamente diferenciados 100
4.5. La libertad (art. 17.1 CE) en relación con las prácticas prohibidas de la inteligencia artificial 100
5. La herencia digital de las personas: bienes y derechos de la personalidad y el derecho a la intimidad y a la protección de datos del causante 102
6. Neuro-tecnologías y derechos y libertades fundamentales 107
7. Conclusiones 113
Bibliografía 118

Capítulo 3. CÓMO ABORDAR JURÍDICAMENTE EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LOS DERECHOS FUNDAMENTALES (Lorenzo Cotino Hueso) 123
1. Constitucionalmente hay que garantizar, guiar y contener la innovación en inteligencia artificial 123
2. Premisas jurídicas y dogmáticas: la dimensión objetiva de los derechos y la dignidad para la garantía de la IA y los derechos fundamentales..... 127

3. Claves, desafíos y deficiencias de la protección de datos como régimen general aplicable a la IA 131
4. La aceleración de la regulación y el Convenio europeo de IA 135
5. Más allá de la retórica: la relevancia de los principios jurídicos en la IA 139
6. ¿Nuevos derechos en la era de la IA? Carta de Derechos digitales, Convenio IA y el RIA 142
7. El impacto colectivo o supraindividual de la IA requiere nuevos modelos de garantía y participación 147
8. La independencia de las (nuevas) autoridades de IA y la AESIA en España 150
9. Gestión de riesgos y la doble proyección para la IA del modelo preventivo de la protección de datos 154
10. El modelo preventivo de protección de derechos del Reglamento IA para los sistemas de alto riesgo y en el Convenio de Europa 156
11. Análisis de riesgos y estudios de impacto de derechos fundamentales para sistemas IA de alto riesgo 160
12. La calidad de la ley como garantía ante el impacto de la IA en los derechos fundamentales 161
13. Conclusiones 164
Bibliografía 165

Capítulo 4. DERECHO PENAL Y DESAFÍOS DE LA INTELIGENCIA ARTIFICIAL (EN EL CONTEXTO DEL NUEVO MARCO REGULATORIO EUROPEO) (Fernando Miró Llinares) 177
1. Presente y futuro del Derecho penal ante las promesas y amenazas de la IA 177
   1.1. Tres desafíos para el Derecho penal derivados de la IA 177
   1.2. A vueltas con la definición de IA (y sus implicaciones para el alcance del impacto en el sistema penal) 182
2. Delito, responsabilidad penal e IA 185
   2.1. Daños y peligros causados por/mediante el uso de sistemas de IA 185
   2.2. Responsabilidad penal e inteligencia artificial 188
Bibliografía 212

Capítulo 5. LA GENERACIÓN DE CONTENIDOS A TRAVÉS DE INTELIGENCIA ARTIFICIAL Y SU INCIDENCIA EN LA PROPIEDAD INTELECTUAL (Sebastián López Maza) 217
1. Introducción 217
2. Cuestiones no controvertidas en el uso de IA 219
3. Cuestiones controvertidas en el uso de IA generativa 223
3.1. La titularidad de derechos sobre los resultados producidos por IA generativa 224
3.2. La originalidad de los resultados producidos por IA generativa 236
3.3. El entrenamiento de los sistemas de IA a partir de obras y prestaciones protegidas 240
4. Conclusiones 251
Bibliografía 252

Capítulo 6. DERECHO DE DAÑOS, ROBÓTICA E INTELIGENCIA ARTIFICIAL (María José Santos Morón) 257
1. Introducción 257
2. ¿Responsabilidad por productos defectuosos o responsabilidad por culpa? 261
3. La Propuesta de Directiva sobre responsabilidad por productos defectuosos [28 de septiembre de 2022, COM (2022) 495] 268
4. La aplicación de las reglas de responsabilidad por culpa 282
4.1. La presunción de nexo causal de la Propuesta de Directiva sobre responsabilidad IA y su limitada operatividad 287
5. Conclusiones 291
Bibliografía 292

Tercera Parte
ESTUDIOS SOBRE ALGORITMOS Y BIG DATA

Capítulo 7. EL USO DE ALGORITMOS POR LAS ADMINISTRACIONES PÚBLICAS (Alejandro Huergo Lora) 297
1. Introducción 297
2. De qué hablamos cuando hablamos de algoritmos 297

2.1. Los "algoritmos" y su limitada utilidad como concepto jurídico .. 297
2.2. Apoyos informáticos para aplicar normas 300
2.3. Instrumentos para tomar decisiones 302
2.4. Actividad administrativa automatizada 304
3. Posibles usos de la inteligencia artificial en la actividad administrativa 308
3.1. Concreción de conceptos legales de tipo probabilístico o predictivos 308
3.2. Decisiones aproximativas o preparatorias 310
3.3. ¿Resoluciones o normas elaboradas mediante inteligencia artificial?.. 312
3.4. Inteligencia artificial generativa 314
4. La regulación del uso de la inteligencia artificial 321
4.1. Aplicación del marco jurídico regulador de la actividad en la que se utiliza la inteligencia artificial 321
4.2. El marco jurídico específico de la inteligencia artificial: justificación.. 323
4.3. El Reglamento de Inteligencia Artificial 324
4.4. Aplicación del Reglamento a las Administraciones Públicas..... 326
5. Conclusiones 327
Bibliografía 329

Capítulo 8. ALGORTIMOS E INTELIGENCIA ARTIFICIAL EN EL DERECHO DIGITAL DEL TRABAJO (Jesús R. Mercader Uguina).. 335
1. La arquitectura del Derecho digital del trabajo 335
2. La empresa y el empleador algorítmico: La era de la empresa post-material 337
3. La gran delegación empresarial: la gestión algorítmica del empleo 339
3.1. Procesos de selección de trabajadores sospechosos 339
3.2. Los algoritmos dirigen la empresa 343
3.3. El control algorítmico del trabajo en la era del capitalismo de la vigilancia 347
3.4. La neurotecnología llega al lugar de trabajo 351
4. Inteligencia artificial y seguridad y salud en el trabajo 354
5. ¿Pueden despedir los algoritmos? 357
6. Hacia una Administración social algorítmica 358
7. Regulando los algoritmos: dimensiones laborales del Reglamento de Inteligencia Artificial 364

8. El impacto en el mercado de trabajo: ¿hacia una cuota de reserva para el trabajo humano? 369
Bibliografía 370

Capítulo 9. BIG DATA Y ALGORITMOS: SU IMPACTO EN EL DERECHO DE LA PROPIEDAD INTELECTUAL, INDUSTRIAL Y COMPETENCIA (Jaume Martí Miravalls) 375
1. Introducción 375
2. Cuestiones conceptuales y terminológicas 377
3. El Big data y los algoritmos como objeto de protección en el Derecho de la propiedad intelectual e industrial 382
4. El Big data y los algoritmos ante el Derecho de la competencia 394
5. Conclusiones 408
Bibliografía 409

Capítulo 10. DISCRIMINACIÓN ALGORÍTMICA (Ana Garriga Domínguez) 411
1. Introducción 411
2. Sistemas de inteligencia artificial y sesgos 414
3. El principio de igualdad ante la discriminación algorítmica 422
4. La protección de los datos personales y la discriminación algorítmica 429
5. La discriminación algorítmica en el reglamento de inteligencia artificial 439
6. Conclusiones 443
Bibliografía 447

Cuarta Parte
ESTUDIOS SOBRE BLOCKCHAIN

Capítulo 11. ESTRUCTURAS DE GOBIERNO EN BLOCKCHAIN (Ana Felicitas Muñoz Pérez) 455
1. Introducción 455
2. La DAO en la estructura de gobierno de la DLT/Blockchain 457
2.1. La arquitectura 457

2.2. El gobierno 459
2.3. Los elementos 462
3. El gobierno de la DAO 464
3.1. La evolución de "The Dao" al "BORG" 464
3.2. Noción y figuras afines 468
3.3. Daos no reguladas 471
3.4. Iniciativas de regulación 484
4. Conclusiones 491
Bibliografía 493

Capítulo 12. LAS APLICACIONES DE LA TECNOLOGÍA DE REGISTROS DISTRIBUIDOS EN LAS SOCIEDADES DE CAPITAL (Reyes Palá Laguna) 501
1. Introducción 501
2. Las aplicaciones de la TRD en el funcionamiento de las sociedades de capital 506
2.1. Consideraciones generales 506
2.2. Los registros societarios en TRD 508
2.3. El ejercicio de los derechos del socio a través de sistemas basados en la TRD en las juntas generales de las grandes sociedades 510
3. La TRD *ad extra*: la financiación de la sociedad 523
3.1. La posibilidad de instrumentar los valores negociables en toquens. 523
3.2. La toquenización de acciones y obligaciones al margen del derecho del mercado de valores 527
3.3. Los toquens como nueva forma de representación de los derechos-valor emitidos por la sociedad 531
3.4. La financiación a través de préstamos toquenizados 533
4. Conclusiones 534
Bibliografía 535

Quinta Parte
ESTUDIOS SOBRE EL METAVERSO

Capítulo 13. METAVERSO, BLOCKCHAIN Y EL REGISTRO DE LA PROPIEDAD (Rocío Perteguer Prieto) 543

1. Introducción 543
2. Metaverso 545
2.1. Concepto y descripción 545
2.2. Elementos necesarios para su creación y ejemplos 546
3. Blockchain 551
3.1. Concepto de blockchain, activos digitales, NFTs y smart contracts 551
3.2. Especial consideración de la nueva regulación por la LNMV 560
4. Contribución de los registros jurídicos 564
4.1. Garantías necesarias del Registro de la Propiedad 564
4.2. Papel del Registro de Bienes Muebles 569
4.3. Desde el Registro Mercantil 571
4.4. Registro de Condiciones Generales de la Contratación 573
Bibliografía 576

Capítulo 14. METAVERSO LABORAL: RIESGOS REALES EN MUNDOS VIRTUALES (Magdalena Nogueira Guastavino) 579
1. Auge y caída del metaverso 579
2. Riesgos transversales con repercusión laboral 581
2.1. La gobernanza 581
2.2. La identidad digital 589
2.3. La protección de datos 592
3. El meta-derecho individual del trabajo 595
3.1. Ley aplicable, mercado de trabajo y selección de personal 595
3.2. Formación con y para el metaverso y riesgos laborales 601
3.3. Salario, tiempo y lugar de trabajo 603
3.4. Otras cuestiones laborales 609
4. Metaverso y derecho colectivo del trabajo 610
5. Poderes del Estado, instituciones laborales públicas y metaverso 612
6. Conclusiones 614
Bibliografía 618

Sexta Parte
ESTUDIOS SOBRE PLATAFORMAS

Capítulo 15. THE INDIVIDUAL EMPLOYMENT RELATIONSHIP THROUGH DIGITAL PLATFORMS (Adalberto Perulli) 625

1. Introduction. Work and technology within platform economy 625
2. Labour law's regulative challenges..... 629
3. The issue related to the qualification of the employment relationship 633
4. The qualification of work relationships within platforms in the single labour law systems 635
5. The qualification of the work relationship of platform workers and the comparative method 638
6. The power of direction and the freedom of choosing whether and when to work..... 644
7. The EU Directive on platform work 647
8. A critique of the legal presumption of the EU Directive on platform work. 652
9. The ban to penalise the rider through reputational algorithmic ranking 657
10. Algorithmic discrimination..... 660
Bibliography..... 664

Capítulo 16. PLATAFORMAS, ALGORITMOS Y PODER EMPRESARIAL (Daniel Pérez del Prado) 669
1. Información, datos y tecnología como fuentes del poder empresarial . 669
2. Algoritmos y poder empresarial 672
3. Plataformas y poder empresarial..... 685
4. Límites y contrapoderes al poder empresarial: el caso de las plataformas 687
4.1. Herramientas basadas en el establecimiento de limitaciones..... 687
4.2. Herramientas basadas en la introducción de transparencia 697
5. Conclusiones 707
Bibliografía..... 709

Séptima Parte
ESTUDIO FINAL

Capítulo 17. NEUROTECNOLOGÍA Y NEURODERECHOS (Rafael Yuste)..... 719
1. Introducción..... 719
2. La revolución neurotecnológica..... 719

3. Los neuroderechos 721
4. Necesidad de neuroderechos 722
5. Pasos hacia la implementación mundial de neuroderechos 723
6. Conclusiones 724
Bibliografía 725

PRÓLOGO

El impacto de la digitalización sobre la vida humana es general y transversal. General porque todos y cada uno de los ámbitos de nuestro día a día se ven afectados, desde los más livianos a los que tienen una mayor transcendencia. También tiene una afectación transversal porque, lógicamente, afecta a todas las ramas del saber, desde la Ingeniería a la Filosofía, pasando, como no puede ser de otro modo, por el Derecho. La revolución tecnológica actual ha cambiado de un modo radical la globalización, la economía, la política y las sociedades.

A pesar de lo mucho que se ha escrito sobre el cambio disruptivo imparable que la digitalización y la inteligencia artificial implican, pues viene ocupando intensamente a la doctrina jurídica especializada desde las distintas opciones de especialización, la presente obra cubre un espacio prácticamente inexplorado por el análisis científico, pues aborda la relación entre la digitalización y el Derecho con una perspectiva multidisciplinar, es decir, desde todas las ramas del Derecho. Su principal aportación consiste precisamente en aunar bajo un mismo volumen estudios especializados de alta calidad acerca de la relación de las tecnologías digitales con el Derecho, de la mano de los especialistas más destacados y desde las ricas y plurales perspectivas que integran el saber jurídico, inmerso en las comunidades jurídicas de la Unión Europea, del Consejo de Europa y de Naciones Unidas. Las innovaciones estudiadas están en pleno desarrollo, en algún caso aún incipiente, pero son irreversibles y en todo caso cuentan con suficiente experiencia como para comprobar la funcionalidad, o su falta, de las soluciones jurídicas ya establecidas o propuestas.

Expreso mi agradecimiento a la Fundación Ramón Areces por el impulso y las facilidades dadas para llevar a cabo un proyecto pionero, convertido en esta magnífica realidad que el lector tiene en sus manos. Comprometida con la investigación de excelencia y la transmisión del conocimiento, el rigor y la pluralidad, esta obra es una muestra acabada del compromiso de la Fundación.

Merecen el mayor reconocimiento por la asunción generosa y entusiasta del proyecto y por su preciso hacer las autoras y autores de este libro, especialistas sobresalientes en cada una de sus disciplinas de especialización, cuyas contribuciones son piezas imprescindibles en el avance de la ciencia jurídica en este

extremadamente complejo ámbito que es el mundo digital. Sin la diligente y eficaz coordinación del profesor Daniel Pérez del Prado este libro colectivo, sencillamente, no hubiera sido posible.

Estoy convencida de que este libro cumplirá con sus objetivos de ofrecer una explicación pormenorizada de la incidencia tecnológica en cada sector de nuestro ordenamiento jurídico y confío en que abrirá perspectivas nuevas para los legisladores y aplicadores de las nuevas realidades jurídicas. Alejado de una pasiva espera del porvenir, este libro se adelanta al análisis jurídico de los cambios ineludibles del sistema jurídico, sin dejar de hacer una doble tarea de proposición y prospección sobre su futuro.

Solo me queda recomendar vivamente su lectura.

María Emilia Casas Baamonde
Directora

Introducción
TECNOLOGÍAS, CIENCIA, ECONOMÍA Y DERECHO

María Emilia Casas Baamonde
Consejo Ciencias Sociales
de la Fundación Ramón Areces
Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad Complutense de Madrid

1. LOS AVANCES IMPARABLES DE LA TECNOCIENCIA

La tecnología es tan antigua como la humanidad y su historia ha estado siempre acompañada de avances tecnológicos. La ciencia ha movido el desarrollo tecnológico, que alcanzó cotas significativas a partir de los siglos XVIII-XIX, aunque las relaciones entre ciencia y tecnología no sean de dirección única y muestren una variada y rica interactuación[1]. Las tecnologías innovadoras de cada momento fueron percibidas por sus protagonistas con el gran valor de cambio que tuvieron y de "ruptura cualitativa" del orden establecido. La introducción de la máquina de vapor condujo a la revolución industrial, inicialmente en Inglaterra y expandida rápidamente al continente europeo, que cambió el mundo de la producción industrial y del trabajo, extendido del día a la noche, y del consumo, incrementó la demanda y las exportaciones de productos manufactureros, promovió desplazamientos masivos de personas del campo a las ciudades, transformó completamente la sociedad, emergiendo nuevas clases sociales, y el comportamiento y la vida humana, generando una nueva civilización, la civilización industrial. En el excelente estudio de M. Alonso Olea, que se inicia con las conocidas *Lectures on the Industrial Revolution* de A. Toynbee[2], se dice que la

---

[1] Sobre la tecnociencia, J.M. Sánchez Ron, "Ciencia, tecnología, economía y poder: de la máquina de vapor al chip", *Ciencia y tecnología: perspectiva desde las Reales Academias*, Instituto de España, Madrid, 2024, p. 97.

[2] Rivington, 1884, publicadas tras su muerte y con las notas de sus alumnos. Con precedentes sobre la industrialización contemporánea en Saint-Simon y Owen. Y con análisis de sus

conmoción causada por la revolución industrial fue solo comparable con la provocada por el descubrimiento del nuevo mundo o, retrocediendo en el tiempo, por la gran revolución del neolítico[3]. Destaca la radical novedad de los factores tecnológicos y, en conjunción con otros, su poder principal de transformar radicalmente "la estructura de la sociedad humana"[4].

La revolución industrial cambió los sistemas de gobierno en Europa. En el Derecho marcó una solución de continuidad en su devenir histórico, poniendo en cuestión la *suma divisio iuris* ulpinianea, entre Derecho privado y público, en que se reprecipitó el sistema jurídico continental desde la formulación de los postulados del Estado de derecho liberal. Multiplicó la aparición de nuevas normas jurídicas, paradigmáticamente de normas "sociales", y dio nacimiento a disciplinas nuevas, jurídicas como el actual Derecho del trabajo y de la previsión social, el Derecho urbanístico o la nueva Criminología, y no jurídicas, como la sociología, "como respuesta intelectual europea" al estudio de la sociedad industrial[5]. Cambió la economía, la filosofía, el arte, sentó las bases de la publicidad.

Los avances científico-tecnológicos en química orgánica y en electromagnetismo y electrodinámica del siglo XIX tuvieron un efecto decisivo en el desarrollo industrial y en la fabricación a gran escala de productos (farmacéuticos, fertilizantes, colorantes), en el desarrollo de la telegrafía y de las comunicaciones. Para Sánchez Ron el impacto de la instalación del primer cable submarino que unió a Europa con Norteamérica en 1866 "fue enorme. Al fin y al cabo, se había conseguido reducir una larga travesía marítima a unos breves instantes, en lo que a las comunicaciones se refiere. *En ninguna otra época de la historia de la humanidad, incluida la presente*, *a pesar de toda la tecnología moderna*, se produjo una ruptura *cualitativa* de orden parecido, aunque no podemos olvidar que inicialmente los cambios no se extendieron a todas las clases sociales"[6]. La introducción de esas redes telegráficas de gran distancia afectó al desarrollo del Derecho

---

efectos en las primeras ediciones de los libros de Beard, Mantoux, Ashton y Flinn, y de otros testimonios de escritores coetáneos.

3 *Introducción al Derecho del trabajo*, 7ª ed., al cuidado del M.E. Casas Baamonde y R. Alonso García, Civitas, Madrid, 2013, pp. 352 y 361.

4 *Op.* cit., pp. 354 y 400 y ss.

5 Alonso Olea, *op*. cit., p. 354.

6 *Op.* cit., p. 101; las cursivas son mías, salvo las correspondientes a la palabra "*cualitativa*", del autor.

internacional, pues precisó del establecimiento de convenios de cooperación internacional. Las transformaciones tecnológicas nunca han podido pasar inadvertidas para el Derecho, cuya historicidad es dimensión óptica esencial para abordar su comprensión.

En el siglo XX las tres revoluciones científicas disruptivas fueron las de la relatividad, la física cuántica y el ADN, siendo la de la física cuántica "la que más ha influido en la industria, economía, y poder político y militar" con hechos como el descubrimiento de la fisión nuclear que permitió la fabricación de bombas atómicas, armamento nuclear, satélites, radares[7]. La invención del transistor en 1947 cambiaría la industria de las comunicaciones. En el ámbito del Derecho tratar de compendiar las reformas más importantes es una tarea imposible dentro de los márgenes de este trabajo. Valga destacar, sin referencia alguna a sus causas, la aparición en el continente europeo de las constituciones normativas y de las jurisdicciones de la Constitución, con la función institucional de control del legislador democrático, y, tras la Segunda Guerra Mundial y la derrota de los regímenes totalitarios, las declaraciones de derechos humanos y fundamentales por las normas supremas de las democracias constitucionales. Esas normas superiores dieron paso a los Estados sociales o Estados de bienestar, de donde arranca el nacimiento del Derecho de la seguridad social.

La historia ha demostrado que rueda con la fuerza de la ciencia y de la tecnología. Y que, sin caer en el "determinismo tecnológico"[8], "la tecnología siempre gana"[9], que no hay nada que pueda detener su fuerza propulsora del progreso, produciendo, como la ciencia, distintas alianzas con la industria, el dinero y los negocios y la política e innovando los procesos productivos; sin esa alianza con la economía, con "los financieros", ni la ciencia ni la tecnología –los conocimientos científicos y tecnológicos no son concebibles aisladamente– tendrían la posibilidad de transformar los sistemas productivos ni las sociedades[10].

---

[7] Sánchez Ron, *op*. cit., p. 102.

[8] Conforme al cual, en su versión más simple, la tecnología determina la historia como causa única; "no por ello deja de ser el fenómeno capital en torno al cual se agrupan todos los demás": Alonso Olea, *op*. cit., pp. 400 y 402.

[9] Sánchez Ron, *op*. cit., p. 98.

[10] F.J. Puerto Sarmiento, "La historia de la ciencia y de la tecnología en España", *Ciencia y tecnología: perspectiva desde las Reales Academias,* cit., pp. 118-119. Vid. la obra de J. Habermas, *Técnica y ciencia como "ideología"*, ed. de Tecnos, Madrid, 2009.

A la revolución del transistor siguió la revolución del microchip (1959-1961), imprescindible para las tecnologías digitales. Las primeras computadoras electrónicas, como ENIAC y UNIVAC en Estados Unidos, aparecieron en los años 40 y 50 del pasado siglo, situándose el surgimiento de la era digital en las décadas de los 60 y 70, con la rápida evolución de la tecnología de la información, los primeros lenguajes de programación de alto nivel y las bases para la creación de ARPANET, precursor de Internet, produciéndose la expansión de internet y la World Wide Web, creada por el británico Tim Berners-Lee, el 12 de mayo de 1989, y el CERN (Organización Europea para la Investigación Nuclear), en los años 90. La creación de internet y de las aplicaciones informáticas (apps) de los teléfonos móviles de segunda generación de los años 90 del pasado siglo, prepararon el cambio disruptivo de la sociedad analógica a la sociedad digital[11].

En lo que llevamos de este nuevo milenio, se ha producido una profunda revolución tecnológica, que ha cambiado los modelos de negocio y de servicios y alumbrado otros nuevos. Como la revolución industrial, no ha surgido súbitamente, "como un rayo caído del cielo"[12], y, como aquella, ha provocado un cataclismo por la profundidad de su capacidad de cambio y por su extensión a toda la economía, desde luego a la industria, a todos los países, a toda la humanidad. El avance de las tecnologías digitales ha transformado profundamente la vida moderna, ofreciendo innumerables beneficios "democráticos" en comunicación, acceso a la información y servicios. Al tiempo, la globalización y la tecnología de la información han producido la concentración del poder digital y económico en plataformas globales, gigantes digitales, cuya capitalización supera el PIB de la mayoría de los países, incluido el nuestro[13], que se alimentan de nuestros datos personales (Alphabet/Google, Amazon, Apple, Meta/Facebook, Microsoft) y "se desenvuelven en instancias de imposible o muy difícil acceso al poder regulador del Estado", capaces, por ello, de "rivalizar con Leviatán y disputarle el poder soberano sobre la vida y la libertad" de las personas[14]. Su uso genera nuevos problemas, jurídicos

---

[11] M. O'Mara, *The Code: Silicon Valley and the Remaking of America*, Penguin Books, 2020.
[12] Alonso Olea, *op*. cit., p. 352.
[13] J.M. González Páramo, "En torno a la regulación de las bigtecht en finanzas", *Anales de la Real Academia de Ciencias Morales y Políticas*, núm. 99, 2022, pp. 247 y ss.
[14] J.L. Requejo Pagés, *La agonía de la democracia*, KRK Ediciones, Oviedo, 2020, p. 46; "La protección de datos, en la encrucijada entre el Derecho de la Unión y la Constitución Española", en M.E. Casas (coord.), *El derecho a la protección de datos personales en la sociedad digital*, Fundación Ramón Areces, Madrid, 2020, pp. 25-26.

sociales, de desigualdad de riqueza e ingresos para los colectivos marginados por el propio proceso de digitalización (brechas digitales, ampliadas por razón de sexo y edad, que son de desigualdad, pobreza y exclusión social)[15].

La automatización inteligente, la robotización y cobotización, el internet de las cosas (IoT), la industria 4.0 camino ya de la comunicación y de la industria 5.0, el *big data*, la blockchain, el metaverso, la biotecnología, la biociencia, la neurociencia o la inteligencia artificial (IA), algunas apenas en sus inicios, son tecnologías muy poderosas, su velocidad de cambio es muy superior, sin precedentes, y su proyección sobre la vida cotidiana de las personas es masiva, por lo que quizás sólo tengan parangón en la historia, en la profundidad del cambio y de sus efectos, con la revolución industrial; siendo incluso su capacidad afectante mayor al colocar a las máquinas en el lugar de las personas compitiendo en inteligencia con la humana, aunque esta haya sido siempre el motor de los cambios, y con un resultado incierto del resultado del combate en sus progresos futuros.

Para el IMF, en su Nota de Discusión sobre "GEN-AI: Artificial Intelligence and the Future of Work", de 14 de enero de 2024[16], la inteligencia artificial, "un amplio espectro de tecnologías diseñadas para permitir a las máquinas percibir, interpretar, actuar y aprender con la intención de emular las capacidades cognitivas humanas", en el que "la IA generativa (GenAI) incluye sistemas como los sofisticados modelos de lenguaje de gran tamaño que pueden crear contenido nuevo, desde texto hasta imágenes, aprendiendo de amplios datos de entrenamiento", está "llamada a cambiar profundamente la economía mundial como una nueva revolución industrial"[17], según algunos analistas[18].

Sin duda, la irrupción de la IA plantea nuevas fronteras a la digitalización y acelera los efectos de la automatización, de la robotización y de la IoT. La dimensión

---

[15] CES, *La digitalización de la economía*, Informe 01/2021, Madrid, 2021, p. 11.

[16] Cazzaniga et al., *Staff Discussion Note* SDN2024/001, International Monetary Fund, Washington, DC; file:// Downloads/SDNEA2024001%20(1).pdf

[17] Pp. 1 y 3. En las predicciones del IMF, la IA afectará al 40% del empleo mundial, porcentaje que desciende al 26% en los países de bajos ingresos y se eleva al 60% en las economías avanzadas por la prevalencia de empleos con tareas cognitivas, con una posible afectación negativa de en torno a la mitad de los empleos afectados, mientras que el resto podría beneficiarse de una mayor productividad por la integración de la IA. Esta distinta incidencia sobre el empleo podría incrementar la brecha digital y la disparidad de ingresos entre países (p. 2).

[18] K. Schwab, *La cuarta revolución industrial*, Debate, Madrid, 2016.

estratégica de la digitalización alcanza los distintos ámbitos de la economía, del trabajo, de la política, del Derecho y de la sociedad industrial[19]. Desde luego, la digitalización no tiene comparación con ninguna otra mutación, salvo, en su caso, con el cambio climático y su evitación del exterminio del planeta, para las generaciones inmersas en estos fenomenales procesos de transición, que, como la industrialización, expulsa y relega a grupos o colectivos sociales, creando desigualdades y convirtiéndoles en "vulnerables". Una transformación de tal calibre de la economía y de la sociedad no podía no proyectarse sobre la política y sobre el Derecho, sobre sus contenidos e instituciones obviamente, pero también sobre los derechos fundamentales, las categorías y dispositivos técnicos de la ciencia jurídica y sobre los procesos de creación, interpretación y aplicación de las normas jurídicas. Mas allá aun, sobre la cultura jurídica de los países.

El cambio climático planetario, al que ha llevado la civilización industrial, exige asimismo un cambio tecnológico, precisando de tecnologías para reducir emisiones (energías renovables, eficiencia energética, reducción/eliminación de residuos) y para adaptarse a sus consecuencias adversas (infraestructuras resilientes, sistemas de alerta temprana); resumidamente, de tecnologías de mitigación llamadas limpias.

Con seguridad, la digitalización, el cambio climático y la innovación tecnológica, en proceso de evolución constante, han tenido en las últimas décadas, tienen y tendrán un impacto exponencial en los ecosistemas jurídicos de los Estados, de las instituciones supranacionales e internacionales. Su efecto de transformación estructural de la economía y de los modelos productivos sostenibles, de las relaciones sociales y del modo de vivir en sociedad, exige el ajuste del sistema político –"que no quiera argumentar contra sí mismo"[20]– y del Derecho y su cambio, que atiende a los problemas reales de la sociedad en que el Derecho encuentra su sitio y su razón de existir. El análisis de nuestro sistema jurídico descubre sin dificultad la presencia de normas, decisiones judiciales y actuaciones administrativas. Es una conclusión ineludible; el cambio es ineluctable.

El Derecho ha comenzado a mostrar su capacidad de adaptación, incluso de innovación, constituyendo ahora su objeto, además de su promoción

---

[19] M. Castells, *La sociedad digital*, Alianza Editorial, Madrid, 2024.
[20] Alonso Olea, *op*. cit., p. 362.

o fomento, la creación y utilización de las nuevas tecnologías y su aplicación, incluida su propia aplicación a la práctica jurídica (judicial, administrativa, a las relaciones contractuales y al comercio entre privados), a la que la digitalización, la IA ofrecen oportunidades innegables[21]. Esta intersección plantea desafíos importantes, éticos y legales.

2. LA DIGITALIZACIÓN COMO IMPERATIVO ECONÓMICO Y POLÍTICO (DE POLÍTICA ECONÓMICA) DE LA UNIÓN EUROPEA Y DE SUS ESTADOS

La "autonomía estratégica" de la Unión Europea, concepto surgido en el ámbito de la defensa y de la seguridad cuando menos en 2013[22], y extendido a la ciencia, la tecnología, el comercio, los datos personales (también industriales y de empresas), las finanzas y las inversiones, es esencial para su autonomía política, para su supervivencia política en el orden global[23]. El concepto se reformuló por la Comisión Europea como Autonomía Estratégica Abierta durante la presidencia española de la Unión en el segundo semestre de 2023. La digitalización, el desarrollo de un mercado único digital, se reafirmó como condición para garantizar la soberanía tecnológica, reforzar la competitividad, facilitar la transición ecológica, crear empleo y mejorar la vida de los ciudadanos; esto es, como elemento clave del desarrollo económico y de la autonomía estratégica de la UE.

Aunque las tecnologías digitales jugaron un importante papel en la crisis del coronavirus (educación digital, crecimiento del comercio electrónico, de las transacciones digitales y de la utilización de plataformas digitales con consecuencias en el crecimiento de la "economía de la entrega", la logística y el transporte de mercancías), la Covid-19 puso de manifiesto las vulnerabilidades de Europa por sus dependencias estratégicas (industrial, tecnológica, energética) de terceros

---

[21] K. D. Ashley, *Artificial Intelligence and Legal Analytics*, Cambridge University Press, 2016; M. Livermore y D. Rockmore, *Law as Data: Computation, Text, and the Future of Legal Analysis*, The Santa Fe Institute Press, 2019.

[22] European Council 19/20 diciembre 2013, *Conclusions*, https://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf, asumido plenamente desde la *Estrategia Global de Política Exterior y de Seguridad* de la UE de 2016, Consejo Europeo 17 octubre 2016, https://data.consilium.europa.eu/doc/document/ST-13202-2016-INIT/es/pdf

[23] J. Borrell, "Por qué es importante la autonomía estratégica europea", Real Instituto Elcano, *Blog, Presencia global*, 23/12/2020.

países, después agravada por la guerra en Ucrania, y la excesiva deslocalización de las industrias estratégicas. En consecuencia, la opción por una reindustrialización digital y verde –la aceleración de la doble transición digital y ecológica– constituyó uno de los objetivos clave de la estrategia europea de una recuperación "sostenible y resiliente", *Next Generation EU*[24]. El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 estableció el *Mecanismo de Recuperación y Resiliencia*, el elemento central de *Next Generation EU*, cuyos ámbitos de actuación, de importancia europea, se estructuraron en seis pilares conocidos: transición ecológica; transformación digital; crecimiento inteligente, sostenible e integrado; cohesión social y territorial; salud y resiliencia económica, social e institucional; y políticas para la próxima generación, la infancia y la juventud, centradas en la educación, la formación y el desarrollo de capacidades. Los planes estatales de recuperación habían de contribuir efectivamente a la consecución de los objetivos de las transiciones digital y energética-climática de la Unión para 2030 y de neutralidad climática para 2050 para obtener la evaluación positiva de las instituciones comunitarias y su financiación[25].

La crisis sanitaria manifestó visiblemente esa dependencia digital de la Unión Europea en la falta de productos imprescindibles, cuyos precios se incrementaron y los plazos de entrega se dilataron por la interrupción de las cadenas mundiales de suministro, lo que produjo el cierre de fábricas y otras incidencias negativas en numerosos sectores, desde luego en el farmacéutico-sanitario, en el energético, en el alimentario y en de la producción automovilística automatizada, en varios países comunitarios, constituyendo la fabricación de chips una opción industrial fundamental dado su creciente valor estratégico para la nube, la internet de las cosas, la conectividad, el espacio, la defensa y los superordenadores.

La Comisión Europea propuso, el 8 de febrero de 2022, una "ley europea de chips" con más de 43.000 millones de euros de inversiones públicas y privadas para reforzar la escasa capacidad de producción de la Unión hasta un 20% en 2030. La "ley" es, en realidad, dentro de un paquete de medidas más amplio, el Reglamento (UE) 2023/1781 del Parlamento Europeo y del Consejo

---

[24] "*Actualizando la Nueva Estrategia Industrial 2020: construyendo un mercado único más fuerte para la recuperación de Europa*" (COM (2021) 350 final).

[25] Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.

de 13 de septiembre de 2023, por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de chips) (texto pertinente a efectos del EEE), en vigor el 21 de septiembre de 2023. Su objetivo es impulsar la soberanía tecnológica, la competitividad y la resiliencia de Europa y contribuir a las transiciones digital y ecológica.

El Plan Industrial del Pacto Verde de la Comisión Europea dio lugar a la aprobación del Reglamento (UE) 2024/1252 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco para garantizar un suministro seguro y sostenible de materias primas fundamentales y por el que se modifican los Reglamentos (UE) núm. 168/2013, (UE) 2018/858, (UE) 2018/1724 y (UE) 2019/1020 y el Reglamento (UE) 2024/1735 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establece un marco de medidas para reforzar el ecosistema europeo de fabricación de tecnologías de cero emisiones netas y se modifica el Reglamento (UE) 2018/1724.

La Unión Europea, que es, ante todo, una comunidad de Derecho, se ha dotado de un marco normativo sólido ante la economía digital y el cambio climático. Tiene en torno a 100 normas centradas en la tecnología y más de 270 reguladores activos en las redes digitales de todos los Estados miembros.

Son sus normas más emblemáticas, en aquel campo y con una finalidad de apoyo a la innovación digital y de respeto de los derechos fundamentales, el Reglamento General de Protección de Datos[26], aplicable a partir de 25 de mayo de 2018, destinado a reforzar los derechos de las personas físicas sobre sus datos y su privacidad en la era digital, aunque sin prescindir de la promoción del despliegue de las tecnologías digitales, ni de la libre circulación de los datos en la economía de datos europea; el Reglamento de Mercados Digitales[27], que regula las condiciones de la competencia equitativa y leal entre las plataformas digitales de la UE o que operen en la UE con independencia de su tamaño y con

---

[26] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (texto pertinente a efectos del EEE).

[27] Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

las grandes empresas tecnológicas (con obligaciones estrictas para los "guardianes de acceso"), vigente desde el 1 de noviembre de 2022 y aplicación completa desde el 25 de junio de 2023; el Reglamento de Servicios Digitales[28], con entrada en vigor el 16 de noviembre de 2022 y aplicación general a partir del 17 de febrero de 2024, estableció nuevas normas para proporcionar seguridad a los usuarios de servicios en línea y de motores de búsqueda y proteger los derechos fundamentales de los ciudadanos de la UE en línea, fijando responsabilidades y obligaciones de rendición de cuentas y de transparencia para los proveedores de servicios de intermediación; y el Reglamento de Inteligencia Artificial[29], vigente desde el 1 de agosto de 2024 y aplicable desde 2 de agosto de 2026, que se presenta por la Unión como la primera norma jurídica del mundo sobre inteligencia artificial, cuyo objeto es garantizar que los sistemas de IA sean seguros, éticos y fiables. La "ley " europea busca de nuevo el equilibrio entre el fomento del uso de los sistemas de IA y el favorecimiento de las inversiones para su aplicación en el mercado único europeo y el establecimiento de obligaciones de transparencia y de supervisión humana, incluso de prohibiciones para los sistemas de IA de "alto riesgo", para su acceso al mercado europeo ante los efectos negativos de esos sistemas para la seguridad y los derechos de las personas, en primer lugar para sus derechos fundamentales. La Declaración Europea sobre los Derechos y Principios Digitales, firmada por sus presidentas y presidente el 15 de diciembre de 2022, se proclamó solemnemente por el Parlamento Europeo, el Consejo y la Comisión el 23 de enero de 2023[30].

En el cierre de la novena e inicio de la décima legislatura del Parlamento Europeo, los informes de Enrico Letta[31], de abril de 2024, a petición de los

---

[28] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (texto pertinente a efectos del EEE).

[29] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) núm. 300/2008, (UE) núm. 167/2013, (UE) núm. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (texto pertinente a efectos del EEE).

[30] 2023/C 23/01, DO C23/1, 23.01.2023.

[31] *Much more than a market. Speed, security, solidarity. Empowering the single Market to deliver a sustainable future and prosperity for all EU Citizens*; https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

Gobiernos belga y español, y de Mario Draghi[32], de septiembre de 2024, por encargo de la Comisión Europea, han insistido en la necesidad de una mayor integración europea y de su mercado, con el cierre del mercado de capitales, y en la importancia de la digitalización –y de la descarbonización– como "la opción más estratégica" de la UE para ganar en competitividad y en autonomía estratégica frente a sus dependencias exteriores, "para garantizar una ventaja competitiva significativa en el escenario mundial, al tiempo que preserva y desarrolla los estándares sociales de los que Europa disfruta con orgullo"[33].

Draghi propone la "reindustrialización" de Europa a través de la digitalización y la innovación; advierte de que "Europa debe reorientar profundamente sus esfuerzos colectivos para cerrar la brecha de innovación con Estados Unidos y China, especialmente en tecnologías avanzadas" limpias, que su posición tecnológica global y la competitividad de su economía se han deteriorado en un contexto geopolítico de incertidumbre y de temor crecientes, y que debe acogerse a la revolución de la IA, que cambiará radicalmente numerosos sectores económicos, para recuperar capacidad en innovación y en productividad[34]. Europa no supo aprovechar la primera revolución de internet y de las tecnologías TIC, software, bases de datos y propiedad intelectual, y tiene dificultades en las nuevas olas digitales: IA y computación cuántica. Pero no puede permitirse quedarse estancada en las "tecnologías e industrias intermedias" del siglo pasado", en "la trampa de la tecnología media". La digitalización es su "desafío existencial". La Unión tiene que cerrar la brecha de innovación, de tecnologías avanzadas y de habilidades, con recualificación constante de las personas. La tecnología es crucial para la inclusión social, siempre que las políticas y el Derecho garanticen oportunidades de educación y de aprendizaje permanente para todas las personas a lo largo de su vida, de forma que los beneficios económicos de la IA se redistribuyan y se combatan las desigualdades. Es necesario un

---

[32] *The future of European competitiveness -A competitiveness strategy for Europe*; https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf ; *In-depth analysis and recommendations*; https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf

[33] Informe Letta, cit., p.12.

[34] Pp. 01, 02 y 10.

extraordinario esfuerzo inversor público-privado para apoyar la digitalización de las empresas, con particular atención a las pymes, aunque el pequeño y mediano tamaño empresarial de las empresas europeas sea una rémora, todo lo cual destaca asimismo Letta[35], y la capacitación de las personas. En su informe Draghi ha cifrado ese esfuerzo en 800 mil millones de euros anuales, también para descarbonización y defensa[36].

La presidenta Von der Leyen anunció que la nueva Comisión Europea aplicaría las conclusiones del informe Draghi. La alianza entre la tecnociencia, la economía y la política se ha producido.

La afectación de Derecho es ineluctable y, matiz sustancial, el Derecho ha de ejercer necesariamente su poder de incidir en la evolución tecnológica de forma que su uso se acomode a las exigencias debidas de respeto de los derechos fundamentales de las personas, de información y transparencia en el uso de algoritmos de modo que las decisiones automatizadas sean controlables, de seguridad, de responsabilidad jurídica y de supervisión humana. El Derecho, en concreto los ordenamientos jurídicos de los Estados miembros de la UE, con las prevenciones técnicas que expondré, han de incorporar soluciones para garantizar la justicia de la transición digital y de la transición energética y climática, y la sostenibilidad climática del desarrollo tecnológico. Al Derecho corresponde "civilizar" la civilización digital y de la IA con el fin de garantizar que el progreso tecnológico se base en la dignidad humana y fortalezca los valores esenciales de las sociedades democráticas.

La digitalización, la tecnología "*movile*", y la IA son, pues, el escenario actual y futuro de la economía, la sociedad y el Derecho, que éste y sus agentes no pueden ignorar, y que lo transforma con una fuerza y una celeridad incontenibles, que el Derecho ha de encauzar.

---

[35] Pp. 39 y ss. y 50 y ss.
[36] Pp. 02, 24, 01, 07, 21, 14.

3. LAS TECNOLOGÍAS DIGITALES Y EL DERECHO; LA REFORMA DE LA CONSTITUCIÓN, LA DEMOCRACIA Y EL ESTADO DE DERECHO

No es equivocada la afirmación de que la creación de disciplinas jurídicas nuevas, además de constituir una "operación simbólica por excelencia", ofrece la ventaja de unir a esos beneficios simbólicos beneficios materiales, al "ofrecer a los juristas que supieran hacer de ello un ideal, un futuro brillante", creando un mercado de trabajo con todo un sistema de puestos jerarquizados (desde la judicatura a los profesores y profesoras, pasando por las Administraciones públicas y la abogacía especializada) y de bienes simbólicos (manuales, monografías, revistas especiales...)[37]. Dejando a un lado sus presuntas motivaciones y la posibilidad misma de su surgimiento, el hecho cierto es que el curso imparable del cambio digital demanda normas jurídicas propias y específicas para esas nuevas realidades sociales, técnicas interpretativas y aplicativas de esas nuevas normas, y un nuevo saber o ciencia jurídica. Las ha producido ya.

Es posible que esa nueva conceptualización o saber jurídico sobre las normas y la jurisprudencia que se ocupan de la utilización y la incidencia de las nuevas tecnologías, ya existente en el ámbito de las disciplinas jurídicas tradicionales, se materialice en la aportación de un *corpus* teórico para el surgimiento de un sistema intelectual racional y lógico, diferenciado o autónomo, un Derecho informático o tecnológico o un Derecho digital o de la digitalización, como ha tomado cuerpo ya en el pasado siglo un Derecho ambiental o medioambiental, especializado en el ámbito del Derecho público, de cuyo contenido actual forman parte las normas sobre las transiciones energética y climática y la sostenibilidad. La Universidad en Internet ofrece un máster en Derecho digital y otro en *Legaltech*.

Pero al constituir el objeto de ese posible Derecho tecnológico cuestiones de afectación común a las distintas disciplinas jurídicas existentes, a todos los sectores del ordenamiento jurídico, el fenómeno seguro es, sin perjuicio de ese alumbramiento futuro, su presencia en todas ellas, que han incorporado, y seguirán haciéndolo, nuevos ingredientes normativos, en todo caso nuevas construcciones interpretativas y teóricas sobre las nuevas realidades tecnológicas, desde la responsabilidad jurídica y la propiedad y su registro en los entornos

---

[37] P. Cam, "Juges rouges et Droit du travail", *Actes de la recherche en sciences sociales*, vol. 19, Le Seuil, París, 1978, p. 10 y nota 23.

de la robotización, la blockchain, o el metaverso, y la utilización de los sistemas de IA hasta los posibles sesgos discriminatorios de las decisiones automatizadas y los algoritmos utilizados en las relaciones privadas, entre administrados y Administraciones y en los litigios que resuelven los jueces y tribunales, pasando por los contratos inteligentes y los delitos informáticos o ciberdelitos. Son ejes temáticos conocidos, pero no únicos, sino acompañados de todo el cortejo de instituciones jurídicas esenciales sobre las que se precipitan las tecnologías, y especialmente la IA, en coherencia con su consustancial naturaleza transversal, de que han de ocuparse los jueces y tribunales y la doctrina científica a partir de las respuestas de las nuevas normas, o en tanto estas no las proporcionen. El estado actual del Derecho dibuja un patrón general de combinación de normas tradicionales que cohabitan con las que se ocupan de las tecnologías digitales y de la IA.

Característica del afán de totalidad de la digitalización, de su empeño de omnipresencia, es su afectación a todo el sistema jurídico y a su estructura, a sus coordenadas espacio-temporales, sin olvidar la también esencial diversidad tecnológica.

A partir de estas observaciones el análisis del Derecho puede emprender distintos caminos, que aquí me limitaré a enunciar.

3.1. La innovación jurídica con causa tecnológica, derechos fundamentales, reformas legislativas e interpretativas. ¿Reformas de las Constituciones? Sobre la reforma de la Constitución española

El primero conduce a identificar los fines y objetivos políticos de las reformas de los marcos regulatorios actualmente vigentes, que en cierta manera ya han quedado descritos. Junto a la articulación de las políticas públicas de fomento y financiación de la digitalización y del despliegue de sistemas de IA, estatales y autonómicas, las reformas normativas han de ocuparse de la tarea particularmente difícil de juridificar el empleo de las tecnologías y de la IA en un territorio vasto para la innovación jurídica, que ha de proyectarse enteramente sobre las principales códigos o normas de las distintas ramas del ordenamiento jurídico. Operación reformadora que ha de hacerse bajo el mandato de la UE de que el proceso transicional sea justo, socialmente justo, eje de la estrategia de crecimiento sostenible de la Comisión Europea. Y aunque ese sea un objetivo político, y no jurídico, como políticos son sus destinatarios, los Estados y los sujetos colectivos llamados a participar en la transición hacia la digitalización, su cumplimiento político se traducirá en la promoción de cambios normativos, sujetos.

Esa justicia transicional se identifica con la inclusión de las personas en el universo digital a través de los sistemas educativos, de formación, de trabajo y empleo, y de protección social. Una competencia digital básica será inexcusable en todo tipo de trabajo. Es fácil establecer la ecuación entre cualificación idónea o demandada-empleo de calidad-adecuadas condiciones de trabajo. La transición justa hacia la digitalización y hacia otras reasignaciones laborales pasa por la educación, la formación y la recualificación profesionales, por la preservación de las competencias y habilidades frente a su obsolescencia (educación *on-line*, aprendizaje permanente, incremento del conocimiento y de las competencias digitales). Hay aquí, por ello, una línea de transformación de los ordenamientos jurídicos indiscutible.

Resulta del mayor interés responder a la cuestión, de primera importancia, de si la Constitución, de la que pronto celebraremos su 46º aniversario, debe ser reformada, también, por el cambio tecnológico. Es un hecho sobradamente acreditado que las tecnologías que utilizan masivamente los datos de las personas, ponen a su disposición espacios de comunicación y conectividad permanentes y abiertos, utilizan predicciones sobre su comportamiento y elaboran perfiles, o desarrollan numerosos e intensos sistemas de censura, vigilancia y control en nombre de la seguridad pública (cámaras inteligentes, reconocimiento facial y análisis de redes sociales), poseen una enorme capacidad de invasión de su privacidad por gobiernos, empresas y otras personas, antes desconocida. Frente al derecho fundamental de libre información pensado para garantizar la libertad de prensa en las sociedades analógicas, la desinformación y la manipulación de la información en línea a través de internet y de las redes sociales es también una realidad constatada.

Es cierto que la tecnología puede reforzar también los derechos fundamentales, de acceso a la justicia por medio de servicios remotos y automatizados de plataformas digitales, de defensa de derechos de propiedad o a la identidad digital a través de blockchain, que permite registrar información de manera transparente e inalterable, de privacidad de los datos personales y del secreto de las comunicaciones mediante mecanismos de ciberseguridad y de cifrado. Como cierto es también que las tecnologías, utilizadas en esa dirección adecuada, no están destinadas a cambiar los valores comunes, sino a adaptarse a ellos[38].

---

[38] T. Kerikmäe y A. Rull, "Theorising on Digital Legal (Outer) Space", en T. Kerikmäe y A. Rull (eds.), *The future of Law and eTechnologies*, Springer International, 2018, pp. 1 y ss.

Sin embargo, la expansión tecnológica y de la IA plantea preocupaciones fundadas y desafíos significativos para la efectividad de los derechos fundamentales de las personas y los modos de su ejercicio en la realidad virtual; de cualquiera de ellos, aunque los que más hayan padecido por causa tecnológica, en las decisiones de nuestros tribunales, en las del TEDH o del TJUE, o en las de otros tribunales comparados, hayan sido los derechos a la protección de datos personales, a la libre expresión y libre información, y a la igualdad y no discriminación. Lo que no es seguro que precise de la reforma de las Constituciones soberanas de los Estados, lo que dependerá de la propia regulación de aquellas sobre los derechos fundamentales y sus relaciones con las normas internacionales de derechos si se modificara la Declaración Universal de derechos humanos para reconocer los neuroderechos, reconocimiento revindicado por un movimiento global de neurocientíficos y juristas con participación destacada de España. El art. 10.2 de nuestra Constitución, y su cláusula de interpretación evolutiva abierta a las normas internacionales y supranacionales, resuelve estos problemas. Hasta el momento, ninguna de las Constituciones de nuestro entorno europeo más próximo ha sido modificadas por causa de la digitalización y la IA, aunque algunas sí lo han sido para introducir el derecho, principio o valor de preservación del medio ambiente.

Volviendo a nuestra Constitución, no es precisa la reforma de los derechos que proclama. Solo la demandarían su artículo 18.4 con el fin de instaurar expresamente en su texto el derecho fundamental a la protección de datos personales y de la identidad digital como derecho fundamental de las personas de disposición y control de sus datos personales frente a terceros en la definición de su contenido esencial hecha por el Tribunal Constitucional[39], y su art. 20.1 para reconocer el derecho de acceso a la información tecnológica, Decisiva será la acción del legislador, primer intérprete de la Constitución, sujeto a ella y, muy en particular, a los derechos fundamentales (art. 53.1), complementada por la interpretación evolutiva del sistema de justicia constitucional, con el Tribunal Constitucional como su intérprete supremo, para dotar de protección efectiva al

[39] Derecho fundamental "creado" por el Tribunal Constitucional, a partir del derecho fundamental a la intimidad (art. 18.1), en el escaso espacio de la formulación literal del citado precepto constitucional –"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"–: SSTC 290/2000, FFJJ 7, 9 y 13; 292/2000, FFJJ 5-11.

ejercicio de los derechos fundamentales frente a los poderes públicos y privados en la sociedad digital y de la IA. Su defensa es objetivo estratégico de la defensa de la democracia constitucional.

Debiera ser obvio que la interpretación constitucional de los derechos fundamentales ha de experimentar cambios en los cánones o juicios de ponderación –principio de proporcionalidad, en su triple dimensión– de aplicación a la afectación de su ejercicio y disfrute por las tecnologías o la IA para dotarles en la sociedad digital de la vigencia efectiva, y de la imposición de su contenido esencial a los legisladores, que la Constitución exige. El ejemplo de la STC 17/2017 es desalentador al desconocer la vulneración del derecho fundamental de huelga, que reconoce el art. 28.2 de la CE, y desarrolla el preconstitucional RDL 17/1977, de 4 de marzo, por el esquirolaje tecnológico. En cambio, las SSTC 58/2018, 6/2019, 47/2019, 122/2019, 150/2019, 27/2020, 88/2020, 83/2023 y 31/1994, apuntan en esa dirección, apoyándose algunas de estas sentencias en decisiones precedentes del TEDH.

La Carta de Derechos Digitales, publicada en julio de 2021[40], puede ser un instrumento de valiosa ayuda para la interpretación jurídica.

La que creo una clave engañosa es la pretendida necesidad, o siquiera utilidad, de duplicar en las Constituciones los derechos fundamentales del mundo físico y analógico y del virtual. La universalidad de los derechos fundamentales y la inexistencia de una discrepancia entre las normas constitucionales que los declaran y establecen sus garantías y la realidad tecnológica hace innecesaria esa operación reformadora.

La necesidad de reforma de nuestra Constitución es, por el contrario, palmaria, en mi opinión, y apoyada en un cierto consenso doctrinal, además de en otros ámbitos materiales que no son aquí del caso, en el trasvase de algunos principios rectores de la política social y económica (protección de la familia, derechos a la seguridad social, a la protección de la salud, a un medio ambiente adecuado, a la vivienda, o derechos de las personas con discapacidad pese a la reciente reforma del art. 49 de 15 de febrero de 2024) a su parte de declaraciones de derechos y su conversión en tales a partir de un contenido esencial discernible. Cuestión distinta es la desgraciada inviabilidad política de la reforma constitucional.

---

[40] https://espanadigital.gob.es/lineas-de-actuacion/carta-de-derechos-digitales

El cambio tecnológico también se proyecta sobre la regulación constitucional del reparto competencial entre el Estado y las comunidades autónomas, que ha sido actualizado en lo referido a las competencias autonómicas por las reformas últimas de sus Estatutos de Autonomía, sin haberse hecho lo mismo con las competencias del Estado del artículo 149 CE. La STC 186/1999 diferenció las medidas de "reconversión industrial" de las actividades de *"promoción de la innovación tecnológica"*. Integradas aquellas en la materia "reestructuración de sectores industriales" y en las competencias autonómicas de desarrollo y ejecución de los planes estatales, estas lo hacen en la de "ordenación de los sectores industriales", en la competencia autonómica "exclusiva" sobre industria, ejercida en el marco de las competencias estatales sobre "bases y coordinación de la planificación general de la actividad económica" (art. 149.1.13ª), "fomento y coordinación general de la investigación científica y técnica" (art. 149.1.15ª) y "regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales" (art. 149.1.1ª). La "promoción de la innovación tecnológica" comprende las medidas que forman "parte de la vida ordinaria de las empresas, que habrán de incorporar de modo continuado las novedades de la ciencia y la técnica para atender a las necesidades impuestas por la competencia en los mercados" (FJ 7).

3.2. Los sistemas de fuentes de producción normativa; la principalidad de la ley (su dignidad democrática)

El segundo camino apunta derechamente al sistema de fuentes de producción normativa y a la estructura del ordenamiento jurídico. El papel principal de la ley parlamentaria –insustituible cuando haya de ser orgánica– debe ser destacado por su función señalada de desarrollo de los derechos fundamentales (arts. 53.1 y 81.1 CE), por los principios de reserva de ley y de congelación del rango, y, en definitiva, por la "dignidad democrática" de la ley, expresión de la voluntad general, esto es, de la voluntad de la mayoría en las democracias constitucionales. A un lado los límites materiales de los decretos-leyes, el cambio tecnológico y la utilización de la IA no deberían alcanzar, de ordinario, a cubrir el presupuesto de la urgente y extraordinaria necesidad que legitimaría constitucionalmente su inclusión en una norma de urgencia (art. 86.2). De ello hay, no obstante, decisiones de distinto signo de la jurisprudencia constitucional.

El debate entre la ley y el reglamento en contextos tecnológicos plantea reflexiones que retoman viejos debates sobre la necesidad de que la ley evite

excesos reglamentistas. Como en el mundo analógico, la ley ha de regular los aspectos generales y remitir al reglamento el desarrollo de cuestiones técnicas y específicas. Además de garantizar la claridad y buena técnica normativa, ello permitiría asegurar una mayor estabilidad de la ley. La tecnología permite, además, explorar nuevos mecanismos normativos. Los contratos inteligentes basados en blockchain podrían automatizar ciertos aspectos del cumplimiento normativo, reduciendo la necesidad de intervenciones legislativas frecuentes.

La recuperación de la ley y de su previsibilidad y determinación regulatorias es un objetivo irrenunciable en beneficio de la calidad de nuestra democracia y de la seguridad jurídica, esencial para el fomento de las inversiones de todo tipo, desde luego en la innovación tecnológica, pero también en las competencias digitales de las personas y en la especialización de los juristas.

En el ámbito propio del Derecho del trabajo, la negociación colectiva ha de tener un protagonismo indiscutible, llamada por reiteradas comunicaciones de la Comisión Europea a participar en los procesos de transición digital y energética y climática y asegurar su justicia social. En este contexto de transformación, el diálogo social cobra una relevancia especial. La participación activa de las organizaciones sindicales y empresariales, y de representaciones de la sociedad civil, garantiza que las normas no solo sean técnicamente adecuadas, sino también socialmente legítimas, ordenadas a asegurar la "justicia" de los procesos de transición. La inclusión de estas voces en el diseño normativo permite anticipar problemas éticos y garantizar que las regulaciones respeten la igualdad de oportunidades y la adquisición de cualificaciones apropiadas.

3.3. Reformas legislativas tecnológicas y técnica normativa

En tercer lugar, no puede dejar de transitarse el camino de la buena técnica normativa La elaboración de las normas debe cuidar la determinación precisa de sus mandatos, su calidad, que innegablemente facilita su aplicación sin litigiosidad y proporciona seguridad jurídica. El análisis de impacto normativo ha de valorar, junto con otros impactos reglamentariamente exigidos, el propiamente tecnológico, que precisará de conocimiento tecnocientífico de la materia que va a ser regulada[41].

---

[41] Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, art. 4.g).

El Gobierno ha creado recientemente la Oficina Nacional de Asesoramiento Científico por Real Decreto 158/2024, de 8 de febrero, con rango de subdirección general, integrada en la estructura de la Presidencia del Gobierno, encargada de establecer "mecanismos institucionales para el asesoramiento científico, identificar y potenciar casos de buenas prácticas dentro y fuera del sector público y ayudar a crear puentes entre el Gobierno y el talento científico que existe en centros de investigación y universidades"; o, como más expresivamente se dice en su web, de llevar el conocimiento científico a las políticas públicas, de "promover la inclusión del conocimiento científico como un pilar más en la toma de decisiones públicas", fomentar la cultura de la política pública informada por la evidencia científica (*'evidence-informed policy making'*) y "promover el valor público de la ciencia y la metodología de gobierno en su conjunto (*'whole-of-government approach'*) para la resolución de problemas complejos"[42]. El Congreso de los Diputados cuenta desde hace unos años, en virtud del convenio suscrito con la Fundación Española para la Ciencia y la Tecnología el 5 de marzo de 2021, con una Oficina de Ciencia y Tecnología, que tiene como principal objetivo proveer a la Cámara de evidencias científicas sobre determinados temas de interés, con objeto de contribuir a la toma de decisiones informadas para el conocimiento científico disponible[43]. Naturalmente, el conocimiento científico se mueve en el plano de la información para la adopción de decisiones políticas, sin sustituir a estas dentro del pluralismo político, valor superior del ordenamiento constitucional (art.1.1 CE).

3.4. El Derecho de la sociedad digital; y sobre el Estado de Derecho legislado y judicial en la democracia constitucional

El cuarto camino sale al encuentro de los caracteres de este Derecho. El avance de la tecnología requiere de marcos legales dinámicos, que, como la novedad de la materia, no pueden estar reñidos con el principio constitucional de seguridad jurídica (art. 9.3 CE). Esa necesaria adaptación normativa a los cambios de las tecnologías emergentes y a los cambios sociales no debe, sin embargo, comprometer la aspiración del marco legal a ser particularmente sólido y responder a una vocación de estabilidad durante su vigencia. Dado el carácter global de la tecnología, las respuestas legales deben coordinarse entre países para evitar

---

42 https://www.onac.gob.es/Paginas/index.aspx
43 www.congreso.es/es/cem/oficinacienciatecnologia

vacíos regulatorios. El Derecho supera las fronteras estatales para acomodar su regulación a la globalización económica, a la innovación tecnológica, a las cadenas mundiales de suministro.

Especial atención merecen las denuncias de un exceso de Derecho y las demandas de un Derecho flexible y de poco Derecho para la regulación del avance y la innovación tecnológica, que se suman a las que se han venido proclamando desde el pasado siglo con causa en las crisis económicas y, paradigmáticamente, en la gran recesión financiero-económica de 2008. El Derecho rígido sería cosa del pasado, del mundo analógico. En un entorno tecnológico dinámico, donde las innovaciones pueden redefinir sectores completos en cuestión de meses, la rigidez de los mandatos normativos, se convertiría en un obstáculo; especialmente infranqueable se señala, para las pymes europeas, sujetas a cargas fiscales y de cumplimiento de diferentes normativas estatales exorbitantes, si, además, las normas, del tipo del Reglamento de Inteligencia Artificial, adoptan enfoques preventivos de su incumplimiento y sanciones disuasorias ante la consumación de ese incumplimiento. Estas denuncias se leen en el informe Draghi, que se queja también del excesivo tiempo de tramitación de los actos normativos de la Unión, mayor si deben ser transpuestos por los Estados, todo lo cual contribuiría a levantar impedimentos infranqueables al cierre urgente de la brecha europea de digitalización y a la imprescindible ganancia de competitividad y productividad de la economía europea. Además, las normas de regulación de tecnologías específicas corren el riesgo de quedar obsoletas tan pronto como estas evolucionen o sean reemplazadas por otras.

Un Derecho flexible y adaptable, un *soft law*, basado en principios generales, previsiones de carácter programático, directrices y normas finalistas y acomodables, ofrecería una mayor capacidad de respuesta a la necesidad imperiosa de digitalización de la economía en todos los sectores, y en concreto a la reindustrialización digital de Europa. Este enfoque permitiría interpretar y aplicar las normas según las circunstancias cambiantes, sin necesidad de constantes reformas legislativas.

No ha sido este, como ha quedado dicho, el enfoque adoptado por la UE, que ha elegido su instrumento normativo de mayor rigidez, el reglamento, para regular la protección de datos personales y su libre circulación en el espacio económico europeo, los mercados y los servicios digitales o la IA; en lo que ha coincidido el informe Letta, que preconiza, en el ámbito legislativo, la priorización de la aprobación de reglamentos para la regulación del mercado único, directamente

aplicables en los Estados miembros, frente a las directivas, que requieren de transposición a los ordenamientos jurídicos de cada país, fragmentan la armonización y causan el *gold plating o sobreregulación* de las normas estatales[44].

Tampoco se acomoda ese enfoque a la buena técnica normativa. Sirva la cita del dictamen del Consejo de Estado núm. 146/2023, de 16 de marzo, "*aun cuando no cabe desconocer la importancia de definir los objetivos que deben guiar la acción de los poderes públicos y aun la conveniencia de incluir en las normas jurídicas los principios que han de inspirar una determinada regulación y orientar su interpretación, es necesario evitar la acumulación en un texto legal de preceptos que se limitan a recoger formulaciones programáticas genéricas y excesivamente abiertas [...]. Una buena técnica normativa exige que las normas jurídicas identifiquen con claridad y precisión los mandatos que imponen, los derechos que reconocen y las conductas que permiten o prohíben, y se abstengan, en cambio, de incorporar declaraciones meramente teleológicas o propósitos sin contenido normativo propio*"[45]. Para esos contenidos existen otros instrumentos jurídicos, a excepción del caso de las leyes de bases en el reparto de competencias con las comunidades autónomas. Pero ni el Código civil, ni el de comercio, ni el penal, ni las grandes leyes sectoriales –no básicas o básicas complementadas con leyes autonómicas– y sus reglamentos pueden dejar de serlo por la necesidad de adaptar sus contenidos a la transformación social tecnológica y de la IA.

Una reflexión final: si el Derecho se volviese principal al regular la incidencia de las tecnologías y de la IA en los distintos ámbitos de la vida económica y social, el espacio de la interpretación judicial evolutiva se agrandaría, confirmándose, también por la vía de la transformación tecnológica, la conversión del Estado de Derecho legal en judicial, puesta de manifiesto y censurada por tantos autores. Iniciada esa conversión del Estado de Derecho con el control jurisdiccional de la constitucionalidad de la ley, evolucionada de la mano de la complejidad creciente de la aplicación/inaplicación de la ley, que decidida por el TJUE y los jueces y tribunales ordinarios apenas esconde un juicio indirecto sobre la validez de la ley estatal inaplicada, la desvinculación del juez del Derecho legítimamente

---

[44] Cit., pp. 125-126.

[45] Consejo de Estado, *Memoria del año 2023*, Madrid, 2024, pp. 174-175; https://www.consejo-estado.es/wp-content/uploads/2024/07/Memoria-2023.pdf; https://www.consejo-estado.es/portal-de-transparencia/asuntos-despachados/comision/derechos-sociales-y-agenda-2030-2/; anteproyecto de Ley de Familias.

aprobado por los órganos de un Estado "basado fundamentalmente en una idea de creación judicial del Derecho"[46] se fortalecería con un Derecho legislado de la sociedad digital y de la IA meramente referencial e indicativo para el arbitrio judicial. Un cambio del modelo de Estado previsto en la Constitución en mi modesto criterio, que poco prometería para el renacimiento del principio de seguridad jurídica en tiempos de incertidumbre tecnológica, que, también para muchos autores, son tiempos de esperanza.

El desafío es, en definitiva, construir y reconstruir un Derecho que fomente la innovación tecnológica y la regule frontalmente, garantizando el respeto de los derechos fundamentales y la justicia social de las transiciones digital y climática y de sus efectos sobre las personas y las sociedades inclusivas, corrigiendo sus efectos de desigualdad económica y social. La transformación tecnológica ha de asegurar la consolidación del modelo social de la Unión Europea y de los Estados de bienestar europeos y de sus democracias constitucionales.

---

[46] F. Caamaño Domínguez, "Los vértices de la desconfianza: Constitución, ley y juez (Releyendo Justicia constitucional y democracia, de Víctor Ferreres Comella)", *Revista Española de Derecho Constitucional*, núm. 65, 2002, p. 389, núm. 1.

Primera Parte

ESTUDIO INTRODUCTORIO

Capítulo 1
JUEZ CON ROBOT, MÁS QUE ROBOT JUEZ

Andrés Ortega Klein
Analista y escritor

1. INTRODUCCIÓN

Max Weber consideraba que la economía y la sociedad modernas pretenden que el ordenamiento jurídico sea racional, calculable y predecible "como una máquina"[1]. Demasiado simple ante tema tan complejo. ¿Qué pensaría el sociólogo alemán al ver las posibilidades que brinda la revolución tecnológica en curso, especialmente la llamada inteligencia artificial (IA), que está en sus inicios? El impacto, desde la formación del Derecho hasta su aplicación, de la ola de innovación a la que nos vemos arrastrados, está ya empezado a forzar que la Justicia adquiera una nueva dimensión, que podríamos calificar de Tecnojusticia[2]. Utilizará robots, entendidos estos como máquinas o como programas con sus algoritmos, para lo que sirve indistintamente hablar de IA o de robots[3]. El Derecho y todo lo que le atañe no podía, no puede, quedar al margen de esta nueva Revolución Industrial, que plantea nuevas cuestiones, nuevas soluciones y nuevos problemas, y que transformará la Justicia en diversos aspectos. ¿Llegaremos,

---

[1] Weber, M. (2000). *Economía y sociedad*, FCE.

[2] Sigo en esto la lógica de Echeverría, J. y Almendros, L. S. (2020). *Tecnopersonas*, Trea.

[3] Los ingenieros industriales suelen limitar el término robot a máquinas. Los de informática o similares incluyen entre ellos los programas. El Diccionario de la RAE define robot como "máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones", mientras que el panhispánico de dudas lo hace de una forma inadecuada como "máquina programable capaz de realizar trabajos antes reservados solo a las personas". En mi libro *La imparable marcha de los robots* (Alianza, 2016) utilicé la definición del ingeniero Eduardo Castelló: un robot es un "algoritmo capaz de interactuar físicamente (a través de algún dispositivo) con su entorno".

como plantea el juez Manuel Marchena[4], a "la sustitución de la persona que dicta el derecho por una máquina que haría lo propio, pero a partir de una información tratada mediante fórmulas algorítmicas"? Hoy, no. Pero mañana es posible que en algunos casos sí, siempre que se den algunas garantías, la principal, que al final de la cadena decisoria haya un juez humano. A la larga, pasado mañana, esta ola, especialmente la capacidad de transformación que supondrá la combinación de IA y la biología sintética[5], con ingeniería genética o su conexión directa mediante implantes a la nueva cibernética, puede llegar a cambiar el concepto y la realidad de lo que llamamos "ser humano", y, por lo tanto, de su Justicia. Unos seres humanos que pueden llegar a ser transhumanos[6].

La IA y otros avances tecnológicos afectarán, están empezando a afectar ya, a todo el recorrido de la Justicia, desde la elaboración de las leyes, a las deliberaciones, en su caso, de los jurados (necesariamente humanos, pues no tiene sentido hablar de jurados por IA, aunque sí apoyados en ella), pasando, claro está por el trabajo de la acusación, del abogado defensor y el papel central de los jueces. Como con toda la IA, hay que aspirar también a una IA en el ámbito jurídico centrada en lo humano (*human centered* o *human centric*), lo que implica, como han señalado Rezaev y Tregubova[7] el respeto a tres principios: el ser humano como eslabón necesario en la cadena de toma y ejecución de decisiones jurídicas; la necesidad de regular la inteligencia artificial en el ámbito del Derecho internacional; y la formulación de un cierto *tabú*, o limitación, en la introducción de las tecnologías de inteligencia artificial.

Estamos cercanos a un Tecnoderecho, aprobado por humanos, escrito y aplicado con ayuda de la IA. Se deriva la posibilidad de tecnoprocesos, informados

---

[4] Marchena, M. (2022). "Inteligencia artificial y Jurisdicción Penal", Discurso leído en el acto de su recepción como Académico de número de la Real Academia de Doctores de España 2022. https://bit.ly/4bjpz8b

[5] Suleyman, M. y Bhaskar, M. (2023). *La ola que viene: Tecnología, poder y el gran dilema del siglo XXI*, Debate. Ofrece una de las mejores panorámicas sobre estas revoluciones conexas y cómo afrontarlas.

[6] Ver Diéguez, A. (2017). *Transhumanismo. La búsqueda tecnológica del mejoramiento humano*, Herder.

[7] Rezaev, A. V. y Tregubova, N. D. (2023). "The Possibility and Necessity of the Human-Centered AI in Legal Theory and Practice". *Journal of Digital Technologies and Law, 1*(2), 564-580. https://doi.org/10.21202/jdtl.2023.24

por la IA, tanto en el examen de los hechos, como en la investigación de los antecedentes y las conclusiones, en las diligencias, para marcar la línea de la acusación, de la defensa, o en la decisión judicial, del veredicto y de la pena, si la conllevara. ¿Iremos hacia un tecnojuicio, con instrumentos robóticos adjudicativos o una justicia algorítmica predictiva, como la incipiente policía predictiva? O, más bien, a un juicio *con* IA, más que *por* IA, un sistema de ayuda robótica en sus diversas fases, más que de sustitución del elemento humano. Aunque el avance de la IA en la labor judicial plantea la cuestión del Razonamiento Jurídico por IA como elemento crucial en el ejercicio de las diversas dimensiones de la actividad judicial, del abogado al juez. Lo que puede derivar en una distopia, si la IA usurpa los principios de la Justicia, o en una utopía si los refuerza e impulsa[8].

Aunque la Justicia es mucho más y cuente con múltiples jurisdicciones, aquí nos centraremos esencial mas no únicamente, en el terreno de las causas penales y civiles, quizás de las más humanas. Los dos principales protagonistas son el acusado, o los que dirimen conflictos entre ellos, sean personas o colectividades, y el juez (en su caso con jurado), el último peldaño de la administración de Justicia. En nuestro sistema, el juez debe aplicar la ley, pero la ley es una entelequia que requiere interpretación. De otro modo, no serían necesarios los jueces, ni todo el sistema, sino que se podría dictar sentencia (y pena) de manera automatizada. Es decir, que lo podría hacer una máquina, como pretendía Max Weber. ¿Puede una máquina apreciar ante un caso, por ejemplo, ante una puñalada mortal a una persona, si se trata de un homicidio voluntario o involuntario o de un asesinato, y para ello, sopesar los factores eximentes o atenuantes, como la defensa propia, o los agravantes? Hoy por hoy, evidentemente no. ¿Y mañana o pasado mañana?

La Justicia vive en polisemia, es decir en pluralidad de significados de las expresiones lingüísticas, en este caso de las leyes. Admite multitud de elementos condicionantes al juicio de lo que ha ocurrido. En los juicios incluso influye la actitud, el tono, la mirada del acusado, lo no palpable, frente al juez, o frente a una IA que habrá avanzado mucho en este terreno de detección de emociones y sinceridades. En el fondo estamos hablando de los elementos intangibles, pero esenciales, en la Justicia. Siempre dentro de una cierta cultura (incluida la internacional), que cambia según las sociedades y los tiempos, aunque sus for-

---

[8] Eliot, L. B. (2020). "An Impact Model of AI on the Principles of Justice: Encompassing the Autonomous Levels of AI Legal Reasoning". https://bit.ly/3wqulkk

mulaciones permanezcan (por ejemplo, el "derecho a la vida", en artículo 15 de la Constitución Española, que no ha impedido aprobar leyes sobre el aborto ni sobre la eutanasia). La formulación puede permanecer cambiando el contenido. La Justicia es una creación intelectual e histórica. ¿Tendrá la IA esta capacidad? ¿Sabría rendir justicia un robot? ¿Cómo un rey absoluto? De momento, ante las IAs específicas más que generales, no. Incluso ante las generales, que superaran o fueran distintas de la inteligencia humana, estas IAs no tendrían, consciencia, ni comprensión para entender sus propias decisiones.

2. INDUCCIÓN, DEDUCCIÓN, ABDUCCIÓN

La IA sin duda es artificial, pero ¿es inteligencia?[9] A la hora de aplicarla a un proceso judicial, debería serlo, y sin embargo no lo es, o, al menos, no lo es aún. No obstante, es capaz de generar resultados que no se le habrían ocurrido a un humano. Aunque a diferencia de la sentencia de un juez, o de un jugador de golf o de ajedrez, no digamos ya de un general en una guerra, no entiende sus propias conclusiones. Bien es verdad que cada vez los humanos entienden menos lo que ocurre dentro de la IA, cómo los algoritmos procesan la información para llegar a conclusiones, tema que abordaremos posteriormente.

Hoy por hoy, la IA es, esencialmente, una inteligencia estadística, probabilística, no exacta ni precisa[10] (ni en el terreno que nos ocupa intrínsecamente justa). De ahí que algunos como Emily M. Bender y Timnit Gebru[11], entre otros, hayan denominado "loros estocásticos" a unas IAs que se limitan a imitar el lenguaje sobre la base de patrones estadísticos de datos, sin comprender su significado. Así, más que deductiva, la actual IA es una inteligencia aproximativa e inductiva. Deriva sus conclusiones o pautas de ingentes cantidades de datos, los *Big Data*, que un humano por sí solo no abarcaría. Es una inteligencia, por llamarla así, que establece correlaciones antes que causalidades. Los LLMs (*large language models*, o grandes modelos de lenguaje), como el chat GPT y otras

---

[9] Ortega, A. (2023). "Artificial, sí; pero ¿inteligencia?", Telos, 28.11.2023. https://bit.ly/3wBReRQ

[10] La exactitud mide la proximidad de un valor medido al valor verdadero, mientras que la precisión mide la proximidad de los valores medidos entre sí.

[11] Bender, E. M, Gebru, T., et al. (2021). "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?", 01.03.2021. https://dl.acm.org/doi/10.1145/3442188.3445922

IA generativas basadas en lógicas esencialmente bayesianas[12], seleccionan en el texto o información que se somete a pautas de lenguaje y de temas, y devuelve la respuesta en forma de textos, imágenes, música, códigos y fórmulas, bastante bien escritos o dibujados, aunque aún de poca fiabilidad. Pero, estas capacidades de la IA generativa, lanzada en 2022-2023 ante el gran público con un impacto global inmediato, y otras IAs se están convirtiendo ya en elementos esenciales de todo procedimiento judicial, ayudando a redactar autos, líneas de defensa, resúmenes del expediente judicial, o antecedentes.

En general, en todos los campos en los que puede operar, las conclusiones de la IA inductiva suelen ser aproximadas, no "prueban", no "demuestran", sino que llegan a aproximaciones por encima de un 95%, pero no exactas. Tampoco los humanos, en el caso que nos ocupa los jueces, todo hay que decirlo. Aunque esta aproximación podrá crecer de la mano de la computación cuántica, por venir. La capacidad deductiva se está desarrollando cada vez más con los avances en razonamiento deductivo en la IA, por ejemplo, en la demostración no simplemente estadística, de algunos problemas matemáticos complejos por parte de AlphaGeometry, de Google DeepMind[13]. AlphaGeometry sintetiza millones de teoremas y pruebas de distintos niveles de complejidad. Es un sistema neurosimbólico que utiliza un modelo de lenguaje neural, entrenado desde cero en los datos sintéticos a gran escala, para guiar un motor de deducción simbólica a través de infinitos puntos de ramificación en problemas desafiantes, explican los autores. ¿Es posible esta tecnología para la interpretación y aplicación del Derecho? Desde luego, facilitaría la vida de los juristas en sistemas, como el de Estados Unidos, que se basan más en los casos precedentes que en la interpretación directa de la Ley.

Si la inducción no es exacta, la deducción tampoco a la hora de aplicar o interpretar las leyes. Esto último es algo más complejo que implica valorar pruebas, elegir entre opciones, y evaluar la influencia de diversos factores, no sólo basándose en precedentes, todo ello con, a menudo, consideraciones culturales, éticas o emocionales. La IA todavía no ha llegado a eso, aunque podría hacerlo

---

[12] Tipo de inferencia estadística en la que las evidencias se emplean para inferir la probabilidad de que una hipótesis pueda ser cierta.

[13] Trinh, T. H., Wu, Y., Le, Q. V., et al. (2024). Solving olympiad geometry without human demonstrations. *Nature 625*, 476-482.

a medida que progrese[14], previsiblemente con algunos límites. En todo caso, la Justicia no es binaria, respondiendo con un "sí" o un "no", con un "0" o un "1".

Sin entrar aquí en el tema central de la intuición para el conocimiento y las decisiones humanas, hay varios caminos en la inferencia, el proceso de sacar conclusiones basadas en pruebas y razonamientos. Los abogados y los jueces, y otros actores judiciales, como un jurado, utilizan la inferencia para construir argumentos y extraer conclusiones a partir de las pruebas presentadas ante los tribunales. La inferencia es algo fundamental en la IA. De hecho, está pasando de ser en un 70% entrenamiento (con datos) y 30% inferencia a invertir esta proporción. Ahora bien, es importante recordar que las inferencias no siempre son exactas. La calidad de la conclusión depende de la calidad de las pruebas y del proceso de razonamiento utilizado, del proceso de inferencias. Los sesgos, prejuicios y la información incompleta pueden dar lugar a inferencias erróneas.

Dentro de la inferencia, entre la inducción, que busca pautas en datos siempre incompletos por muy masivos que sean, y la deducción, en la que la conclusión sigue a las premisas, existe una tercera opción, la abducción, que se abre crecientemente paso en este terreno. Esta consiste en buscar con una conjetura la explicación mejor o más probable, que se aplicaría a diversos campos, entre ellos la Justicia, y, ante un resultado repetir el proceso para mejorar la conclusión[15]. El razonamiento abductivo formula una hipótesis que sea la mejor explicación posible de los datos disponibles y sobre esa base vuelve a comenzar el proceso hasta llegar a una explicación satisfactoria o completa. Los jueces, fiscales, abogados defensores, jurados y otros, por medio de presunciones y pistas para probar los hechos, utilizan más ese razonamiento abductivo, con el cual se llega a conclusiones no contenidas en las premisas. Es un proceso iterativo que opera hacia atrás. A medida que se recopilan más datos, es posible que sea necesario volver a evaluar las hipótesis y seleccionar una nueva hipótesis más probable. Es como puede operar un policía o un detective. También la IA. Es como más se acercaría al proceso de decisión de un juez. En este sentido, el robot juez, en la medida en que se desarrolle, tenderá a ser cada vez más abductivo.

---

[14] Entrevista con Jensen Huang, CEO de NVIDIA, 24 de febrero de 2024. Wired. Nvidia CEO Jensen Huang Is Powering the AI Revolution | WIRED.

[15] Ortega, A. (2023). "Nuevas Inteligencias", *Telos*, 25.05.23 https://telos.fundaciontelefonica.com/nuevas-inteligencias/

Para Luciano Floridi[16] la IA no tiene un enfoque descriptivo ni prescriptivo del mundo. Inscribe nuevos artefactos que interactúan con la naturaleza, convirtiéndose en parte de ella. La tecnología de inteligencia artificial, aplicada al Derecho, como a otras cosas, asume que existen patrones generales que tratarán de la misma manera casos similares. No es el caso del juez humano para el que cada caso tiende a ser independiente, aunque tenga precedentes.

Las IAs son máquinas que aprenden, de sí mismas, de sus propios procesos y conclusiones o de la información con la que se les entrena, aunque no sean conscientes de ello. Tampoco está claro qué es la conciencia humana (sí que la tenemos, al menos a ratos) y, sin embargo, los humanos aprenden también. El aprendizaje de las máquinas será crucial en este campo del Derecho y la Justicia, quizás incluso sacando inducciones, deducciones o abducciones que a los juristas humanos no se les había ocurrido, como algunas IAs avanzadas han descubierto nuevas maneras de jugar, por ejemplo, al ajedrez o al go, en las que los propios grandes maestros no habían pensado. Ahora, estos se entrenan con IAs para mejorar su juego. Lo mismo puede pasar con el Derecho y su aplicación. Especialmente con el desarrollo de una IA simbólica, frente a la subsimbólica. El enfoque subsimbólico, como explica Asunción Gómez Pérez, se centra en el aprendizaje automático de modelos numéricos a partir de cantidades masivas de datos. El simbólico emplea símbolos alfanuméricos –es decir, palabras– y reglas lógicas para representar los datos y los conocimientos que los humanos tienen acerca de un dominio para, posteriormente, generar nuevo conocimiento mediante procesos de inferencia o de razonamiento[17]. Se acerca más a lo que ahora entendemos por IA generativa en lenguaje natural.

Ahora bien, no cabe obviar que la IA también se equivoca. Alan Turing (1912-1954) uno de los pioneros y padres fundadores de la informática y de la IA, ya reconoció el derecho al error de las máquinas. El de los seres humanos se da por supuesto. También el juez humano se equivoca. La introducción de la IA en algunos ensayos en sistemas judiciales no suele llegar a conclusiones superiores a un 97% de certeza (en otros campos puede ser superior). ¿Es comparable

---

[16] Floridi, A. (2014). *The Fourth Revolution: how the infosphere is reshaping human reality*, Oxford University Press.

[17] Gómez Pérez, A. (2023). "Inteligencia artificial y lengua española", discurso de ingreso en la Real Academia Española, 21.05.2023 https://bit.ly/48spb4I

a la capacidad de generar la verdad jurídica de un juez (que no es la verdad como se entiende en Ciencia o Filosofía)? Sin duda. ¿Equivale eso a la máxima de "más allá de toda duda razonable"? El 100% de certeza tampoco es humano en el terreno que nos ocupa. Aunque haya "hechos probados" también cuentan los datos indiciarios, entre otros. De ahí lo de "razonable", pero lo razonable no está definido de manera clara y computable. La profesión jurídica está plagada de ambigüedades[18]. Ni la Justicia humana, ni asistida por IA, ni una eventual justicia solo por IA, son garantía contra estas ambigüedades, aunque las puede reducir, ni contra los errores judiciales. ¿Quién los rectifica si domina la IA? ¿La propia IA utilizada, otra superior, o un juez humano?

3. ¿JUSTICIA ALGORÍTMICA?

¿Reemplazarán las máquinas o los sistemas de adjudicación por IA a los seres humanos en el proceso judicial? Caben pocas dudas de que estas máquinas o sistemas se irán crecientemente encargando de algunas tareas que hasta ahora desempeñaban humanos o de que, como poco, trabajarán con ellos, como ya se ha analizado en otros capítulos. Aquí lo que nos interesa es la cuestión de si la tecnología pueda remplazar al fiscal, al juez, o incluso al abogado defensor.

No se trata de ciencia ficción. La justicia algorítmica ya se está experimentando en diversos lugares. En Países Bajos para separaciones matrimoniales. En Reino Unido para reclamaciones civiles inferiores a 10.000 libras. En España para detectar en comisaría denuncias falsas con un 91% de aciertos. En China con un fiscal capaz de presentar cargos con un 97% de precisión. En Estados Unidos para ayudar al juez a calcular el riesgo de reincidencia en caso de puesta en libertad condicional ante nuevos delitos (apareciendo en el proceso sesgos en contra de los negros derivados de los propios datos que los que se han entrado a la IA). También en el sector privado. Por ejemplo, el sistema de resolución de disputas de las empresas eBay y PayPal gestiona unos sesenta millones de desacuerdos al

[18] Osarodion Progress Friday (LL.B, University of Benin) (2023). "Artificial intelligence in the realm of law: a bane or a boon vis-a-vis the legality or otherwise of a robot lawyer", Research Paper. https://bit.ly/49aYP88

año, lo que representa tres veces todo el sistema judicial estadounidense. El 90% de estas disputas se resuelven utilizando tan solo la tecnología[19].

Se han ensayado ya numerosos prototipos de ayuda a los abogados y ciudadanos. En Alemania, el proyecto *Argumentum* ha desarrollado un *software* para apoyar la identificación, el análisis y la selección automatizados de estructuras de argumentación jurídica. En Rusia, se ha intentado crear un sistema intelectual, apodado "Robot Abogado", para proporcionar a los letrados información sobre los procesos con distintos niveles de complejidad. En Brasil, se está investigando un sistema de recuperación de información jurídica de precisión, llamado Razonamiento Basado en Casos (RBC), en el que se usan casos anteriores para resolver otros actuales. En Italia se intenta definir los componentes teóricos y tecnológicos que permitan a un ciudadano obtener orientación y formación sobre conceptos jurídicos a partir de una descripción textual de un caso. Es decir que algunas investigaciones en curso tratan de servir directamente a los ciudadanos en apuros con la Justicia. En Italia, el Consejo de Estado italiano exige control sobre las decisiones administrativas "digitales": el juez debe controlar cada paso lógico dado por el algoritmo, anulando la decisión administrativa si la motivación no es coherente o suficiente[20].

El impacto de la tecnología en lo judicial resulta imparable, pero plantea diversos problemas de calado. Hay un consenso entre juristas en que el judicial es, con el arte, una de las actividades humanas en la que la naturaleza humana se manifiesta más plenamente, en la que la razón y la emoción están presentes, sin que tenga que prevalecer la segunda, sino el equilibrio entre ambas[21,22]. Otros van más lejos y opinan que las emociones son un componente esencial del razonamiento y son una guía cognitiva no sustituible. Sin emociones, un hombre

---

[19] Rule, C. (2023). "Separating the People from the Problem", Practice, julio de 2020, citado por Suleyman, M. y Bhaskar, M.: *La ola que viene: Tecnología, poder y el gran dilema del siglo XXI*, Debate.

[20] Porcaro, K. (2023). "Robot Lawyers Are About to Flood the Courts", *Wired*, 27/6/23, https://bit.ly/42YZxDn y Ovi, C., Salvia, L., Tonnara, P. y Perrone, F., "The judge of the future: artificial intelligence and justice", https://bit.ly/3wIdKIY

[21] John Tasioulas. "The Rule of Algorithm and the Rule of Law", febrero de 2024. https://bit.ly/3P6W9R1

[22] Alfaia Sampaio, E., Seixas, J. J. y Gomes, P. G. (2019). "Artificial intelligence and the judicial ruling", European Judicial Training Network. https://bit.ly/3wqulkk

puede razonar perfectamente pero no es capaz de decidir[23]. Un juez no puede juzgar según sus emociones o sentimientos, como la compasión o la misericordia, pues se podría dejar llevar por sus sesgos personales, ideológicos o religiosos[24], pero los tiene y le influyen.

Los robots son capaces de detectar emociones en los seres humanos, de ser empáticos, pero no de tener emociones ellos mismos, al menos de momento. La IA podría ser capaz, ya lo es de hecho, no sólo de captar nuestras emociones, sino también nuestros deseos, incluso de hacernos desear cosas que no sabemos que deseamos. Es la base de la nueva publicidad. Puede acabar conociéndonos mejor de lo que nos conocemos a nosotros mismos. Acabar sabiendo, sino lo que, sí cómo pensamos, nuestras tendencias, nuestras preferencias. Esa información en manos de la acusación o un juez puede ser muy dañina para la seguridad del acusado. Aunque, de hecho, como se ha mencionado, ya se empieza a usar para, por ejemplo, calibrar, para ayudar al juez a sopesar la posibilidad de reincidencias antes de poner a un reo en libertad condicional.

Esas capacidades podrían llevar a que un veredicto dictado por un juez artificial, por un robot juez, no solo no fuera exacto, como hemos visto, sino tampoco justo. Luego están las convicciones morales, ideológicas o religiosas que se pueden asemejar a las emociones. Jueces y juristas deberían dictaminar sin dejarse influir por ellas. Pero, en un cierto grado, parecen inevitables[25]. ¿Sería una garantía que las máquinas no tengan convicciones morales, más allá de la programación a partir de instrucciones humanas (que puede ser sesgadas)? Probablemente no.

¿Puede un robot juez ser imparcial? Para Marchena[26] y otros, del robot juez no puede esperarse la "justa decisión". "Decidir no es lo mismo que ejecutar programas". Para Tasioulas, un robot juez "socavaría la explicabilidad, la rendición de cuentas y la reciprocidad o la comunidad que están íntimamente ligadas al cumplimiento ideal del Estado de Derecho y, en particular, el desiderátum de

---

[23] Ovi, et. al. *Op. cit.*

[24] Marchena, M. *Op. cit.*

[25] De La Cuadra Salcedo, T. (2024). "Las convicciones morales de los magistrados y las decisiones de los tribunales", *El País*, 24 de enero de 2024. https://bit.ly/3IjYe8u

[26] Marchena, M. *Op. cit.*

congruencia entre la ley y la decisión oficial"[27]. ¿Sería mejor, más imparcial, un robot juez, sin emociones, sin convicciones morales, ideológicas o religiosas? Tampoco, porque carecería de otros atributos necesarios.

Aunque las famosas tres leyes de la robótica de Asimov no son morales sino utilitarias. El robot no tendría consciencia de aplicarlas. Pero las aplicaría. Asimov se dio cuenta más tarde que eran insuficientes, o contradictorias, e introdujo una cuarta, más protectora: un robot no puede hacer daño a la humanidad o, por inacción, permitir que la humanidad sufra daño[28]. En todo caso, se han demostrado que son insuficientes. ¿Sería capaz una IA de dirimir el caso de un no binario que quisiera adoptar a un niño o niña sin decantar su propio sexo?

El futuro que se entreve en este campo no es uno de máquinas que reemplacen a humanos en la decisión judicial, sino de un sistema humano-máquina, que puede conservar rasgos emocionales y morales. Y que tenga en cuenta que la ética y la moral, incluso partiendo de la Declaración Universal de los Derechos Humanos, son cambiantes en términos históricos y geográficos. Hay entre los humanos varias maneras de enfocar estas cuestiones. ¿Cómo se trasladará esto a las máquinas y a la Tecnojusticia? El caso del coche autónomo es el ejemplo más trillado. Un nuevo derecho humano puede ser el derecho a saber con qué criterios éticos y morales funcionan las máquinas que nos afectan. Un derecho más difícil de cumplir cuando, como se ha explicado, el funcionamiento interno de las propias IA se convierte en opaco a medida que los programas se vuelven más complejos.

La cuestión ética está en el centro de los debates para regular la IA en la Justicia. La Comisión Europea para la Eficiencia de la Justicia (CEPEJ) del Consejo de Europa adoptó en 2018 el primer texto europeo, una Carta[29], que establece principios éticos relacionados con el uso de la inteligencia artificial (IA) en los sistemas judiciales. La Carta proporciona un marco de cinco principios que pueden guiar a los responsables políticos, legisladores y profesionales de la justicia cuando lidian con el rápido desarrollo de la IA en los procesos judiciales

---

[27] Tasioulas, J. *Op. cit.*

[28] Ortega, A. (2016). *La imparable marcha de los robots*, Alianza Editorial, pp. 51-52 y 100-102.

[29] European Commission for the Efficiency of Justice (CEPEJ) (2018). *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, Consejo de Europa. https://bit.ly/4317CHC

nacionales: 1) Principio de respeto de los derechos fundamentales: garantizar que el diseño y la aplicación de herramientas y servicios de inteligencia artificial sean compatibles con los derechos fundamentales; 2) Principio de no discriminación: impedir específicamente el desarrollo o la intensificación de cualquier discriminación entre individuos o grupos de individuos; 3) Principio de calidad y seguridad: en relación con el procesamiento de resoluciones judiciales y datos, utilizar fuentes certificadas y datos intangibles con modelos elaborados de forma multidisciplinar, en un entorno tecnológico seguro; 4) Principio de transparencia, imparcialidad y equidad: hacer accesibles y comprensibles los métodos de tratamiento de datos, autorizar auditorías externas; y 5) Principio de "bajo el control del usuario": excluir un enfoque prescriptivo y garantizar que los usuarios sean actores informados y controlen las decisiones tomadas. Para la CEPEJ, el cumplimiento de estos principios debe garantizarse en el tratamiento de las resoluciones judiciales y de los datos por algoritmos y en el uso que se haga de ellos.

Su objetivo es garantizar que los usuarios sean actores informados y tengan el control de sus decisiones. Pero no dice cómo. Le falta la dimensión técnica, ingenieril, para asegurar que la IA que se pueda utilizar en la Justicia sea veraz y confiable (*truthful and reliable*), más incluso que transparente y entendible.

Una de las mayores preocupaciones en torno al despliegue de grandes modelos de lenguaje (LLMs, que están detrás de la IA generativa) es su complicada relación con la verdad, ejemplificada en su tendencia a alucinar, como señala el investigador y emprendedor Richard Socher[30]. Alucinar, en este contexto significa generar información plausible pero incorrecta o sin sentido, generar información que no es real o que no se basa en datos reales, por haber sido la IA generativa entrenada con datos que son inexactos o incompletos, ser demasiado creativa y generar información que no es consistente con los datos con los que se entrenó, o ser utilizada para engañar a la gente, por ejemplo, para crear noticias falsas o propaganda[31], entre otras razones. Algunos autores[32] consideran que las alucinaciones son inevitables, son una «limitación innata», de

---

[30] Socher, R. (2024). Entrevista en Exponential View de Azeem Azhar, 31/01/2024. https://bit.ly/3P7T7Mp

[31] Definición data por Gemini.

[32] Xu, Z., Jain, S. y Kankanhalli, M. (2024). "Hallucination is Inevitable: An Innate Limitation of Large Language Models". https://bit.ly/3IkLs9O

los grandes modelos de lenguaje debido a su diseño: no hay representación de hechos o cosas, solo correlaciones estadísticas.

Ya ocurrió en el caso de un abogado neoyorquino que utilizó ChatGPT como ayuda para redactar el informe de su caso contra la aerolínea colombiana Avianca. La IA le proporcionó jurisprudencia totalmente ficticia. Fue inmediatamente denunciado por el abogado contrario y el juez, y el defensor fue multado. Por eso quizás los grandes bufetes no quieren precipitarse en invertir en una IA que plantea dudas, aún más si su información es externa o saca la información del bufete fuera para megadatos que otros puede utilizar[33]. La Justicia no se puede permitir alucinar (en este sentido, ni en otros), aunque la alucinación puede generar creatividad también en el campo judicial, como en otros. Hay que insistir en la necesidad de que la IA sea no solo A, sino I, inteligencia, lo que no está aún adquirido.

La Unión Europea, en la Ley (Reglamento) de IA[34] finalmente aprobada a principios de 2024, va más allá. Será posiblemente la regulación más avanzada de la IA en cuanto a garantías, aunque la china no carece de interés[35]. En cuanto al ámbito judicial, un dominio que señala como de "alto riesgo", la norma europea exige el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia. Ha introducido un mecanismo específico para asegurar que los derechos fundamentales estén suficientemente protegidos frente a cualquier posible uso indebido de los sistemas de IA.

¿Pero servirá la regulación? Probablemente, en el mundo, la actividad jurídica, especialmente la de los abogados, sea de las más auto-reguladas. Ahora, se están introduciendo estas nuevas regulaciones generales. No es seguro que funcionen si la tecnología avanza mucho más deprisa que ellas. La tecnología puede, suele, avanzar más rápidamente que la regulación, y "contenerla", como propone Suleyman[36], puede no resultar ni efectivo ni incluso viable.

---

[33] Citado por Foley, S. (2023). "AI in law, consulting and professional services", *Financial Times*, 20/7/23. https://bit.ly/3TkdhVX

[34] Reglamento de Inteligencia Artificial: el Consejo y el Parlamento alcanzan un acuerdo sobre las primeras normas del mundo en materia de inteligencia artificial - Consilium (europa.eu), 09.12.2023. https://bit.ly/3v5Cvy1

[35] Sheehan, M. (2024). *Tracing the Roots of China's AI Regulations*, Carnegie Endowment for International Peace. https://bit.ly/49RloPi

[36] *Op. cit.*

En cuanto a lo policial, teniendo en cuenta las particularidades de las autoridades policiales y la necesidad de preservar su capacidad para utilizar la IA en sus labores esenciales, la nueva regulación europea señala, por ejemplo, que todo uso de un sistema de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley debe estar autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro. Prohíbe algunos casos de vigilancia policial predictiva de personas, pero no de manera general.

¿Es el factor humano una garantía? La IA puede reducir los valores de humanidad en el sistema judicial. También el espacio de interpretación en la comprensión del significado contextual de una determinada disposición normativa, por lo que el texto legal se volverá muy rígido en su aplicación. Esta es una visión no ya Occidental, sino que viene de Oriente[37]. Además, si la IA fuera perfecta –que no será pues en materia de Justicia no es ni será una ciencia exacta–, no serían necesarios ni jueces, ni fiscales, ni abogados. Bastarían, si acaso, algunos ingenieros para supervisar la IA.

Los algoritmos predictivos, al resumir la información relevante mejor y más eficientemente que el cerebro de un humano y avanzar conclusiones pueden, además de ahorrar tiempo, contribuir a racionalizar la toma de decisiones de los diversos actores judiciales. Como se ha apuntado, en algunos procedimientos penales en Estados Unidos se aplican estos algoritmos predictivos para calcular ante una demanda de libertad condicional, el riesgo de reincidencia, es decir la probabilidad –estamos siempre en probabilidades o posibilidades, no en cálculos exactos– de que el acusado o reo cometa otro delito. Es una ayuda al juez. Aunque se han dado casos en que esta IA, debido a los datos con que se había entrenado, estaba sesgada en caso de los negros. Pero en el caso de Estado v. Loomis, el Tribunal Suprema de Wisconsin sostuvo que el uso en un juicio judicial de un algoritmo para la evaluación del riesgo de reincidencia no violó los derechos del acusado a un juicio justo. Sorprendentemente, ni el tribunal ni los acusados eran realmente conscientes de la estructura del algoritmo[38]. En todo

---

[37] Shidarta y Munir, A. B. (2020). "Can artificial intelligence technology replace judges in Deciding legal matters?" *HamdardIslamicus*, Vol. 43, núm. S-1 617-630. https://bit.ly/49A84PK

[38] Ovi, C. *Op. cit*.

caso, como ya hemos apuntado, la IA se puede equivocar tanto como un juez o un jurado.

El famoso Reglamento General de Protección de Datos de la UE[39], de 2016, señala que "a fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial". Y (art. 22) añade que "todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar." Claro, una clave está en el "únicamente".

Se va abriendo paso, con fuerza y autoridad, la idea de que la IA, o la automatización, tiene que tener límites en el terreno judicial, y de que la decisión final corresponde a un juez/jurado humanos. En un proceso, la IA tiene, o tendrá a medida que se desarrolle, varias ventajas: todos los antecedentes, toda la información general. Puede redactar resúmenes e informes cortos del sumario, para el juez, para los jurados, el fiscal o los abogados, es decir, para todos los operadores judiciales. Pero al final es necesaria la deliberación humana, aunque la influencia de la IA, con sus resúmenes e incluso recomendaciones, será central. Podrá haber Justicia con robots, jueces con robots, pero difícilmente robots jueces. Lo que seguirá siendo necesario, como garantía jurídica, será el juicio oral, con un juez (o varios), apoyados por IA. Aunque para cuestiones menores, como las que se están experimentando con IA, se abran nuevos caminos. Dicho esto, como se ha apuntado, la intervención de la IA puede generar nueva jurisprudencia.

Las posibilidades que brinda la IA, siempre mejorándose, la están convertido en indispensable, incluso para la búsqueda de ese criterio normativo y objetivo que tenía que acompañar las decisiones judiciales. Ahora bien, aunque detrás esté la IA, el que los acusados humanos tengan derecho a ser juzgados por humanos, por jueces y en algunos casos un jurado, se va a imponer en todos los Estados de Derecho, y en tribunales internacionales. El derecho a que los humanos tengan que ser juzgados por humanos, por un juez y en su caso jurados, se impondrá como exigencia general, como un nuevo derecho humano. Significará

[39] https://bit.ly/3P6X0kH

la entronización de la deliberación humana. Lo que obliga a que los programas de IA interaccionen siempre con el juez, los jurados, los testigos y los acusados. No que les sustituyan. E interaccionen con ellos por separado, pues será una garantía de proceso justo. No puede ser que todo recaiga en una única IA.

La psicóloga Mandeep Dhami señala de los delincuentes con los que ha trabajado que incluso si el juez humano puede cometer más errores, siguen prefiriendo un humano a un algoritmo. "Quieren ese toque humano"[40]. No sólo es una cuestión psicológica o de trato. También de la ya cuestión del recurso a una sentencia dictada por IA. Hay que prever cómo cabrían recursos contra veredictos y sentencias dictadas por una IA, y quién los resolvería: ¿Otra IA, la misma, o un juez humano? A pesar de las mayores posibilidades de errores, la preferencia por el juez humano puede deberse también a que se facilitarán los recursos. Quizás también por ese diálogo tan platónico entre el abogado y el cliente, o entre el juez y el acusado.

El juez humano, o las partes, desde luego la defensa, pero también la acusación, deben garantizarse la posibilidad de acceder a cómo la máquina ha llegado a su conclusión, para poder recurrir. Lo prevé la CEPEJ, y también el reglamento sobre IA de la Unión Europea. Hay un problema. A saber, si se usa la IA es por la capacidad de los programas de examinar una serie inmensa de datos, incluidos precedentes, y de procesar todo ello para llegar a unas conclusiones, un proceso que supera con mucho las capacidades humanas. Lo que, por definición, hace que los humanos difícilmente puedan controlarlo, incluso conocerlo, aunque fuera a posteriori.

4. TRANSPARENCIA Y EXPLICABILIDAD

"Lo que importa es el resultado, no el proceso" mantiene el jurista Eugene Volokh, que se ha volcado sobre esta cuestión del robot juez[41]. Parte de la idea de que los jueces deben limitarse a aplicar la ley más que interpretarla generando Derecho en el camino. Deben ser "*la bouche de la loi*"[42]. Responde a la tradición cultural de la Revolución Francesa, que no es compartida por muchos sistemas

---

[40] Citado por Tassioulas, J. *Op. cit.*

[41] Volokh, E. (2019). "Chief justice robots", Duke Law Journal, Vol. 68:1135. https://bit.ly/3ToRc92v

[42] Ovi, C. et al. *Op. cit.*

jurídicos, para empezar, el de Estados Unidos. Volokh se pronuncia a favor, en principio, de sistemas de IA que remplacen a los jueces, a condición de que estos sistemas puedan superar una versión jurídica del Test de Turing, persuadiendo a un grupo de abogados expertos de que su juicio legal es al menos tan correcto como el de un juez humano. Claro que Volokh ha estudiado la cuestión antes de la llegada de la IA Generativa, que trabaja en lenguaje natural, como el ChatGPT de OpenIA u otros, que han hecho que, como poco, se requiera una profunda actualización de esa prueba que busca a demostrar si un humano está comunicándose con otro humano o con una máquina.

Más razonable resulta John Tassioulas[43], director del Oxford University's Institute for Ethics in AI, cuando señala que hay que prestar más atención al proceso por el cual se llega a decisiones judiciales. Tasioulas se sirve de Platón, en *Las Leyes*, cuando describe la diferencia cualitativa entre lo que llama un "médico libre", es decir, formado y capaz de explicar el tratamiento a su paciente, y un "médico esclavo", que no puede explicar lo que hace y trabaja por ensayo y error. Aunque ambos son médicos, el método del médico libre, un proceso que se suele llamar "pensar", "razonar" o "inteligencia, explica Tasioulas, es superior, según el filósofo griego, porque es capaz de hacer cooperar al paciente, que no es sólo un sujeto, sino también un participante activo.

El debate en curso es una derivada, ahora con la IA, de la vieja disputa sobre la importancia relativa del *input* y del *output*. Richard Susskind[44] defiende la importancia del "pensamiento de resultados", que "nos insta a centrarnos no en cómo hacen lo que hacen, sino en los resultados y beneficios que aportan". Las máquinas, según esta visión, pueden llegar a decisiones sin replicar la forma en que los jueces piensan y razonan (que no son siempre las mismas), sino con unas capacidades y métodos diferentes, hoy por hoy, derivados de los datos masivos a los que tengan acceso pasado por una capacidad de procesamiento que crece día a día.

Ahora bien, con la IA, con un robot juez robot, un predominio del *input* equivale a renunciar a la explicabilidad del fallo, del proceso. La explicabilidad o transparencia es un principio reclamado por muchas declaraciones o medidas

---

[43] Tasioulas, J. *Op. cit.*

[44] Susskind, R. (2019). *Online Courts and the Future of Justice*, Oxford University Press, cap. 28.

sobre la IA, incluida la Ley de la IA de la UE, de un modo general. Implica que el proceso interno por el cual una IA llega a una conclusión debe ser entendible, si no por todo el mundo, sí al menos por expertos. Ahora, bien, insistimos, esta explicabilidad o transparencia de lo que ocurre dentro de la IA cada vez se vuelve más difícil con la mayor complejidad de los sistemas de aprendizaje profundo (*deep learning*) y las redes neuronales. La IA más avanzada no explica cómo llega a sus conclusiones. Crecientemente los procesos internos de las IAs avanzadas se están convirtiendo en "cajas negras", es decir, que no se sabe lo que pasa en su seno. Pero, pese a los avances en la neurociencia, en buena parte también es una caja negra el cerebro. En este caso, el cerebro de un juez.

En la Justicia, la única manera de superar este obstáculo es conservar la decisión, sobre todo el veredicto y la sentencia, en manos humanas. Una cosa es plantearlo, como derecho o principio, y otra ser capaces de responder a ellos, de aplicarlos. La falta de transparencia algorítmica lleva a "una quiebra indiscutible del derecho de defensa", pues "impedirá que alguien pueda defenderse de una conclusión que no puede conocer en sus fundamentos", como apunta Marchena[45].

La exigencia de explicabilidad implicaría que los juristas, y desde luego, jueces, fiscales y abogados, al menos algunos de ellos, deberán estudiar cómo funciona la IA, sin por ello tener que convertirse en "juristas ingenieros". Tendrá que haber una estrecha colaboración entre algunos ingenieros y algunos juristas a este respecto, para plantear casos y recursos ante decisión tomadas por o con IA. En el caso de los juristas, algo parecido al carné de conducir: para lograr el básico no se requiere saber de mecánica, pero para el de camiones o autobuses, sí. La IA obligará a cambiar las carreras jurídicas y el contenido de las oposiciones a juez, fiscal y otras.

Más allá, o más acá, una cuestión central, que señala Tasioulas, es si la IA futura es capaz de generar de forma fiable decisiones jurídicamente sólidas y deseables, acordes con los valores del Estado de Derecho. De momento, a la luz de los experimentos antes citados, el cumplimiento de este requisito está limitado, pero con el crecimiento exponencial de las capacidades de la IA, podría cumplirse. Incluso que las decisiones incorporen cuestiones de contexto, sin sesgo, y con menos exposición –o mejor capacidad de detectarla– a una

---

[45] *Op. cit.*

desinformación que está yendo in crescendo con la simbiosis entre los avances en la IA (en la actualidad, con la inteligencia artificial generativa) y los cambios constantes en las redes sociales y otros medios de comunicación. El impacto de los *fake news* está creciendo, y puede influir en la actividad judicial, por ejemplo, falseando pruebas o generando ambientes no buscados. La IA lo facilita, pero hace más fácil también detectar estos nuevos fraudes. Está en juego la autonomía de la racionalidad humana.

La creciente dependencia de la Justicia en la IA puede tener otras consecuencias indeseables, como que los agentes humanos de la Justicia se acostumbren, entre otras razones por el "factor pereza" y pierdan capacidades propias autónomas. La deliberación entre humanos puede ayudar a mantenerlas. A la larga, como se ha señalado, la Justicia por IA puede generar decisiones o soluciones que a unos humanos no se les ocurran, con mayor capacidad de objetividad, y de distanciamiento de las emociones o valores –y entorno cultural– del juez, aunque la IA seguirá pautas.

Se plantea también la cuestión cultural o civilizatoria. Como señala Richard E. Nisbett[46], "en los países occidentales, los conflictos entre individuos se resuelven en gran medida mediante enfrentamientos legales, mientras que en Oriente es mucho más probable que se resuelvan a través de intermediarios". En Occidente, se suele suponer que en esta clase de resolución de conflictos que es la Justicia, habrá un ganador y un perdedor. En Oriente se persigue la reducción de la hostilidad y se busca el compromiso. En Occidente la Justicia suele representarse con una mujer con los ojos vendados sosteniendo una balanza en una mano y una espada en la otra. La balanza representa la equidad, y los ojos vendados, la imparcialidad y la objetividad. En China, y entre los asiáticos, la Justicia toma la forma de una figura masculina, llamada Yu Di, sentada en un trono, sosteniendo una vara de bambú en una mano y un martillo en la otra, como poder supremo que debe ser respetado y obedecido. En la Unión, la Justicia se asocia a menudo con la feminidad, la compasión y la empatía. En China, la justicia con la masculinidad, la autoridad y la fuerza. ¿Sería un juez robot chino distinto de uno alemán o estadounidense? Está por ver en qué medida la IA incorpora diferencias culturales, y cómo la IA puede acercar, o separar, estas culturas. La IA puede ser

---

[46] Nisbett, R. E. (2024). *The Geography of Thought: How Asians and Westerners Think Differently - and Why*, Free Press.

entrenada con culturas de base distintas, digamos por ejemplo Aristóteles frente a Confucio, y producir resultados diferentes según el entorno cultural. O la IA puede acercar estas culturas judiciales y resultar en algo más universal, especialmente si se muestra necesaria una mayor colaboración judicial mundial o global. ¿Un juez aristotélico frente a un robot confuciano/taoísta?

Esta ampliación conceptual puede ir acompañada, de la mano de la IA, de una reducción del espacio de interpretación contextual de una norma, por lo que algunos consideran que el texto jurídico se volverá muy rígido en su aplicación[47].

Hay una figura que, por su carácter político, sin duda exigiría la decisión humana, por mucho que se apoyara en una IA, a saber, el perdón, ya sea bajo la forma de indulto u otras. Aunque, por volver a Turing, probablemente la decisión de una IA hubiera resultado menos fría que el Perdón Real otorgado por la reina Isabel II de Inglaterra al descifrador de códigos (de la máquina alemana Enigma) durante la Segunda Guerra Mundial y pionero de la informática y de la IA, por su condena en 1952 a castración química por homosexualidad –formalmente por "grave indecencia" (gross indecency) por el código penal de 1885– que le llevó al suicidio poco más de dos años después. El texto de la decisión no puede ser más escueto. Ni siquiera borra el delito por el que se le condenó[48]. Además, ese perdón póstumo llegó sólo en 2013, casi 60 años después de la muerte del genio. Justicia humana inhumana. El Parlamento tuvo que aprobar en 2017 la Ley de Policía y Crimen conocida como "Ley Alan Turing", de amnistía para los hombres que fueron amonestados o condenados en virtud de la legislación histórica que ilegalizaba los actos homosexuales. Así se pudo aplicar el Perdón Real. Una IA hubiera escrito un texto menos frío. ¿Sabrá la Tecnojusticia perdonar? Además de contribuir a cambiar la Ley de acuerdo con los cambios en la sociedad o adelantándose a ellos.

5. NEUROCIENCIA, LIBRE ALBEDRÍO Y RESPONSABILIDAD

La IA no es el único campo tecnológico que está entrando en el mundo del Derecho y de la Justicia. Están también los avances en Neurociencia, que a su vez se apoyan sobre el desarrollo de la IA. Se ha tratado en un anterior capítulo.

---

[47] Shidarta y Munir, *op. cit.*

[48] El texto está disponible en: https://bit.ly/49yWsMX

Queremos aquí apuntar que un primer problema que se presenta, de nuevo, es el libre albedrío (*free will*, en inglés), que algunos avances en la neurociencia están poniendo en cuestión. No es algo nuevo, pero la ciencia actual se acerca más a consideraciones sobre su inexistencia: unos instantes, microsegundos, antes de actuar, de ser conscientes de ir a hacer algo, el cerebro ya ha determinado lo que uno va a hacer. No entraremos aquí en el detalle, sino en las consecuencias y tratamiento, tanto para los humanos como para las máquinas, los robots y programas.

Como indican diversos estudiosos, sin libre albedrío no habría responsabilidad del sujeto. Sam Harris[49] señala que, si los científicos declararan la inexistencia del libre albedrío, podría generarse una guerra cultural de amplitud difícil de calibrar, en todo caso superior a la que generó, y sigue generando, la Teoría de la Evolución. Siguiendo esta línea, la libertad de hacer lo que uno piensa hacer, y no actuar de otro modo, sigue siendo básica para la libertad política y social. Ahora bien, cómo se forma esa voluntad sigue siendo algo que la ciencia aún no puede responder. En buena parte, un misterio.

Sea como sea, y antes de la explosión de la Neurociencia, en 1978 el Tribunal Supremo de EE. UU. (United States vs Grayson)[50], ante el intento del acusado de apuntar en esa dirección, de negar que actuar siguiendo su *free will*, calificó el libre albedrío de fundamento "universal y persistente" de su sistema jurídico, distinto de "una visión determinista de la conducta humana que es incompatible con los preceptos subyacentes de nuestro sistema de justicia penal".

¿Está el juez sometido al libre albedrío? La demanda de imparcialidad, de interpretación razonable de la Ley y la coherencia con el hecho que está juzgando, llevarían a concluir que no. O al menos sería un libre albedrío dentro de unos límites. A lo que una máquina podría aproximarse. Pero la realidad, al menos aparente, es otra.

Lo que lleva a otro tipo de consideraciones. ¿Tienen, o pueden llegar a tener, los robots (máquinas y programas) libre albedrío? La respuesta, a estas alturas y en el horizonte previsible es claramente negativa. ¿Exime esto de la

---

[49] Harris, S. (2012). *Free Will*, Free Press, y Robert M. Sapolsky (2023). *Determined: A Science of Life without Free Will.*

[50] United States v. Grayson: 438 U.S. 41 (1978). Justia US Supreme Court Center. https://bit.ly/3P57Ho4

responsabilidad de los robots en caso de que provoquen disrupciones, funcionamiento erróneo o consecuencias negativas o mal? Lo que se puede aplicar al Derecho penal común o al derecho de guerra y otros.

Además, de la más intensa participación de las propias máquinas en nuestras vidas se derivará algún tipo de responsabilidad de estas. ¿Llegaremos a juzgar a robots, o la influencia de los robots en los comportamientos de los seres humanos? Es decir, que la cuestión no es solo la del tecnojuez, o robot juez, sino la del tecnoacusado o robot acusado. Es lo que cada vez más frecuentemente se llama el "Derecho de los Robots", terreno en el que ha entrado hasta el Parlamento Europeo en 2017[51], al plantear que a largo plazo se estudiara otorgar una "personalidad jurídica específica" para los robots avanzados para facilitar la determinación de responsabilidades en caso de causar daños. Quizás a largo plazo se planteen incluso unos derechos de los robots, si llegan a ser sentientes[52], no digamos ya conscientes, como se van ampliando los derechos de los animales, partiendo de los mamíferos, y avanzado hacia los invertebrados. De hecho, el propio Turing, que reflexionó sobre estos temas antes de que las propias máquinas de IA llegasen a existir o se llamasen así, el concebir máquinas que aprenden, más que realizar tareas concretas con ellas, debería llevar a modificar nuestras relaciones con estos ingenios, con mayor equidad hacia ellos[53].

Ahora bien, como apunta Sylwia Wojtczak[54], para adentrarse en estos terrenos hay que deshacerse del mito de que los criterios de subjetividad jurídica son la consciencia (o sean sentientes *sentience*) y la razón, siguiendo una "única jerarquía o secuencia de entidades, organizadas según su grado de similitud con los seres humanos", o que el lugar de una entidad en esta jerarquía determina el alcance de la subjetividad que se le atribuye. Más bien, argumenta Wojtczak, es la participación o presencia en la vida social, cualquiera que sea el papel, el verdadero criterio de subjetividad. Las máquinas, los robots, van a participar crecientemente, de hecho, ya lo hacen, en la vida social. A pesar de los peligros

---

[51] Robots e inteligencia artificial: el PE pide normas europeas | Noticias | Parlamento Europeo (europa.eu), 16.02.2017. https://bit.ly/3V1MH5q

[52] Término que Xavier Zubiri prefería a "sintiente". Zubiri, X. (2004). *Inteligencia Sentiente*, Tecnos.

[53] Boyer, E. (2023). *Turing*, Les Pérégrines, Paris, pp. 78 y 79.

[54] Wojtczak, S. (2022). "Endowing Artificial Intelligence with legal subjectivity". *AI & Soc 37*, 205-213. https://bit.ly/48Djnp4

potenciales que supone dotar a la IA de algún tipo de subjetividad, parece ineludible llegar a ello, más pronto que tarde.

Sin llegar tan lejos, ¿se puede penar o castigar a un robot? O incluso, con mayores avances, ¿podría un día un robot juez castigar a un robot persona? ¿Con un juicio entre IAs? ¿Máquina contra máquina? En todo caso, hoy por hoy, y mañana, los robots carecen de voluntad libre o consciencia sobre sus acciones. Es decir, carecen de responsabilidad moral[55] como señala Antonio Diéguez. Pero sus acciones tienen consecuencias legales. Aunque nos pueda parecer una ilusión de que son responsables, ¿quién es verdaderamente el responsable de ellas? ¿Los fabricantes, incluidos los diseñadores de sus programas, el propietario de ellos, como en el caso de los animales, o alguna otra posibilidad? Diéguez plantea, sin resolverla, la cuestión del "prejuicio antropocéntrico" si la IA demuestra que, como ya hemos apuntado, puede ser inteligente de forma muy distinta al modo en que lo son las personas (o algunos animales). Podría llegarse a "una forma distinta de ser agente moral, y por tanto susceptible de responsabilidad". Con el crecimiento en número y sofisticación de los robots, serán problemas que, cada vez más, tendrán que plantearse los juristas, que habrán de adquirir conocimientos sobre el funcionamiento de estas máquinas. Habrá que desarrollar una neurociencia específica para las máquinas. Desde luego cuando se trate de juzgar el comportamiento de máquinas autónomas, es decir que funcionan por sí mismas, no bajo control de un humano, incluyendo armas autónomas, a menudo llamadas "robots asesinos".

Quedémonos en la Neurociencia y la Neurotecnología para los humanos. Unos humanos que se van a integrar con las máquinas, o las máquinas en ellos, ya sea con métodos invasivos, como implantes (ya se están anunciado, Elon Musk lo ha hecho desde su empresa Neurolink aunque ha sido bastante discutido)[56], mini y microrobotsrobots, o *neurodust*, inyectados en el cuerpo, o externos, con interfaces cerebro-máquina. De hecho, ya lo estamos haciendo casi en cierta forma con, por ejemplo, los teléfonos móviles llamados inteligentes. "La neurotecnología impactará con aplicaciones que ni pensamos", y no solo en el campo

---

[55] Diéguez, A. (2023). "¿Pueden ser responsables las máquinas?", *Letras Libres*, 1 de julio. https://bit.ly/49BRjUg

[56] Ver por ejemplo, "Elon Musk's Neuralink brain chip: what scientists think of first human trial", *Nature*, 02.02.2024. https://bit.ly/4bS09yC

de la salud, indica el científico y tecnólogo José Carmena[57]. ¿Qué consecuencias tendrá esto si las máquinas cambian a las personas, así "aumentadas", o simplemente influyen sobre ellas de una u otra forma, en la manera de pensar, de decidir de los humanos, incluidos los jueces? ¿Llevará la neurociencia, como apuntan Carmena y otros, a generar modelos matemáticos, réplicas digitales, de una persona, basados en datos que pueden predecir, o explicar, mucho acerca de su comportamiento o sus decisiones? Estas posibilidades pueden convertirse en un instrumento para la Justicia predictiva, para el juez, tecnojuez también en el terreno de la Neurociencia.

En un informe publicado por la Law Society en Reino Unido[58], la institución aborda los retos y oportunidades que ofrece la neurociencia a los profesionales del sector jurídico. Destaca la posibilidad de mejorar sus capacidades a través de implantes digitales, redecillas, o cascos o simplemente Internet. La Neurotecnología, concluye, repercutirá en el Derecho y creará retos y oportunidades. Influirá en la forma de trabajar de los jueces, abogados y otros y su rendimiento cognitivo. Por no hablar de la elaboración de leyes. ¿Personas aumentadas, jueces aumentados, fiscales aumentados, abogados aumentados, y hasta legisladores aumentados? Pues la IA también influirá en la elaboración de leyes y otros textos jurídicos, ayudando o remplazando la labor de diversas figuras políticas o funcionariales.

¿Y la defensa de los derechos del acusado? La neurociencia puede facilitar el acceso a nuestras mentes, no solo por parte de empresas y gobiernos, sino también del sistema policial y judicial. La neurotecnología emergente puede ser muy prometedora, pero, como alerta Nita Farahany[59], solo si actualizamos o reforzamos nuestro concepto de libertad y privacidad para maximizar los beneficios y minimizar los riesgos de hacerlo. Quizás sea necesario, si los acompaña un sistema para hacerlos efectivos, proclamar unos "neuroderechos", como está intentando el neurocientífico Rafael Yuste[60], para el cual nuestros "datos cerebrales

---

[57] Entrevista, José Carmena: "La neurotecnología impactará con aplicaciones que ni pensamos, no solo de salud" - Valencia Plaza, 28.01.2024. https://bit.ly/3TivseO

[58] McCay, A. (2022). *Neurotechnology, law and the legal profession*, Law Society, agosto de 2022. https://bit.ly/3SXOh5E

[59] Farahany, N. (2023). *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*, St. Martin's Press.

[60] Declaración de València sobre la incorporación de los Neuroderechos en la Declaración Internacional de Derechos Humanos, 2023. https://bit.ly/430C7xo

pueden ser uno de los pocos baluartes que quedan contra el compromiso total de la privacidad en la vida moderna".

Y de estos y otros avances tecnológicos y nuevas capacidades surgirán nuevos tipos de delitos. Por ejemplo, en la realidad virtual. En todo caso, la realidad virtual es también realidad. Es algo que ven filósofos como David Chalmers[61], pero que también percibieron otros antes de que se hablara de IA, como José Ortega y Gasset[62] en los principios del siglo pasado, pues la realidad virtual puede estar también en un texto o en un cuadro. Ortega y Gasset (1883-1955) no vivió en los tiempos digitales en los que nos encontramos. Pero si manejó la idea de "realidad virtual" (RV) aunque utilizara más el término de "virtualidad". "El más frecuente error de perspectiva consiste en proyectar todo sobre el plano de lo real. Ahora bien: una de las dimensiones del mundo es la virtualidad, e importa sobre manera que aprendamos a caminar por él", escribía en 1917. El enfoque de Ortega, centrado en el concepto de "vivencia" puede ser útil para entender el impacto de la realidad virtual de hoy en día en los humanos, incluidos los jueces. Y en esa actividad humana que es el Derecho también debe aprender a caminar por la virtualidad. En esa realidad virtual, se plantean los mismos problemas judiciales que en la física. ¿Caben jueces-avatares? Como con todos los avatares, tras ellos tiene que haber una persona, con un programa, una IA.

La realidad virtual plantea nuevos tipos de delitos o crímenes, incluido, por ejemplo, el secuestro o asesinato de avatares además de amenazas, robos, acosos y otros, a los que la policía está prestando cada vez más atención[63], en la actualidad y de cara a lo que puede venir con el Metaverso. Interpol, la agencia internacional de la policía, llegó a la conclusión en un reciente informe de que "con su creciente uso y número de participantes, es necesario definir lo que constituye delitos y daños en el Metaverso" y lanzó un programa para formar a agentes en

---

[61] Chalmers, D. J. (2022). Reality+. *Virtual World and the Problems of Philosophy*, Allen Lane.

[62] Ortega y Gasset, J. (2005). "Ensayo de estética a manera de prólogo", 1914, Obras Completas I, 664-680, Taurus, 2004; "Para la cultura del amor", 1917, Obras Completas II, 278, Taurus, 2004; "Ideas sobre la novela", 1925, Obras Completas III, 901, Taurus.

[63] "Attacks in the metaverse are booming. Police are starting to pay attention", *The Washington Post*, 04.02.24 https://bit.ly/49UvSNZ

este nuevo campo. El mundo virtual permite a Interpol ofrecer cursos de formación de inmersión a las fuerzas del orden de todo el mundo[64].

Un ejemplo es el acoso o las violaciones de mujeres, aunque sea a través de avatares. No están aún contempladas de forma general en los diversos ordenamientos jurídicos. Pero pueden tener efectos psicológicos en las víctimas parecidos a los de una violación en el mundo físico. Algunos de estos problemas han migrado a las aplicaciones sociales de realidad virtual, donde los usuarios interactúan entre sí en bares virtuales, conciertos y otros espacios. Según un estudio de 2018[65] el 49% de las mujeres que usaban entonces regularmente la realidad virtual informaron haber experimentado al menos un caso de acoso sexual.

El Metaverso, u otro tipo de realidad virtual, requerirá de un derecho específico, no solo para bienes virtuales sino también para la protección y límites autorizados de las personas virtuales en ese espacio. Más que jueces especiales para el Metaverso, dada la relación entre la realidad física y la realidad virtual, parece recomendable, que los jueces, y en general la Justicia, no establezcan separaciones, sino que su jurisdicción cubra ambos mundos.

6. CONCLUSIONES: EFICIENCIA Y RAPIDEZ. ¿HACIA UN TRANSJUEZ?

En enero de 2023, una empresa tecnológica estadounidense, DoNotPay Inc, anunció el lanzamiento de un "robot abogado" que representaría por primera vez a una persona en un tribunal estadounidense, lo que abrió una polémica entre juristas en el país. La fiscalía se opuso y lo bloqueó. En 2015, el caso de Lola vs Skadden, en el que se introdujeron elementos de automatización por parte de la defensa, contribuyó a aclarar algunas cosas al hacer una sana distinción entre el "ejercicio de la abogacía" y las tareas "que de otro modo serían realizadas por una máquina", que abrió una espita de permisibilidad en el uso de programas informáticos por los abogados[66].

---

[64] Interpol. Nota 20.10.22. "INTERPOL launches first global pólice Metaverse". https://bit.ly/49XJTuk

[65] Pluto VR and The Extended Mind: Survey of Social VR Users, 2018. https://bit.ly/49Apb3X

[66] Osarodion Progress Friday. *Op. cit.*

La práctica del Derecho con IA se está transformando ya con los bancos de datos, con la IA generativa y con la IA aún por venir, aunque, según un análisis en *The Economist*[67], no sustituirá de forma masiva a los abogados, pero quizás sí a sus ayudantes. La Justicia con IA y aún más por IA tiene muchos detractores, si bien cabe poca duda de que la hará más accesible y más rápida, lo que sería un gran avance para un país como España donde la Justicia es demasiado lenta. No digamos ya en países como Brasil o India, donde los casos se acumulan en los juzgados por decenas de millones, generando no ya retrasos sino injusticia. Para Susskind, la ayuda de la IA y otros sistemas tecnológicos puede "reducir esta injusticia manifiesta, en vez de intentar lograr una justicia perfecta metafísica"[68]. Y este plus de rapidez, menor coste, y menos trabajo (también interviene la ayuda contra el factor pereza que puede suponer la IA) vale para la función de todos los actores, desde el fiscal, al juez, pasando, naturalmente, por los abogados. La capacidad de investigación jurídica ha aumentado de forma espectacular, lo que muchos llaman exponencial, con programas de IA especializados. Son numerosos los que pueden revisar documentos jurídicos más rápido y mejor que los abogados, fiscales, jueces y otros. Todos tienen que preparar su caso lo mejor posible, y la IA se está convirtiendo en herramienta indispensable con este fin.

Lo que a su vez plantea problemas de seguridad, de ciberseguridad, ante hackers y ante las nuevas posibilidades que traerá la computación cuántica, también en este campo. La tecnología del Blockchain puede ayudar a garantizar mayor seguridad y privacidad. Además, la IA puede reducir los sesgos de los agentes humanos, especialmente del juez, o de los jurados si se apoyan en ellas, aunque introducir otros. Se puede lograr, en principio, sin reducir el garantismo, pero, como hemos apuntado, conlleva peligros.

Quizás el uso de la IA puede facilitar que la fiscalía no sólo acuse, sino que, como requiere el Código Penal italiano, también busque en su investigación pruebas a favor del sospechoso, y no solo alegaciones para construir su acusación[69].

---

[67] "Generative AI could radically alter the practice of law", *The Economist*, 6 de junio de 2023.
[68] Citado por Kelly, J. (2022). "AI-driven justice may be better than none at all", *Financial Times*, 29.09.22.
[69] Ovi, C., et al. *Op. cit.*

Ahora bien, de una Justicia que use la IA, a una Justicia impartida por la IA, hay un mundo de diferencia. Como hemos apuntado, la Justicia es una construcción intelectual, en la que, como tal, no puede desaparecer las personas. Mucho antes del reciente surgimiento de la actual IA, o de la que se puede entrever para el futuro, pero tomando en cuenta esos horizontes, Richard Susskind consideraba en 1996 que "la función judicial podría limitarse en gran medida o bien a lo que los ordenadores no pueden hacer, o (según una opinión) no deberían hacer". Añadiendo que "los jueces suelen proceder caso por caso; son practicantes del viejo, denostado e indispensable arte de la casuística"[70]. Por volver a Max Weber, la IA siempre será una máquina, sujeta a errores y malfuncionamientos. También los humanos, aunque con la ayuda de la IA pueden reducir este fallo consustancial a su humanidad. Pero es algo ante lo que los usuarios de la IA deben ser conscientes y tener mucha cautela[71].

Sin llegar a tanto, como en todas las profesiones y oficios, los agentes judiciales tendrán que aprender a usarla y a trabajar en equipo con especialistas en varias materias. Hoy el conocimiento más puntero es híbrido, interdisciplinar. El que no sepa hacerlo, no podrá progresar, en todos los campos, incluso en trabajos manuales que la automatización no eliminará. Y a más largo plazo las personas, al menos una parte de ellas, tendrán que incorporarla de alguna forma a sus propios cerebros. Es lo que defienden los transhumanistas, y apuntan algunos ensayos en curso como el mencionado de la empresa Neuralink.

Los agentes humanos que la gestionan pueden aprender de lo que recomienda la IA. Ingenieros y juristas pueden diseñar nuevas "IAs judiciales" que aprendiendo enseñen a los agentes humanos. El propio Turing abrió la posibilidad de "inteligencias compartidas" entre humano y máquina, de "redistribución de las inteligencias", como lo entiende Elsa Boyer[72]. Lo que se aplicaría también al campo jurídico y al judicial. Sería, si funcionase la idea, también una manera de garantizar el factor humano en la Justicia, el juez con robot y no el robot juez. Pasaríamos así de la Tecnojusticia a la "Justicia compartida" entre humanos y máquinas. O, si la mente, el cuerpo, humano llegara a incorporar las nuevas tecnologías, se generarían, más que robot jueces, jueces "mejorados"

---

[70] Susskind, R. (1996). *The Future of law*, Oxford University Press.
[71] Osarodion...
[72] Boyer, E. *Op. cit.*

o transjueces, Transjusticia, en suma. Es un horizonte, quizás no tan lejano, que nos introduciría en una nueva dimensión. Dejémoslo ahí[73].

BIBLIOGRAFÍA

Alfaia Sampaio, E., Seixas, J. J. y Gomes, P. G. (2019). "Artificial intelligence and the judicial ruling", *European Judicial Training Network*.

Bender, E. M. y Gebru, T., et al. (2021). "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?", FACCT Procedings, 1 de marzo. https://dl.acm.org/doi/10.1145/3442188.3445922

Boyer, E. (2023). Turing, *Les Pérégrines*, Paris.

Chalmers, D. J. (2022). *Reality+. Virtual World and the Problems of Philosophy*, Allen Lane.

De la Cuadra Salcedo, T. (2024). "Las convicciones morales de los magistrados y las decisiones de los tribunales", *El País*, 24 de enero de 2024. https://bit.ly/3IjYe8u

Diéguez, A. (2017). *Transhumanismo. La búsqueda tecnológica del mejoramiento humano*, Herder.

— (2023). "¿Pueden ser responsables las máquinas?", *Letras Libres*, 1 de julio. https://bit.ly/49BRjUg

Echeverría, J. y Almendros, L. S. (2020). *Tecnopersonas*, Trea.

Eliot, L. B. (2020). "An Impact Model of AI on the Principles of Justice: Encompassing the Autonomous Levels of AI Legal Reasoning", Team Portugal I. https://bit.ly/3wqulkk

European Commission For The Efficiency Of Justice (CEPEJ) (2018). *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, Consejo de Europa.

Farahany, N. (2023). *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*, St. Martin's Press.

---

[73] Agradezco a José Enrique Serrano los enriquecedores comentarios realizados a anteriores versiones de este capítulo.

Floridi, L. (2014). *The Fourth Revolution: how the infosphere is reshaping human reality*, Oxford University Press.

Gómez Pérez, A. (2023). "Inteligencia artificial y lengua española", discurso de ingreso en la Real Academia Española, 21 de mayo. https://bit.ly/48spb4I

Harris, S. (2012). *Free Will*, Free Press.

Marchena, M. (2022). "Inteligencia artificial y Jurisdicción Penal", Discurso de recepción en la Real Academia de Doctores de España. https://bit.ly/4bjpz8b

McCay, A. (2022). "Neurotechnology, law and the legal profession", *Law Society*, agosto. https://bit.ly/3SXOh5E

Nisbett, R. E. (2004). *The Geography of Thought: How Asians and Westerners Think Differently - and Why*, Free Press.

Ortega, A. (2016). *La imparable marcha de los robots*, Alianza Editorial.

— (2023). "Nuevas Inteligencias", *Telos*, 25 de mayo. https://telos.fundaciontelefonica.com/nuevas-inteligencias/

— (2023). "Artificial, sí; pero ¿inteligencia?", *Telos*, 28 de noviembre. https://bit.ly/3wBReRQ

Osarodion Progress Friday (LL.B, University of Benin) (2023). "Artificial intelligence in the realm of law: a bane or a boon vis-a-vis the legality or otherwise of a robot lawyer", *Research Paper*. https://bit.ly/49aYP88

Porcaro, K. (2023). "Robot Lawyers Are About to Flood the Courts", *Wired*, 27 de junio. https://bit.ly/42YZxDn

Rezaev, A. V. y Tregubova, N. D. (2023). "The Possibility and Necessity of the Human-Centered AI in Legal Theory and Practice". *Journal of Digital Technologies and Law, 1*(2). https://doi.org/10.21202/jdtl.2023.24

Sapolsky, R. M. (2024). *Determined: A Science of Life without Free Will*, Vintage.

Sheehan, M. (2024). *Tracing the Roots of China's AI Regulations*, Carnegie Endowment for International Peace, febrero. https://bit.ly/49RloPi

Shidarta y Munir, A. B. (2020). "Can artificial intelligence technology replace judges in deciding legal matters?" *HamdardIslamicus*, Vol. 43 núm. S-1. https://bit.ly/49A84PK

Suleyman, M. y Bhaskar, M. (2023). *La ola que viene: Tecnología, poder y el gran dilema del siglo XXI*, Debate.

Susskind, R. (2019). *Online Courts and the Future of Justice*, Oxford University Press.

Tasioulas, J. (2024). "The Rule of Algorithm and the Rule of Law", SSNR, *Vienna Lectures on Legal Philosophy*, febrero. https://bit.ly/3P6W9R1

Tonnara, P. y Perrone, F. (2019). "The judge of the future: artificial intelligence and justice", *TEAM ITALY 2 - THEMIS 2019, SEMIFINAL D*. Judicial Ethics and Professional Conduct. https://bit.ly/3wIdKIY

Trinh, T. H., Wu, Y., Le, Q. V. et al. (2024).: "Solving olympiad geometry without human demonstrations". *Nature 625*, 476-482.

Volokh, E. (2019). "Chief justice robots", *Duke Law Journal*, Vol. 68:1135. https://bit.ly/3ToRc92v

Weber, M. (2000). *Economía y sociedad*, trad. de J. Echavarría FCE.

Wojtczak, S. (2022). "Endowing Artificial Intelligence with legal subjectivity". *AI & Soc 37*. https://bit.ly/48Djnp4

Segunda Parte

ESTUDIOS SOBRE ROBÓTICA E INTELIGENCIA ARTIFICIAL

Capítulo 2
DERECHOS FUNDAMENTALES EN LA SOCIEDAD DIGITAL Y DE LA INTELIGENCIA ARTIFICIAL

Tomás de la Quadra-Salcedo Fernández del Castillo
Catedrático Emérito de Derecho Administrativo
Universidad Carlos III de Madrid
https://orcid.org/0000-0001-9420-2698

1. INTRODUCCIÓN

Una primera aclaración es necesaria respecto a que sociedad digital y sociedad de la inteligencia artificial (IA) guardan una íntima relación en la medida en que la IA puede considerarse como la última y más avanzada fase de la sociedad digital; esta última podría conceptuarse, pues, como un género del que la IA sería una especie.

Las diferencias entre las distintas manifestaciones de la sociedad digital, cada una con sus sistemas, aplicaciones y dispositivos digitales aplicados en distintos ámbitos, son enormes. Por debajo de todos ellos está la electrónica y los semiconductores (con sus chips cada vez más pequeños e infinitamente más potentes) y la digitalización de informaciones que ha permitido el procesamiento de datos binarios (unos y ceros) para automatizar tareas diarias de las que no siempre somos conscientes. Una lavadora automática o un lavavajillas ejecuta un programa de lavado que escogemos soportado por una placa base electrónica con instrucciones digitalizada; placas base que –muchos más complejas y capaces y también progresivamente más potentes– también están en las calculadoras o en los ordenadores. Estamos ante antecedentes más o menos remotos de la inteligencia artificial en cuanto dispositivos y aplicaciones basados en la digitalización y en los progresivos avances de una electrónica realizados al amparo de ciencias como la nanotecnología que han llegado a límites insospechados. Es una evolución de la sociedad digital que va desde las aplicaciones más sencillas –siempre a partir de esa digitalización de informaciones y del empleo de

dispositivos electrónicos cada vez más complejos– hasta dar el salto a la inteligencia artificial cuando se permite que el dispositivo (el coche autónomo por ejemplo) sea capaz por sí mismo, ante las diferentes situaciones o eventos de los que recibe información (inputs), de reaccionar físicamente frenando el coche ante un peatón que se cruza o recalcular primero la ruta a seguir antes de cambiar, también físicamente, de dirección (por congestión de tráfico por accidente sobrevenido en la ruta inicialmente prevista).

Son infinitos los ejemplos de aprovechamiento de una digitalización que se soportan en una electrónica con elementos o chips cuya unidad de medida es en nanómetros, pero cuya potencia crece exponencialmente. Las calculadoras son un ejemplo en el aprovechamiento de la digitalización, como también lo son los ordenadores que empleamos o las redes de comunicaciones electrónicas que permiten que las personas nos comuniquemos unas con otras o que distintos aparatos lo hagan entre sí y de forma automática: el internet de las cosas. Otro paso más lo representan los teléfonos inteligentes con funciones polivalentes o la multitud de aparatos y dispositivos de los servicios de radiodiagnóstico (radiografías, tomografías computerizadas, resonancia magnética, etc.) o quirúrgicos (robot "Da Vinci") hospitalarios que no se explican sin digitalización y programas que a partir de todo ello incorporan progresivamente inteligencia artificial. Del mismo modo ocurre con los programas de reconocimiento y tratamiento de la voz, con las impresoras 3D o con los vehículos autónomos capaces de reaccionar ante las infinitas incidencias de tráfico y de adoptar, se dice, decisiones supuestamente éticas –en caso de pérdidas inesperadas o accidentales de control del vehículo (frenos, por ejemplo)– sobre hacía donde dirigir el vehículo para causar el menor dado (¿el niño, el joven o el anciano?).

En fin, el último nivel es el de la Inteligencia artificial generativa capaz de responder cuestiones, proponer soluciones o darlas, incluso, por sí misma, sin que el propio programa haya predeterminado todos los términos de la solución, pues la propia "máquina" (el ordenador) aprende a partir de los datos con los que se la entrena.

Tal vez el programa de un aparato doméstico con sus elementos electrónicos o el dispositivo que en el aeropuerto nos da acceso a su interior a partir de un lector del código QR del billete –podría decirse que "decide" darnos acceso– no pueda considerarse un ejemplo de IA, pero no cabe duda de que

tiene siempre elementos necesarios con los que también cuenta la inteligencia artificial –lo digital y un mínimo de programación–, aunque la IA añada tantas cosas que suponen un salto cualitativo enorme por su capacidad de dar respuesta por sí misma ante cuestiones y problemas no estrictamente preprogramados. De ahí las diferencias de programas y sistemas digitales con la IA propiamente dicha y no digamos con la generativa y los denominados "modelos fundacionales".

La conclusión es, por tanto, que la IA no puede desconectarse de la sociedad digital con la que comparte muchas cosas y está en su base; entre otras cosas como fuente de datos masivos –de *Big Data*– sin los cuales la IA no podría desarrollarse. Hablar de sociedad digital en general es, así, apropiado, pues resulta expresivo de la multitud de ámbitos, sistemas, aparatos y dispositivos presentes en nuestra vida con distintos niveles de autonomía que empleamos para distintos propósitos o finalidades y que son fuente de datos con los cuales operará la IA. La IA es la punta de lanza de la sociedad digital que no desplegaría todas sus potencialidades sin comunicaciones electrónicas, sensores, ordenadores locales, etc. Elementos todos ellos, también la IA, que no funcionarían sin la digitalización misma o la reducción de cosas y acciones a sistemas binarios (1 y 0).

La contraposición entre derechos fundamentales versus sociedad digital y la IA que en sus distintas modalidades está en su centro merece una precisión inicial. La de que debe evitarse toda aproximación "*ludita*" a la sociedad digital semejante a la que a principios del siglo XIX se oponía en Inglaterra a la mecanización en el ámbito textil y en general a los avances tecnológicos de la época. La sociedad digital será fuente de enormes ventajas para la humanidad y no tiene sentido oponerse a su avance, lo que no quita que haya que ser conscientes de las posibilidades de su empleo torcido o dañino para las personas. Pero eso ocurre con todos los avances en la historia: cualquier instrumento creado por el hombre por inocente que sea (unas tijeras, una botella) puede servir para el mal o para matar a alguien. Lo mismo ocurre con objetos de la naturaleza –una piedra o la quijada de Caín– sin que por eso hayamos de prescindir de ellos.

Los riesgos de mal uso de la sociedad digital no tienen que ser muy diferentes de los existentes en la sociedad tradicional (aunque lo sean sus consecuencias) y por tanto nuestra posición no debería ser muy diferente: no se trata de prohibir, ni de impedir, sino de regular. Son dos las características de la sociedad digital: por una parte, su presencia y ubicuidad universal en todas las actividades

y lugares con permanencia de sus registros y, por otra, la tendencia a la concentración global de la tecnología y los servicios que ofrece.

La primera característica determina una universalización y generalización de la dislocación de los espacios tradicionales de relación y actuación de las personas y por eso mismo un trastorno, disrupción y trastrocamiento de las reglas de conducta aplicables en tales espacios. A ese trastrocamiento de las reglas por dislocación de los espacios se dedican los siguientes apartados que lo muestran en distintos ámbitos y sobre distintos derechos y libertades fundamentales comenzando por una breve referencia a ese concepto de dislocación que se contiene en el siguiente apartado 2; para a continuación mostrar en los sucesivos apartados sus efectos sobre distintos derechos provocados en diferentes ámbitos por los distintos usos de los sistemas, programas y aplicaciones de la sociedad digital. Es el caso, entre muchos otros que podrían citarse, de la perenne permanencia y facilidad de acceso a informaciones ciertas de las personas con eventual afección a sus derechos (derecho al olvido) que de ello puede seguirse (apartado 3); o el de las posibilidades que el tratamiento de datos abre para que los algoritmos discriminen en los precios que se ofrecen en los mercados a distancia, *on line* o *e-comerce* (apartado 4); o los problemas que en relación con la herencia suscita la categorización de contenidos digitales como bienes o derechos de la personalidad y su eventual afección a la intimidad o a la protección de sus datos (apartado 5); o sobre los datos de registro de la actividad cerebral y su tratamiento y las consecuencias de su posible empleo para otras finalidades (apartado 6); y para acabar con unas conclusiones sobre cómo se suscitan riesgos que trascienden la dimensión individual de los derechos fundamentales subrayando los que surgen para la democracia y el mercado debidos a la segunda característica (la tendencia a la concentración global de la tecnología y los servicios) y las transformaciones que para el Derecho supone la regulación de la sociedad digital (apartado 7).

2. DISLOCACIÓN DE ESPACIOS DE RELACIÓN Y TRASTROCAMIENTO DE REGLAS DE CONDUCTA

La sociedad digital con todos sus sistemas, instrumentos y dispositivos abre nuevos espacios donde las personas entran en acción y relación unas con otras y en los que quedan registradas sus acciones, deseos y preferencias. Se trata de lugar nuevos, lugares virtuales podríamos decir, con la característica de que en ellos es posible que las relaciones, conversaciones, intercambios, transacciones,

datos de todo ello, etc., se mantengan de forma perenne y con posibilidades de acceso simultáneo o subsiguiente en cualquier momento y desde cualquier lugar por un número indefinido de personas, lo que constituye esos espacios, *loci* o lugares digitales, en disímiles de los lugares en que se producen las relaciones en el mundo tradicional. Tan disímiles que suelen determinar una dislocación, trastrocamiento o transformación de las reglas aplicables en el espacio o mundo tradicional respecto de las aplicables en los nuevos espacios o entornos digitales.

Esas características podrían alterarse, en algunos casos, a voluntad de las personas que intervienen en los espacios digitales o que los organizan; también la accesibilidad universal puede limitarse, como en las redes sociales, en la medida en que desde el inicio se delimiten condiciones de acceso y de relación para los sujetos que accedan a determinados y concretos espacios. Pero lo que los partícipes coloquen suban o digan en ese espacio digital no siempre puede ser modificado o alterado por los demás, aunque pudiera ser objetado o discutido por quienes tengan acceso a dicho espacio o atribuyan al organizador o administrador poderes de eliminación.

Esa inicial accesibilidad universal –que se refiere no solo a los sujetos que pueden acceder en principio, sino también a los lugares desde los que se puede acceder– determina unas características y consecuencias que pueden verse a través de los ejemplos que en los siguientes aparados se irán exponiendo para poner de relieve cómo, en la mayor parte de los casos, se alteran las reglas de conducta que veníamos aplicando en el mundo tradicional. La permanencia en el tiempo de lo que queda registrado en los espacios virtuales tiene también consecuencias importantes como enseguida se verá, pues es como si a las tres dimensiones espaciales se le añadiera una cuarta dimensión temporal que determina la necesidad de cambiar las reglas que aplicamos en el espacio tridimensional en el que habitualmente nos relacionamos con los demás.

3. LA PERMANENCIA DE INFORMACIONES CIERTAS SOBRE LAS PERSONAS: EL DERECHO AL OLVIDO COMO PRIMER EJEMPLO DE RECONSTRUCCIÓN DE LÍMITES Y REGLAS EN ESPACIOS DIGITALES

El derecho al olvido ha encontrado reconocimiento en la jurisprudencia de los tribunales (tribunales españoles en primer lugar en trance de revisar las decisiones de la Agencia de protección de datos y posteriormente del Tribunal de

Justicia de la UE) para acabar teniendo acogida en el reglamento de Protección de Datos[1] y en los artículos 93 y 94 de la Ley Orgánica 3/2018[2].

La sociedad digital ha determinado que noticias ciertas, pero que de alguna forma afecten al nombre o prestigio de una persona, pueden llegar a ser retiradas de los registros digitales y de la indexación de los buscadores a los efectos de que no se perpetúe el deterioro que para el nombre y la imagen de la persona afectada puede suponer el fácil acceso en cualquier momento y desde cualquier lugar al conocimiento de determinadas conductas realizadas en un pasado más o menos distante. Por el contrario, en las publicaciones en soporte papel –especialmente periódicos– una vez distribuidas y en posesión de sus destinatarios no tiene sentido recogerlas de sus lectores uno a uno, ni unos días después, ni unos meses o años después; no tanto por el coste que ello supondría, sino sobre todo por su inutilidad pues, aparte de destruidas por el propio lector o destinadas a otros usos, habrán sido olvidadas. Por otra parte, la rectificación de una información puede tener sentido cuando no se ajuste a la verdad, pero no es lo mismo cuando la información es cierta.

Sin embargo, en el mundo digital la cuarta dimensión temporal –la permanencia o vocación de eternidad (si se permite tal término) de la información digital– y la gran facilidad de acceso y localización da lugar a que informaciones ciertas que no podrían ser objeto de rectificación, ni de acción alguna de responsabilidad en el momento en que se publicaron, puedan producir efectos lesivos posteriormente para las personas aludidas.

Es el caso de la jurisprudencia "Costeja"[3] relativa a la obligación de los buscadores de abstenerse de la indexación nominativa de noticias relativas a una persona determinada, por cierto que hubiera sido el anuncio judicial de subasta de un inmueble para el pago de determinadas deudas. La función de tal anuncio

---

[1] Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[3] Sentencia del Tribunal de Justicia de 13 de mayo de 2014, Asunto C 131/12. Cuestión prejudicial planteada por la Audiencia Nacional en el recurso interpuesto por Google contra decisión de la Agencia Española de protección de Datos (Google Spain, S.L. y Google Inc. c. Agencia Española de Protección de Datos y Mario Costeja González).

era la de permitir una concurrencia de licitadores que garantizase el precio justo de mercado por el bien objeto de subasta, pero pasados unos años y desaparecida ya la función del anuncio de garantizar la concurrencia de ofertas en la subasta, continuar dando acceso a la noticia por el nombre de la persona solo sirve para otra cosa: para perjudicar eventualmente la imagen de la persona titular del bien subastado y sus relaciones comerciales al porder ser vista como persona incumplidora de sus obligaciones.

El reglamento de Protección de Datos[4] ha dado acogida a ese derecho al olvido en el artículo 17 que la Ley Orgánica 3/2018 ha articulado en sus artículos 93 y 94. Pero el que tenga ya solución positiva no impide recordarlo aquí, tanto para exponer sus razones como por poner de manifiesto el cambio que produce el mundo digital en la interpretación de la aplicación y extensión de los derechos fundamentales en ese espacio digital que obliga a buscar soluciones nuevas, como obligó a los tribunales incluso cuando las normas nada habían dicho al respecto. Así ocurrió cuando la Agencia de Protección de Datos primero, en su resolución de 21 de enero de 2010, y la Audiencia Nacional posteriormente, en su sentencia de 29 de diciembre de 2014, tras plantear la cuestión prejudicial correspondiente (resuelta por el Tribunal de Justicia en su sentencia de 13 de mayo de 2014) tuvieron que reconocer, sin norma previa que lo hubiera establecido, un derecho al olvido como prevalente sobre el derecho a la información.

Se trata con ello de poner de manifiesto los problemas que suscita la dislocación de espacios y su influencia en la interpretación y aplicación de los derechos en su mutua articulación. Lo que ocurre es que en el mundo tradicional convencional a nadie se le puede impedir que siga recordando toda su vida la noticia de esa publicación de la subasta de un bien de alguien a quien conoce; pero eso no quita que la mayor parte de las personas que le conocieran o no hayan llegado nunca a enterarse de esa noticia o se hayan olvidado de la misma. Y desde luego el resto de la humanidad en países lejanos o distantes jamás llegarán a tener conciencia de la noticia que afectaba a dicha persona. La flaqueza de la memoria y el tiempo han sido siempre barreras naturales que protegen suficientemente a la persona de forma que no quede marcada eternamente por su

---

[4] Reglamento (UE) 2016/679 de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

conducta o sus errores, aunque ni siquiera se trate de conductas delictivas. Pero esas barreras se rompen en la sociedad digital y ello nos obliga a plantearnos una regulación positiva de un derecho nuevo, que no deja de ser concreción de derechos pre-existentes que el mundo digital exige rediseñar. Es significativo de esa pre-existencia el que, incluso en el ámbito penal, la sociedad hubiera hecho una reflexión conducente a que quien había pagado por sus actos y cumplido la pena pudiese obtener, pasado un tiempo, certificado de antecedentes penales completamente limpio. Se trataba de facilitar la reinserción social de los delincuentes evitando que el recuerdo de lo que habían hecho les apartase definitivamente, cumplida la pena, de una vida social normalizada.

La sociedad digital ha cambiado todo eso con el registro indefinido de las noticias y con la existencia de buscadores que facilitan su accesibilidad. Ante esa realidad surge la necesidad de un pronunciamiento, de una elección; de alguna forma de una decisión ética acerca de en qué medida la vida de una persona puede quedar cambiada y marcada para siempre por su conducta pasada, cuando no cuenta ya en la sociedad digital con la flaqueza de la memoria, el tiempo transcurrido y la distancia que propician de forma natural el olvido. En el caso del derecho al olvido ha sido una construcción jurisprudencial en primer término la que reconoció y declaró tal derecho que ha sido posteriormente consagrado normativamente por el propio reglamento de Protección de Datos.

El ejemplo del derecho al olvido sirve para mostrar cómo la sociedad digital produce un dislocamiento respecto de soportes tradicionales de la noticia en que el paso de los días les privaba de su función informativa propia y hacía muy difícil acceder a la misma por lo que, salvo excepciones, la regla era que lo publicado –cierto y legítimo–, no había por qué destruirlo ni impedir el acceso a su contenido, haciendo improcedente desde el derecho a la información medida alguna limitando el acceso a noticias ciertas, aunque pudieran perjudicar de algún modo a los citados en las mismas. Nunca se pensó en prohibir las hemerotecas que mantienen, todavía hoy, registro general de todas las noticias publicadas en la prensa, pues el soporte papel hace muy difícil la búsqueda por nombres. Con los buscadores y rastreadores electrónicos ("arañas") eso ha terminado.

El surgimiento del soporte digital cambia los términos de la cuestión al mantener permanentemente la noticia y permitir un acceso facilísimo a la misma con buscadores digitales desde cualquier lugar del mundo y en cualquier momento posterior.

En un escenario digital radicalmente distinto del tradicional, que disloca los soportes y su accesibilidad, la regla que venía rigiendo en el escenario tradicional sobre el alcance y sentido del derecho fundamental a la información (dar, buscar y recibir) no sirve ya del mismo modo, por lo que es necesario reconstruirla atendiendo a valores y principios jurídicos, pero también éticos subyacentes al ordenamiento entero que hay que desvelar y descubrir en sus profundidades. Principios jurídicos y éticos a desvelar que tengan en cuenta las consecuencias de los nuevos soportes conforme a los valores y principios permanentes, pero aplicados al nuevo escenario. Los derechos fundamentales al honor, la propia imagen o la intimidad cobran nuevos perfiles en su articulación con el derecho a la información y la legislación limitadora del uso de la informática a que se refiere el artículo 18.4 de la Constitución, expresión en dicho artículo de un nuevo derecho fundamental a la protección de datos como ha puesto de relieve el Tribunal Constitucional[5].

En todo caso los nuevos soportes exigen cambiar las antiguas reglas, aunque los valores presupuestos en ellas para antiguos soportes no cambian propiamente, sino que exigen nuevas formulaciones que solo aparentemente son contradictorias con las anteriores puesto que al final mantienen su esencia, razón de ser y finalidad. Ello no quita que en su reconstrucción pueda percibirse una voluntad ética, aunque no desconectada –arbitraria o caprichosamente– de la ética misma que está detrás del entero ordenamiento y de los valores a que responde. No siempre las condiciones materiales determinan la conciencia[6], sino que a veces, en estadios más avanzados de civilización –y la Declaración universal de Derechos humanos con todas sus dificultades de implementación abrió uno de ellos– la conciencia determina las reglas de uso de los medios materiales.

---

[5] *Vid.* STC 290/2000, de 30 de noviembre de 2000 y STC 292/2000, de 30 de noviembre de 2000 (Fj 5º y 6º).

[6] Cfr. Marx, K. (2008). "Contribución de la Crítica de la Economía Política", Siglo XXI editores, 9ª edición, pp. 4 y 5 del Prólogo: *"El modo de producción de la vida material determina el proceso social, político e intelectual de la vida en general. No es la conciencia de los hombres lo que determina su ser, sino, por el contrario, es su existencia social lo que determina su conciencia".*

4. ALTERACIÓN ASIMÉTRICA DE LA POSICIÓN DE OFERENTES Y DEMANDANTES EN MERCADOS EN LÍNEA: DISCRIMINACIÓN ALGORÍTMICA DE PRECIOS Y PRECIOS DINÁMICOS. EL SÍNDROME ROBIN HOOD EN MERCADOS A DISTANCIA

De la digitalización de nuestras sociedades se esperaban con razón grandes ventajas y entre ellas no era la menor la del acceso a un mercado abierto y global que favoreciera las oportunidades del acceso a un mercado más transparente y competitivo donde el consumidor de bienes y servicios pudiera elegir sin condicionamientos locales o restricciones geográficas y, con ello, favorecer la competencia y la eficiencia en un mercado más global.

Las comunicaciones y libros de la Comisión europea no han dejado de manifestarse en ese sentido[7]. Ello no quiere decir que la implementación de la economía y de un mercado digital no suscite problemas como han puesto de relieve sanciones diversas a las grandes tecnológicas por prácticas diversas contrarias a la competencia a las que la aprobación de la Ley de Mercados digitales trata de poner coto. Esas dificultades son una llamada de atención a la necesidad de regulación de tales mercados como trata de hacer el Reglamento 2022/1925[8] de 14 de septiembre desde la perspectiva sobre todo del derecho de la competencia.

Pero hay otra perspectiva que es la que, al margen de la competencia entre empresas oferentes de precios y servicios semejantes, se da entre el concreto oferente y el comprador. Es una experiencia común cómo, cuando tratamos de

---

[7] Al menos desde la temprana declaración del Consejo de Lisboa en marzo de 2000 ya se indicaba *"8. El paso a una economía digital, basada en el conocimiento, fruto de nuevos bienes y servicios será un poderoso motor para el crecimiento, la competitividad y el empleo. Además, será capaz de mejorar la calidad de vida de los ciudadanos y el medio ambiente. Para aprovechar al máximo esta oportunidad, se invita al Consejo y a la Comisión a que preparen un Plan de Acción global eEurope que se presentará al Consejo Europeo en junio de este año"*. Tras él no han dejado de presentarse comunicaciones y libros blancos sobre lo mismo.

[8] Reglamento (UE) 2022/1925 de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). Al amparo de dicho Reglamento la Comisión a 5 de septiembre de 2023, la Comisión ha designado seis guardianes de acceso Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft por lo que deberán para cumplir la lista completa de obligaciones y prohibiciones ofreciendo más opciones y más libertad a los usuarios finales y a los usuarios profesionales de los servicios de los guardianes de acceso.

comprar *on-line* un billete de avión o reservar un hotel sucede que, tras una primera sesión exploratoria, al segundo o tercer intento los precios van subiendo, todo ello sin perjuicio de avisos del tipo "*solo quedan tres plazas*" o similares que tratan de empujar ("nudging") a comprar cuanto antes.

Estamos ante supuestos de discriminación algorítmica de precios o de "precios dinámicos" o personalizados que se formulan por los ofertantes de bienes y servicios en función de diversos criterios. Unos tienen que ver con el perfil del comprador que pueden extraer de sus datos. Algunos datos son de carácter más o menos objetivo, pero que, con ayuda de inteligencia artificial (IA), pueden ser reveladores de algunas características personales, como sería el caso del lugar desde el que se está realizando la compra (el distrito postal es relevante a esos efectos), el tipo de procesador o de ordenador o dispositivo que se emplea (Mac o Windows, ordenador o teléfono), la hora en que se realiza la compra, etc. Otros datos son de carácter más subjetivo y buscan, con ayuda de IA, perfilar al demandante de bienes y servicios para conocer sus pulsiones compradoras, sus preferencias y limitaciones de gasto a partir de conocimiento datos previos de sus consultas, compras u otro tipo de prácticas o actividades (incluso en redes sociales o visitas a páginas web); no tanto, necesariamente, de sus personales comportamientos, sino más bien de los de la dirección IP (detrás de la cual suele estar la misma persona) desde la que se inicia el concreto proceso de comprar a distancia en la que la IA del vendedor empleará el perfilado de esa dirección IP (y, así, de la persona que está detrás)[9].

---

[9] *Vid.* sobre la discriminación algorítmica en precios Alfaro, Jesús, *"Precios personalizados y discriminación" en Almacén de Derecho;* Rubí, Antonio en "Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores", Revista de Educación y Derecho, núm. 24, abril 2021-septiembre 2021, accesible en https://almacendederecho.org/precios-personalizados-discriminacion; Pastrana Esparraga, María, "Los precios personalizados como práctica anticompetitiva de discriminación mediante el uso de algoritmos" en El sistema jurídico ante la digitalización: estudios de derecho privado / coord. por Jonatan Cruz Ángeles et al. (2021), Tirant lo Blanc; Antón Juárez, Isabel,
"Marketplaces que personalizan precios a través del big data y de los algoritmos: ¿esta práctica es legal en atención al derecho de la competencia europeo?", Cuadernos de Derecho Transnacional (marzo 2021), Vol. 13, núm. 1; Tena Arregui Rodrigo (2019), *¿Son justos los precios personalizados mediante algoritmos? Blog, "Contratos, Economía, Internet y Nuevas Tecnologías";* Santos Botelho, Catarina (2024), en "*The End of the Deception? – Counteracting Algorithmic Discrimination in the Digital Age", The Oxford Handbook on Digital Constitutionalism,* Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4659451 y Melvin Tjon, Akon (2020), *'Personalized Pricing Using Payment Data: Legality and Limits under European Union and Luxembourg Law'*. European Business Law Review 31, núm. 5.

Los datos para ese perfilado a partir de las direcciones IP[10] se consiguen a partir de los que facilitan las grandes plataformas de comunicación o búsqueda (Google, Amazon, Facebook o Meta, Microsoft, etc.) o los propios proveedores de bienes y servicios a partir del empleo que los usuarios realizan de sus dispositivos digitales (o de los datos que estos dispositivos revelan en cuanto a su localización, desplazamientos, gastos, etc.) y que facilitan a intermediarios de datos (brokers) que a su vez –agregados todos– los ofrecen, de nuevo, por un precio a las empresas vendedoras de bienes o servicios.

Las direcciones IP pueden considerarse datos personales en la medida en que, aunque no revelen quien es la persona (física o jurídica) que está detrás de ella (e incluso aunque puedan ser varias las personas que utilizan una misma dirección IP, aunque no sea lo más frecuente) puede llegar a saberse quién es[11]. En todo caso a efectos de las transacciones digitales no es relevante relacionar la dirección IP con la persona concreta que haya detrás con sus nombres y apellidos, aunque al final de la transacción –al comprar un billete de avión o reservar un hotel– pueda desde esa dirección facilitarse el nombre y apellidos para consumar la transacción.

La discriminación algorítmica de precios en función de los datos subjetivos del comprador on-line ha sido objeto de tratamiento en la literatura académica desde la perspectiva económica[12]. En algunos casos con juicios positivos porque permitiría discriminar en función de la capacidad de pago de cada cual, lo

---

[10] La dirección IP o *Internet Protocol es la dirección única que identifica a un dispositivo en Internet.*

[11] Artículo 4.1 del Reglamento 2016/179, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos los define:
"datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

[12] *Vid.* Maggiolino, Mariateresa (2017). *"Personalized Prices in European Competition Law"*, Bocconi Legal Studies Research, en SSRN: https://ssrn.com/abstract=2984840 or http://dx.doi.org/10.2139/ssrn.2984840; Ryan, Calo: *"Digital market manipulation"*, George Washington Law Review 82, 4 (2014); Bar-Gill. Oren: *"Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions"*; Hannak, Aniko et al. (2014), *"Measuring Price Discrimination and Steering on E-commerce Web Sites"*, Proceedings of the 2014 Conference on Internet Measurement Conference 305, 316.

que, según algunos, parecería ofrecer ventajas, pues permitiría vender a precios menores a quienes tengan menor capacidad económica –o menos interés o necesidad– a costa de obtener precios superiores o muy superiores a los de mayor capacidad económica o interés. Esa interpretación del significado y alcance de la discriminación algorítmica de precios resulta bastante discutible y parece presuponer una ingenua visión filantrópica –una visión Robin Hood de quitar a los más ricos para dárselo a los pobres, tarea que parecería encomendarse a vendedores de bienes y servicios movidos por su, por otra parte, legítimo ánimo de lucro–, pues más bien los vendedores tratarán (como es lógico por otra parte) de obtener el máximo beneficio posible para ellos, pero sin que el conjunto de compradores ni la sociedad se beneficien.

En todo caso, lo que se produce es una alteración del funcionamiento tradicional del mercado minorista en el que la gente preguntaba (y sigue preguntando) por el precio de las cosas, dando por supuesto que el precio es el mismo para todos y que todos tienen derecho a la igualdad de trato. Lo que se altera también es la simetría tradicional de posiciones de vendedor y comprador en que ninguno sabía en principio las razones del otro para comprar o vender, ni los gastos o los beneficios respectivos que uno y otro iban a obtener salvo los que voluntariamente desvelasen en el momento de la compra. El comprador podía saber en el mercado tradicional, desde luego, el precio o la calidad de productos iguales o similares de otros vendedores y con ello tomar su decisión; pero también el vendedor podía saber en ese mercado tradicional los precios y calidades a los que sus competidores venden y con ello tomar la decisión de su propio precio. Con todo ello se construían los precios en competencia en el mercado minorista tradicional.

Esa simetría se altera radicalmente –y con ello la formación tradicional de precios en un mercado en competencia– cuando en las compraventas en línea o a distancia una de las partes tiene los perfiles de la compradora con sus hábitos, sus inclinaciones, su capacidad, sus manías o sus dependencias. Y se consuma esa alteración cuando tal conocimiento no se limita a ofrecerle con mayor precisión aquello que busca o a ofrecérselo de forma más atrayente –por las fotos, las explicaciones, las opiniones o comentarios de otros compradores precedentes, etc., dado el perfil del comprador que conoce y aplica automáticamente la IA del vendedor– sino que se erige en criterio para fijar un elemento central de la transacción misma como es el precio, hasta el punto de fijar precios distintos ("*personalizados*") para cada comprador en función de lo que se sabe de él y su perfil.

En ocasiones los precios diferenciados pueden deberse no tanto al perfil que el vendedor tiene del comprador, sino del propio comportamiento de este en el momento de comprar o de relacionarse con la plataforma de compra del vendedor o con la página web del propio vendedor. Una reiteración de visitas a la propia página, por ejemplo, puede revelar una inclinación a comprar o un interés en la compra que puede incentivarse o empujarse con subidas sucesivas de precios que le induzcan a no demorar más la compra. En estos casos es el propio programa de IA el que ha predeterminado la táctica vendedora ante comportamientos de los compradores con la ayuda de IA y de estudios psicológicos y estadísticos, pero sin tener en cuenta un perfilado previo personal de la dirección IP y con ello de la persona que está detrás.

También los precios diferenciados o dinámicos pueden responder a una previa estrategia vendedora que no dependa del conocimiento del perfil del comprador, sino del momento que compra por suponer que si compra un billete de avión o reserva una habitación de hotel en una fecha muy cercana al servicio se podría deber a una urgencia y que, en esas condiciones, es probable que el usuario pague lo que le pidan.

En cualquier caso, la asimetría entre compradores y vendedores en línea o a distancia no puede ser mayor, sin que el comprador sea consciente de que su situación como comprador en línea ha cambiado radicalmente respecto de la tradicional, pero sin que nadie le advierta de ello. La cuestión aquí no es, sin embargo, si las reglas de compraventa puedan ser diferentes en el mercado tradicional y en el mercado digital (en línea u online) por tener alguna justificación tal cambio de reglas –que los precios en el mercado digital sean diferentes según el perfil de los consumidores– a consecuencia de la alteración misma del entorno digital en que se produce la transacción; en absoluto. La cuestión es por qué, en defecto de tal justificación, se está afectando a los derechos de los consumidores, a su derecho a la igualdad, a su derecho a la información, a su derecho a la protección de datos y, finalmente, a su derecho a la libertad.

La cuestión en este caso, en defecto de justificación para diferenciar precios, es la contraria: que el paso del entorno tradicional al entorno digital no legitima una alteración de la posición de las partes compradora y vendedora en lo que hace a los criterios y términos de la determinación de los precios.

La pregunta tiene trascendencia en cuanto el poder económico actual de las tecnológicas –y el encabezamiento que ostentan en las bolsas de valores,

especialmente la de Wall Street– tiene que ver con una economía de datos que se ha convertido en una especie de "oro negro" del siglo XXI. En ese valor de los datos uno de los componentes[13] radica en su utilidad para ese perfilado a efectos de fijación del precio en las relaciones entre compradores y vendedores, especialmente en el mercado minorista, por lo que una regulación que limite esa funcionalidad de los datos en esas relaciones en línea entre compradores y vendedores puede afectar a la valoración de las tecnológicas.

Pero más allá de la trascendencia que una determinada regulación del comercio electrónico (*e-commerce*) o comercio en línea pueda tener en el valor de las tecnológicas, la cuestión en este caso merece una aproximación desde el derecho a la igualdad (art. 14 CE), a la protección de datos (art. 18.4 CE), al derecho a la información (art. 20 CE), la protección de una economía de mercado (art. 38 CE), la protección del consumidor (art. 51 CE) y en último término desde el derecho a la libertad (art. 17.1 de la Constitución) . Derechos fundamentales y principios contenidos todos en el Título I de la Constitución sobre "derechos y deberes fundamentales" aunque en distintos capítulos y secciones.

4.1. Derecho a la igualdad

El derecho a la igualdad del artículo 14 CE queda afectado, en principio, cuando sobre la base del perfilado de cada comprador –y sin que este sea siquiera consciente– se le discrimina en el precio por determinadas características personales, sociales, de capacidad. En concreto parecería incurrir en esa categoría residual del citado art. 14 relativa a "cualquier otra condición o circunstancia personal o social". No solo, por tanto, raza, sexo, religión y las demás razones explicitadas en el art. 14 de nuestra Constitución, sino por "*cualquier otra condición o circunstancia personal o social*". Son los propios vendedores a distancia los que erigen las

[13] Otros valores, al margen de la fijación del precio, radicarán en un mejor estudio de los mercados, en anticipar preferencias y tendencias de compradores y en una mejor publicidad de las ofertas.

"cookies" cedidas en una de esas otras "condiciones o circunstancias" "personales o sociales"[14] al tomarlas como los criterios determinantes del precio[15].

La afirmación de que todos son iguales "ante la Ley" podía dar motivo para que algunos entendiesen que es la Ley misma quien no puede discriminar, pero que nada impide que lo hagan los particulares en sus relaciones entre ellos –relaciones entre particulares– pues la discriminación no la haría la Ley misma, sino las conductas privadas en relaciones de esa naturaleza. Se trata de una vieja cuestión que ha sido objeto de tratamiento y a la que se ha enfrentado el Tribunal Constitucional aceptando en muchos casos la vigencia de los derechos fundamentales en las relaciones entre particulares, aunque haya supuestos en que quepa excluir esa vigencia o matizarla, especialmente en las relaciones con connotaciones *intuitu personae*[16].

No es admisible una interpretación que excluya el derecho a la igualdad sin más en relaciones entre particulares. No cabría permitir, por ejemplo, diferencias salariales por razones de raza, religión o creencias; por eso mismo las que se hacen por razón de sexo tratan de objetivarse muchas veces en falsas razones objetivas. Lo mismo sucedería en la admisión o no en hoteles o restaurantes

---

[14] El "yo soy yo y mi circunstancia" de Ortega y Gasset se reconstruye en el mundo digital (con las *cookies* que dejan rastros de visitas a páginas web, *likes*, *mails*, etc.) que hasta tal punto dicen algo de nosotros (de unas circunstancias que nos explican y definen) que se hace valioso vender nuestros datos y perfilarnos con ellos para determinar un elemento esencial de la oferta en toda compraventa como es el precio, cuya fijación se entrega al automatismo de la IA.

[15] Desde luego, quedaría fuera de toda idea de desigualdad discriminatoria los supuestos en que la desigualdad (aparte de motivos legítimos –niños, jubilados, parados, etc.– susceptibles de políticas positivas incluso promovidas o alentadas por políticas públicas) responda a bienes o prestaciones objetivamente diferentes (clase *business* o butacas más amplias o separadas o con derecho a servicios específicos de comida o bebida en aviones, por ejemplo), incluso aunque la diferencia en precio en más que se pague no se corresponda realmente con la mejora recibida.

[16] *Vid.* Quadra Salcedo Fernández del Castillo, T. (2013). "Derecho público, Derecho privado y derechos fundamentales", *Revista General de Derecho Administrativo 34*; también del mismo "El recurso de amparo y los derechos fundamentales en las relaciones entre particulares", Ed. Civitas, 1981; García Torres, J. y Jiménez Blanco, A. (1986). "Derechos fundamentales y relaciones entre particulares: la Drittwirkung en la jurisprudencia del Tribunal Constitucional", *Cuadernos Civitas*, Madrid; Cruz Villalón, P. (1988). "Derechos fundamentales y Derecho Privado", en Academia Sevillana del Notariado; Beladiez Rojo, M. "La eficacia de los derechos fundamentales entre particulares"; Alegre Ávila, J.M. "Acerca de los derechos subjetivos: derechos fundamentales y eficacia de los derechos en las relaciones entre particulares", en AEPDA disponible en https://www.aepda.es/AEPDAEntrada-3385-Acerca-de-los-derechos-subjetivos-derechos-fundamentales-y-eficacia-de-los-derechos-en-las-relaciones-entre-particulares.aspx

en función de esos mismos criterios. Todo establecimiento o servicio abierto al público en general tiene que respetar el principio de igualdad de ese público general al que se apela.

En esa línea se mueve el artículo 21.1 de la Carta de los derechos fundamentales de la Unión Europea[17] al empezar por prohibir de forma genérica "toda discriminación", si bien particularizando acto seguido –aunque de forma enunciativa y no limitativa– algunas causas de la misma entre las que incluye la "propiedad" o el "patrimonio"[18] como elemento más novedoso. En definitiva, que los motivos de discriminación no están cerrados en la Carta europea, como tampoco lo están en el artículo 14 de la Constitución española.

4.2. Derecho a la protección de datos (art. 18.4 CE) y Derecho a la información (art. 20 CE)

El derecho fundamental a la protección de datos previsto en el artículo 18.4 de la Constitución y desarrollado conforme a la normativa de la UE también obliga a una reconsideración de la práctica de precios algorítmicamente diferenciado desde el momento en que el tratamiento de los datos se somete a una serie de limitaciones. La primera la de ser tratados los datos de manera lícita, leal y transparente en relación con el interesado; datos recogidos con fines determinados, explícitos y legítimos, sin que sean tratados ulteriormente de manera incompatible con dichos fines (art. 5.1 a) y b) del Reglamento 2016/679).

Para considerar la lealtad y transparencia en el tratamiento de datos para fines determinados, explícitos y legítimos hay que recordar cómo se produce y en qué concluye todo. En efecto, al hacer uso de buscadores y acceder a páginas web, se pregunta al usuario si consiente la política de cookies[19] y le permite configurarlas

---

[17] *1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.*

[18] "*Property*" es el término que se emplea en la versión inglesa de la Carta a diferencia del término "patrimonio" de la española y la italiana. La francesa emplea el término "*fortune*" y la alemana "*Vermögens*" (fortuna o bienes).

[19] El consentimiento al uso de los datos de uso aparece al acceder a las páginas web donde ser realizan compras y transacciones y suele ser del siguiente tipo: "*Utilizamos cookies propias y de terceros con fines analíticos, de personalización y de publicidad, para mostrarte ofertas personalizadas*

o rechazarlas. Ese es el momento en que se da el consentimiento para ese tratamiento; consentimiento que es el que legitima el tratamiento para uno o varios fines específicos, aunque puede dudarse de si es un "consentimiento informado" sobre tales fines específicos, singularmente cuando se le dice al eventual comprador por internet que su consentimiento a esa política de *"cookies"* se hace "*para ofrecer a nuestros clientes mejores servicios personalizados*". La realidad es que se pueden estar empleando tales "*cookies*" para aumentar el precio que el tal "*cliente"* va a pagar en relación con el que puedan pagar los demás al conocer su mayor necesidad y predisposición a comprar, sus preferencias, hábitos, manías o capacidad económica. En definitiva, nada parece tener que ver con "*ofrecerle mejores servicios personalizados*".

Tal vez la lealtad y trasparencia exigiría, para poder hablar de un consentimiento informado del cliente, que se le aclarase que esos "*mejores servicios personalizados*" que se le prometen pueden comportar precios superiores a los que se ofrecen a otros clientes por idénticos bienes y servicios; o que, en el momento mismo de la compra del concreto bien o servicio, se la haga saber –antes de clicar el "acepto"– que se le está dando un "mejor servicio personalizado" que consiste en cobrarle más precio que a otros clientes por el mismo bien o servicio.

En algunos casos el consentimiento que se pide no se justifica con el engañoso argumento de ofrecer mejores servicios personalizados, sino a cambio de no pagar un precio por el acceso a la plataforma o página web en que se va a realizar la compraventa. Con tal oferta lo que se pretendería decir y justificar es que no se engaña a nadie por ceder sus datos, ya que estaría claro que se cederían por no tener que pagar nada por el servicio y que se acepta voluntaria y conscientemente esa cesión; cesión que no es a cambio de nada sino a cambio de una ventaja: no tener que pagar nada por el acceso. Sin embargo, la justificación de ese trato sigue sin ser leal

---

sobre productos nuestros y de terceros, tanto en nuestra web como fuera de ella, relacionadas con tus preferencias en base a un perfil elaborado a partir de tus hábitos de navegación. Para más información, lee la política de cookies" con oferta de configurar cookies o rechazarlas. También del tipo "*Al hacer clic en "Sí, acepto", aceptas que utilicemos cookies para mejorar tu experiencia de navegación, personalizar los contenidos, proporcionar funciones de redes sociales y analizar nuestro tráfico. También podemos compartir información con nuestros socios publicitarios, de análisis y de redes sociales para sus propios fines. Puedes gestionar tu configuración de cookies haciendo clic en el botón "Ver configuración de cookies". Para obtener más información sobre cómo tratamos tus datos personales, consulta nuestra Política de cookies o nuestra Política de privacidad*".

o equitativa ("*fairness*") puesto que el cesionario de sus datos no sabe en realidad la trascendencia de lo que cede y sus consecuencias para él mismo[20].

Sería equitativa y leal si se le informase, en el momento de aceptar la cesión de datos, de que esos datos podrían servir, incluso, para ofrecerle los mismos productos a precios más caros que a otros consumidores o para empujarles a comprar (*nudging*) en función del perfilado de sus inclinaciones o tendencias. Asimismo, seria equitativa y leal si en el momento concreto de ir ya a aceptar una compra concreta se le informase a ese comprador de que el precio de esa compra se ha calculado con un precio personalizado que es superior al que se vende a otros en función del perfilado de sus datos.

Claro que es bastante probable que ningún vendedor esté dispuesto a ser tan transparente y leal como para aclararle al comprador hasta ese punto (en el momento mismo de la compra) las consecuencias concretas de su cesión de datos en relación con el precio. Y no parece que el legislador que promueve las transacciones en línea, la economía digital y el *e-commerce* quiera aguar la fiesta.

En cualquier caso, no parece que el tratamiento de datos sea leal y equitativo ni para fines concretos y determinados cuando se le oculta un elemento fundamental de toda transacción comercial como es el precio y que el mismo, tratado algorítmicamente, puede ser superior al general o al mínimo de partida.

Por otra parte, no parece respetarse el artículo 22.1 del Reglamento 2016/679 que prohíbe que los interesados –en este caso los compradores– sean objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

En este caso la "decisión" es la del vendedor: el precio que se le ofrece online y que, como toda oferta, es vinculante y constituye una "decisión" del oferente. Es verdad que puede no aceptarla el comprador y por tanto no le obliga; pero no puede negarse que sí hay una decisión (la del vendedor en línea) basada en la elaboración de perfiles sin intervención humana, ni negarse que produce efectos jurídicos (los que produce para el oferente), aparte que "afecta significativamente

---

[20] Zuiderveen Borgesius Frederik y Poort Joost (2017). "Online Price Discrimination and EU Data Privacy Law" *Consum Policy*, p. 364. Disponible en SSRN: https://ssrn.com/abstract=3009188 or http://dx.doi.org/10.2139/ssrn.3009188

de modo similar" al comprador, puesto que este cree que ese es el precio de mercado –es decir el precio común a que se vende y compran las cosas por todos en el mercado sin perfiles previos– cuando, en realidad, es un precio formado fuera del mercado por un algoritmo. De ahí que esa falsa creencia de que es el precio de mercado le "afecta significativamente" (locución esta del artículo 22.1) para aceptar un precio automatizado a partir del perfilado.

Hay en todo esto un pecado original de Europa, desde la primera Directiva 95/46/CE de 24 de octubre de 1995[21], al ver con condescendencia el empleo de los datos con fines de lo que se llamaba "prospección comercial" (de confuso significado); probablemente pensando que podría servir para incentivar el dinamismo inversor y favorecer el crecimiento de la actividad económica a la vez que la competencia en bienes y servicios en un mercado "en línea" en que los compradores tendrían más oportunidades para comparar ellos mismos los mejores precios y calidades. Las cosas no han ido, siempre, por ese camino. Lo cierto es que por las razones que fueran, incluidas las mejores intenciones de las que se dice que el infierno está empedrado, la Directiva 95/45/CE dejó testimonio de esa condescendencia hacia los Estados miembros respecto del empleo de datos y su cesión con fines de lo que denominaba "prospección comercial" en sus Considerandos 30[22] y 71[23].

El nuevo Reglamento 2016/679 no emplea ya la locución "prospección comercial" –de impreciso significado– en sus considerandos, pero la consagra en su articulado al prever el empleo de datos con fines de lo que denomina "mercadotecnia directa" en su artículo 21.2: "*Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan,*

---

[21] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[22] Considerando 30: *"Los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial".*

[23] Considerando 71: "*La presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a tratamientos de datos personales".*

incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia".

La mercadotecnia directa –definida por la RAE como "*el conjunto de principios y prácticas que buscan el aumento del comercio, especialmente de la demanda*"– recibe así del propio Reglamento como una especie de "patente de corso", reforzada con el calificativo de "directa" que sugiere que la mercadotecnia indirecta no permite siquiera oposición al tratamiento de datos de cada uno. Ese reconocimiento del derecho del afectado a oponerse confirma que tal "mercadotecnia" queda legitimada, aunque con el remedio, consolador para la conciencia de Europa, de que se reconoce el derecho a oponerse.

Nada más hay en el reglamento que permita legitimar claramente el empleo de los datos con fines de discriminación de precios, aunque estas referencias a la prospección y a la mercadotecnia directa nos indica dónde está el origen de un problema que ha acabado cristalizando en la discriminación de precios a la que la UE tal vez no pensó que se llegaría, pero que ante su realidad exigiría alguna reacción por infracción de los principios de lealtad, transparencia y equidad (*fairness)* que inspira la normativa de datos.

Y es en ese contexto en que el derecho a dar y recibir información veraz del artículo 20 de la Constitución cobra relevancia, pero no ya en relación con los medios de comunicación social, sino en relación con cualquiera que se vaya a quedar con datos de los demás con obligación de informar con claridad de los términos en que requiere su consentimiento y con qué fines y alcance. El usuario en los entornos digitales tiene derecho a ser informado con claridad del alcance y significado del consentimiento que se le reclama como exige el artículo 7.2 del Reglamento 2016/679; exigencia que hay que conectar con el derecho a recibir información veraz del artículo 20.1 d) de la Constitución. Veracidad violada cuando se le informa de que sus datos servirán para ofrecerle un mejor servicio, pero se le oculta que ese mejor servicio puede suponer que los precios que se le ofrezcan sean más altos que los de otros compradores a distancia del mismo bien o servicio.

4.3. La garantía de los derechos de consumidores y usuarios (art. 51 CE)

La discriminación de precios no puede ser consentida por el Estado desde los principios del art. 31 de la CE que obligan a los poderes públicos a proteger los intereses económicos de los consumidores y usuarios.

Los poderes públicos tienen así la obligación de verificar si la discriminación algorítmica de precios tiene alguna justificación y si no la tiene, como parece, impedirla.

4.4. La libertad de empresa en el marco de una economía de mercado (art. 38 CE) y los precios algorítmicamente diferenciados

El art. 38 de la Constitución reconoce la libertad de empresa en el marco de una economía de mercado. Tal referencia a la economía de mercado legitima intervenciones de los poderes públicos limitativas de la libertad de empresa, pero no ya en atención a bienes tales como la salud, el medio ambiente, el patrimonio histórico, la propiedad industrial o intelectual, etc., sino en atención a garantizar la existencia misma de un mercado en el que, por existir competencia entre oferentes, se crucen la oferta y la demanda para la formación de precios.

Los precios diferenciados determinados automáticamente por algoritmos a partir de datos personales suponen una alteración de esa economía de mercado. Una alteración que rompe los modos del mercado tradicional para construir otro sobre la base de unas diferencias asimétricas de conocimientos entre oferente y demandante.

En esas condiciones la libertad de empresa no puede ser argumento para permitir los precios diferenciados una vez que estos suponen una ruptura de la tradicional economía de mercado que, como Institución básica de la economía, muta sustancialmente.

4.5. La libertad (art. 17.1 CE) en relación con las prácticas prohibidas de la inteligencia artificial

El nuevo Reglamento de Inteligencia artificial pendiente de publicar ha recogido unas modificaciones muy importantes respecto de la propuesta inicial de la Comisión en relación con lo que denomina "practicas prohibidas". Entre ellas están aquellas que alteren de manera sustancial el comportamiento de una persona, mermando su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado.

Esa descripción de las prácticas prohibidas parece que refleja bastante fielmente la que se produce cuando se le da un precio diferenciado al comprador *on-line* que cree que se le está ofreciendo el mismo precio al que ese concreto

vendedor vende sus bienes y servicios al resto de compradores, ignorando que se le está discriminando con base en un algoritmo que tiene en cuenta sus circunstancias personales para fijar el precio y que no llega ni a sospechar que esa diferenciación esté ocurriendo.

Los términos del artículo 5 del reglamento de Inteligencia Artificial no parece que puedan eludirse fácilmente: "*Quedan prohibidas las siguientes prácticas de IA:*

a) *La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;*

b) *La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra*".

Las referencias del Reglamento a la "alteración del comportamiento de una persona" o "la merma apreciable de su capacidad para tomar una decisión informada" no parece que esté aludiendo a otra cosa que a la alteración de la libertad de una persona para tomar decisiones; a la libertad contenida en el artículo 17.1 de la Constitución. No entendida como la libertad física para entrar o salir físicamente, sino a la libertad moral de tomar decisiones libres con conocimiento de causa. Es verdad que el artículo se refiere a una "merma apreciable de la capacidad de tomar una decisión informada" y que ello ofrece un margen de interpretación. No obstante, el criterio de interpretación consistiría en preguntarse si hay merma apreciable de la capacidad de tomar una decisión informada, cuando la persona hubiera decidido no comprarlo de habérsele informado de que el precio que se le ofrece es superior al que se ofrece a otros por el mismo bien o servicio. La falta de información supondría, así, una merma decisiva en su capacidad.

5. LA HERENCIA DIGITAL DE LAS PERSONAS: BIENES Y DERECHOS DE LA PERSONALIDAD Y EL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS DEL CAUSANTE

La sociedad digital permite un uso de las tecnologías de las redes sociales o de aparatos y dispositivos de todo tipo (teléfonos inteligentes, correos electrónicos, pagos con el teléfono o con tarjetas de crédito, etc.) que dejan un rastro de nuestra vida y de nuestro comportamiento que plantea problemas nuevos en relación con la herencia que no tienen respuesta siempre clara en el Derecho.

Se trata de saber en qué medida el rastro que el usuario deja en redes sociales, en correos electrónicos, en los gastos de compras, viajes, hoteles, contactos, etc., que quedan registradas en nuestros ordenadores o de las redes sociales en las que participa o en la nube deben ser accesibles para los herederos cuando una persona fallece. Se trata de determinar en relación con la herencia cuál es la naturaleza del conjunto de cosas y datos que podría considerarse aparentemente que integran la herencia propiamente dicha; cuestión que con sus propias dificultades puede estar clara en relación con las cosas en escenarios tradicionales o convencionales, pero que se dislocan en escenarios digitales[24]. Lo ocurrido en Alemania puede mostrar lo que se quiere decir. Los padres de una adolescente querían acceder a la cuenta de Facebook de su hija que había muerto en 2012 en un accidente en el metro de Berlín, aunque más que un accidente podía tratarse de un suicidio, pues los padres sospechaban que pudo deberse a un acoso que habría sufrido. Facebook tiene unas condiciones para los usuarios por las que estos aceptan al abrir sus cuentas –condiciones, que nadie lee– que, cuando el usuario muere, Facebook cierra la cuenta y, si acaso, coloca una referencia conmemorativa de la persona titular de la cuenta. Angustiados los padres por la sospecha del acoso que su hija podía haber sufrido querían tener acceso a su cuenta en la plataforma de la red social de Facebook para saber qué había ocurrido y qué podía haberle llevado a esa decisión fatal. Ante la negativa de Facebook acudieron a la justicia

---

[24] *Vid.* Santos Morón, M. J. (2018). "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho transnacional*, Vol. 10, núm 1. También Diaz Alabart, S. (2020). "La protección de los datos y contenidos digitales de las personas fallecidas" Ed. Reus, pp. 11-16; Bodas Daga, Mª. E. (2007), "La defensa "post mortem" de los derechos de la personalidad", Bosch, Barcelona.

que les reconoció en primera instancia en 2015 el derecho a acceder a la cuenta y a su contenido por lo que Facebook quedaba obligada a permitirle tal acceso.

Sin embargo, la plataforma recurrió la sentencia de primera instancia y el Tribunal de apelación la anuló en 2017 denegando el derecho de los padres a ese acceso a la cuenta de su hija. Finalmente, el Tribunal Supremo acabó dando la razón a los padres en Sentencia del de 12 de julio de 2018.

No puede negarse que la decisión del Tribunal Supremo alemán tiene su lógica y su fundamento e incluso antecedentes en lo que hace a los diarios a los que las personas confían sus sentimientos más íntimos sin desear, tal vez, que sus próximos lleguen a conocerlos o leerlos. No obstante la solución del supremo alemán no es sin más exportable a todo el mundo y ha sido objeto de debate en la doctrina internacional, ya que cabe discutir la naturaleza de una cuenta de esas características en un escenario digital.

La Ley Orgánica 3/2018 de protección de datos personales de 5 de diciembre establece esa misma solución para España en su artículo 96 al disponer que no solo los herederos de los fallecidos, sino incluso sus allegados, podrán dirigirse a los prestadores de servicios de la sociedad de la información para acceder a los contenidos gestionados por dichos prestadores con la única salvedad de que el fallecido lo hubiera prohibido expresamente. Con ello se legitima con carácter general el derecho de herederos y allegados a acceder a los contenidos digitales, salvo expresa prohibición.

No es sin embargo ni la única solución posible ni la más ajustada al derecho a la intimidad de la persona fallecida o a los derechos de terceros que aparezcan en esos contenidos digitales. La solución francesa es, por ejemplo, la contraria al disponer el artículo 84 de la Ley sobre la informática, los ficheros y las libertades la extinción al fallecimiento de la persona de los derechos que tenía sobre sus datos (entre ellos el derecho de acceso e información), sin que pasen a sus herederos, salvo en los supuestos previstos en su artículo 85. Artículo que exige, en todo caso, expresa previsión del fallecido, aparte de otras previsiones en protección de terceros[25]. La regla es, por tanto, en Francia la de que salvo expresa

[25] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modificada por la Ordenanza núm. 2019-964 de 18 septiembre 2019 dictada en aplicación de la Loi núm. 2019-222 du 23 marzo de 2019.

previsión en contra del causante los derechos sobre los datos que tenía la persona se extinguen a su muerte ("muerte digital").

No se trata aquí de entrar a discutir la solución dada por el artículo 96 de la Ley Orgánica 3/2018 con el equívoco término de "testamento digital" en lugar de "herencia digital"–pues el problema consiste en determinar los bienes o derechos que pueden ser objeto de herencia y no la forma de expresar la voluntad testamentaria[26]–, sino de poner de relieve la existencia de nuevos problemas que permiten soluciones distintas y mejores de los que en este caso el legislador no ha sido completamente consciente al minusvalorar los problemas que se plantean cuando el fallecido no ha expresado su voluntad al respecto. Ahí radica la cuestión que la ley pasa por alto al limitarse a prever el caso de manifestación expresa de prohibición (haciéndolo, además, de forma incompleta) pero no los supuestos de silencio.

Para empezar, se trata de saber si los contenidos digitales son, sin más, un bien susceptible de herencia o un bien o un derecho de la personalidad que se extingue con la persona o no susceptible de transmisión o en qué condiciones o, en cualquier caso, si se trata de datos personales protegidos y, por tanto, no trasmisibles[27]. El soporte físico de un diario íntimo se ha podido tender a asimilarlo a un bien, pues el soporte se erige en un elemento físicamente visible. Pero en un escenario digital las cosas no son lo mismo y no solo por el elemento físico que lo pueda contener (puede ser el ordenador del fallecido, pero no la nube en la que se guarda), sino porque, en primer lugar, el acceso a la red social exige una cuenta y una clave que lo protege y que obliga a la plataforma a evitar accesos no autorizados. En segundo lugar, no puede olvidarse que, en una cuenta de una red social, igual que puede pasar con los correos electrónicos, puede quedar la vida entera de una persona: sus ideas, pensamientos y sentimientos, así como sus relaciones y contactos más personales. Y no solo de la persona fallecida, sino de los terceros que con ella se relacionan y que se puede suponer que en la mayor parte

---

[26] *Vid.* Cámara Lapuente, S. (2019). "La sucesión mortis causa en el patrimonio digital", El notario del siglo XXI, *revista del Colegio Notarial de Madrid*, núm. 84, quien afirma en p. 411 que el testamento digital no existe.

[27] Tal es la consideración del artículo 63.2 de la Ley francesa para una República digital ("Loi pour une République numérique" núm. 2016-1321 du 7 octubre) que modifica el artículo 40.1 de la Ley núm. 78-17 de 6 de enero de 1978 relativa a la "Informática, los ficheros y las libertades" y relaciona la eliminación de registros digitales de la persona al fallecer con el carácter de datos personales, al margen de regular los casos, condiciones y finalidades en que quepa, pese a ello, su mantenimiento.

de los casos excluían de esa relación a herederos y allegados presentes y futuros; terceros que también tiene su derecho fundamental a la intimidad.

Es posible que el titular de la cuenta en la red social (o de su cuenta de correo electrónico o del uso del teléfono móvil o de los pagos hechos con el mismo) no quisiera que nadie –y tal vez menos sus allegados o herederos– tuvieran acceso a la misma para conocer sus opiniones en las redes, sus preferencias, sus relaciones o sus correos electrónicos, etc.

Todo ello plantea un primer problema sobre si estamos antes bienes propiamente dichos o ante derechos de la personalidad o, sin más, ante datos personales que deben seguir su régimen de protección general[28]. Ante la muerte del titular de la cuenta sin dejar nada dicho al respecto se plantea qué solución debe dar el legislador cuando el fallecido no ha dicho nada sobre ello. La cuestión para el legislador es determinar qué protegemos: el derecho de los demás considerando que el ordenador y la cuenta son bienes que deben seguir el régimen común de los bienes de la herencia o más bien el derecho a la intimidad y privacidad del fallecido y de los terceros que con él se relacionan y que, como su intimidad, desaparecen con la persona[29]. La jurisprudencia hubiera tenido que decir algo cuando se le plantease la cuestión, pero el artículo 96 de la Ley Orgánica 3/2018 ha zanjado la cuestión, salvo dudas de constitucionalidad.

El apartado VII de la Carta de Derechos digitales aprobada el 14 de julio de 2021, aborda el problema consciente de que la Ley actual no acaba de solucionarlo cuando el fallecido no ha dicho nada al respecto o cuando lo que ha dicho está en una cláusula de un contrato de adhesión que no suele ser jamás leído por nadie al darse de alta en una red social. La Carta no pretendía tener valor vinculante, sino señalar principios y orientaciones. En este caso la Carta establece

---

[28] *Vid.* Otero Crespo, M. (2019). "La sucesión en los "bienes digitales". La respuesta plurilegislativa española", *Revista de Derecho Civil*, Vol. VI, núm. 4 (octubre-diciembre). También Ginebra Molins, M. E.: "Morir en la era digital. Voluntades digitales, intimidad y protección de datos personales", en *Derecho Mercantil y Tecnología*, Madrid Parra, A. (dir.), Blanco Sánchez, M. J. (coord.) y Ordelin Font, J. L. y Oro Boff, S. (julio 2020). "Bienes digitales personales y sucesión *mortis causa*:la regulación del testamento digital en el ordenamiento jurídico español", *Revista de Derecho (Valdivia)* Vol. XXXIII, núm. 1, p. 121.

[29] El Reglamento de datos 2016/679 deja fuere según reconoce su considerando 27 los datos de las personas fallecidas cuya regulación se entrega a los Estados. Por su parte el artículo 2.2 b) de la Ley Orgánica 3/2018 excluye de su ámbito de aplicación el tratamiento de datos de las personas fallecidas, salvo lo previsto en su artículo 3º.

que será el legislador quien decida la cuestión, pero indica los problemas que este habrá de resolver y que el art.º 96 de la Ley Orgánica 3/2018 no resuelve[30].

La cuestión, por tanto, consiste en saber cuál es el valor más importante a proteger en relación con soportes digitales que –de forma consciente o inconsciente de su trascendencia futura para herederos y allegados– registran nuestra actividad, pensamientos y sentimientos que tal vez solamente queremos que sean conocidos por determinadas personas; en saber si el valor a proteger es el de la propiedad suponiendo que se trate propiamente de bienes susceptibles de ser heredados o si se trata también de derechos de la personalidad cuyo custodio pudieran ser los herederos en la medida en que se trate de proteger o, si más bien, se trata de defender la intimidad o privacidad y la memoria del fallecido y de los terceros con que se relacionaba. La cuestión radica en determinar en qué medida el fallecido deseaba o no deseaba que los datos y los rastros de sus decisiones, sus preferencias y su vida personal o más íntima fuesen desvelados a los herederos o más bien, por el contrario, hubiera deseado que no lo supieran o que no fueran conocidos por nadie.

Tal es el dilema que debería haber resuelto el legislador. Lo pueden hacer desde luego también los tribunales al hilo de los casos que se les presenten, pero parece necesario un debate público y una reflexión social al respecto que conscientemente acabe llevándose a un texto legal. Los criterios tradicionales sobre el derecho de propiedad y las reglas hereditarias son aplicables sin duda en relación con los bienes materiales del fallecido, pero el problema que se suscita para empezar consiste en saber si los datos registrados en cuentas de redes sociales o cuentas de correo son propiamente bienes y si sus titulares son conscientes de que un día sus herederos van a tener acceso a esas cuentas y a registros que son

---

[30] Apartado VII de la Carta de Derechos Digitales: "VII. *Conforme a la ley que rija la sucesión, se reconoce el derecho a la herencia digital de todos los bienes y derechos de los que, en el entorno digital, fuera titular la persona fallecida.*

- *Corresponde al legislador determinar los bienes y derechos de carácter digital de naturaleza patrimonial transmisibles por herencia y los bienes de la personalidad que pueden ser objeto de defensa, preservación y memoria, así como las personas llamadas, en su caso, a tal función, en defecto de señalamiento por el fallecido.*
- *Se promoverá que la legislación contemple los supuestos en los que, atendidos los derechos de la persona fallecida o de terceros y en particular la protección de su intimidad y del secreto de sus comunicaciones, proceda la extinción del patrimonio digital o su no accesibilidad fuera de las personas a quienes se distribuyeron o se permitió acceder, en los casos en que aquella no haya dejado manifestación expresa sobre su destino".*

expresión de la privacidad del fallecido; registros sobre aspectos reservados que nunca consideró, tal vez, que fueran desvelados a nadie, salvo a aquellos a quienes se dirigieran las comunicaciones en el ámbito restringido en ocasiones de una red social con limitados participantes o no abierta al público en general.

De nuevo, pues, la dislocación se produce en los escenarios digitales respecto de los tradicionales y la necesidad de determinar si las reglas para el mundo convencional o tradicional son aplicables en el mundo digital. Ello aparte de determinar si estamos ante bienes o ante derechos de la personalidad[31]. Las reglas a aplicar en escenarios digitales podrían parecer contradictorias con las aplicadas en el escenario tradicional: en el digital se podría presumir tal vez la existencia de un deber de reserva y respeto a la intimidad mientras no resulte evidente que la voluntad del fallecido fuera la de que sus registros se conocieran por sus herederos. Pero también pudiera ocurrir que, pese a tal presunción, fuese necesario el acceso a estos registros (rastros de la vida íntima y personal manifestada en sus relaciones en redes sociales y en el uso de aparatos y medios electrónicos) ya sea para determinar la voluntad del fallecido a ese respecto o para conocer sus bienes, contratos, obligaciones y responsabilidades que pueden afectar a la determinación de la herencia misma, de sus obligaciones o sus derechos antes del fallecimiento.

Es un ejemplo de cómo la sociedad digital rompe las categorías en los escenarios nuevos que ella misma abre en los que se suscitan nuevos retos y problemas que obligan al legislador a ponderar valores y principios, incluso con apelaciones a la ética que subyace en el sistema jurídico para optar por aquello que le parezca más adecuado al conjunto del ordenamiento y al orden de valores y principios que expresa.

6. NEURO-TECNOLOGÍAS Y DERECHOS Y LIBERTADES FUNDAMENTALES

Las neuro-tecnologías que permiten la curación de enfermedades como Alzheimer, depresión, esquizofrenia, Parkinson, etc., suscitan grandes esperanzas, pero comportan también una serie de riesgos que preocupan especialmente a los científicos que están investigando en estos campos.

El interfaz cerebro ordenador es un dispositivo relevante que permite, a través de sensores colocados cerca del cerebro (con técnicas no invasivas como

---

[31] Santos Morón, M. J. "La denominada...". *Ob. cit*., párrafos 11, 12, 18, 19 y 20.

diademas, gorros, boinas, etc.) o en su interior (con técnicas invasivas de colocación de chips o diminutas placas metálicas) registrar la actividad eléctrica cerebral, enviándola a un ordenador que, con IA, la descifra para, en un último paso, inducir o provocar estímulos que desde fuera corrijan y curen las enfermedades, objetivo primero de estas investigaciones.

Pero no puede desconocerse que su empleo puede entrañar diversos riesgos; unos derivados del propio proceso de curación de las enfermedades y la prudencia con que deban acometerse, lo que corresponde a las ciencias médicas y a la ética y deontología profesional. Otros relacionados con el mal uso que pudiera hacerse de esos registros y de las técnicas de inducción o provocación de estímulos por abuso del encargado del tratamiento o por intromisión o robo (hackeo) por un tercero para fines distintos y ajenos a la curación.

Al margen de esos riegos de uso fraudulento de registros de la actividad cerebral y del empleo del interfaz por terceros, preocupan también a los investigadores riesgos como la pérdida de la conciencia, que a veces se produce en personas sometidas a distintos tratamientos médicos como es el caso del electroshock o la alteración de la personalidad que pueda derivarse de la mera conexión con la IA de un ordenador y las secuelas de dependencia o confusión que ello puede producir, aún sin que nadie persiga maliciosamente tales efectos[32].

Todo ello sin ignorar las eventuales y conscientes manipulaciones de la voluntad o la alteración de la personalidad de los sometidos a dichos tratamientos neurológicos por parte de terceros o con finalidades ajenas a las terapéuticas. Manipulación fraudulenta a partir de los datos registrados de la actividad cerebral de un paciente que pueden llegar a identificar no solamente sus ideas y sensaciones conscientes, sino incluso las subconscientes con ayuda de inteligencia artificial.

No se trata aquí de un perfilado de la persona a partir de datos recopilados de sus preferencias, gustos, inclinaciones, etc., que se obtengan a partir de sus

---

[32] Así lo recoge. Yuste, Rafael, Goering, Sara et al. (2017). "Four ethical priorities for neurotechnologies and AI", *Revista Nature*, 8 noviembre, accesible en https://www.nature.com/news/four-ethical-priorities-for-neurotechnologies-and-ai-1.22960. En página 162 explica cómo personas que han recibido estimulación cerebral profunda a través de electrodos relatan después sensación de pérdida de voluntad e identidad. Al margen de si esa estimulación se produce por razones terapéuticas, el dato debe retenerse, aun notando la distinta consideración que merece que las razones sean terapéuticas u otras diferentes.

hábitos, consultas, actividades y manifestaciones en redes sociales, etc., sino de que los datos de su actividad cerebral lo que hacen es desvelar directamente –y en ese sentido compartir con el observador del desciframiento realizado por la IA de su actividad cerebral– el yo más esencial o "mismidad" de la persona con la posibilidad de influir y cambiar esa "mismidad" de la persona a través de la IA y del interfaz cerebro-ordenador; cambiar su mente, su alma o su mismidad al imponerle comportamientos o ideas más o menos perturbadoras (agresivas contra otros o contra sí mismo) o manipuladoras (sobre lo que le gusta, lo que quiere comprar o sobre sus ideas sociales, políticas o religiosas).

Observación y eventual inducción de cambio mental que ni siquiera realizaría otra persona (sin descartar que también pudiera ocurrir), sino el propio programa de IA que interactúa con la actividad cerebral del sujeto, enviándole estímulos eléctricos a determinadas zonas del cerebro que provocan pensamientos, deseos o decisiones que la persona podría llegar a asumir como propias sin llegar a sospechar que son inducidas, ni que su origen está en un programa de IA preparado de antemano y originariamente por un autor humano, pero actualizado y mejorado por el sistema mismo de IA al margen de todas intervención humana, en función de los datos de prueba o de experiencias del propio sistema en los casos de deep-learning, IA generativa o de uso general.

En un contexto terapéutico la finalidad curativa exigirá determinadas medidas de prudencia, buenas prácticas y garantía del secreto de los datos de la actividad cerebral. El problema surge cuando, al margen de la finalidad terapéutica –y presumiblemente por terceros, aunque no solo, que roban o penetran en la conexión del interfaz cerebro-ordenador–, se quieran imponer esos comportamientos con finalidades diversas.

Los riesgos de esas neuro-tecnologías se acrecientan si se piensa en las propuestas de transhumanistas o posthumanistas de mejorar o aumentar a la persona o dotarla de capacidades o poderes extraordinarios[33], lo que obliga a considerar

---

[33] *Vid.* sobre el transhumanismo el Manifiesto del Transhumanismo de la Asociación Humanity+ en la dirección https://humanityplus.org y el manifiesto en https://humanityplus.org) / Philosophy (https://humanityplus.org/philosophy/) / Transhumanist Declaration. *Vid.* también De Asís roig, R. y Laukytehottois, M. "Sobre el transhumanismo: Transhumanismo inclusivo", en *Soluciones tecnológicas para los problemas ligados al envejecimiento: cuestiones éticas y jurídicas,* ed. coord. por Atienza Macías, E., Alkorta Idiakez, I. (dir.), Dykinson, 2020; también la obra colectiva "El transhumanisme sota la lupa" Torralba, F. (coord.), The Club de

si la oportunidad de permitir tales mejoras –y su grado y condiciones[34]– es algo que corresponde a la libre decisión y consentimiento informado de cada uno o si la sociedad tiene algo que decir. Algo que decir, puesto que pueden acabar alterándose por una parte las condiciones de igualdad de las personas y por otra parte las condiciones de la propia libertad e identidad de cada uno. Condiciones que tienen íntima relación con la esencia de una sociedad democrática o con la libre competencia en una economía de mercado.

No puede olvidarse que el registro de la actividad cerebral de una persona es transformado en datos que la inteligencia artificial descifra e interpreta. Pero sería un error reducir lo que se hace con las neuro-tecnologías a una mera cuestión de tratamiento de datos de la actividad cerebral, que se solucionaría con aplicar la normativa de datos. Como señala el profesor Yuste con las neuro tecnologías se está entrando directamente en la mente –el alma, dirían algunos– de la persona y el tratamiento jurídico de esa actividad merece otra consideración[35]. A tal efecto él propone la consideración de todo aquello que tiene que ver con la actividad del cerebro como algo relativo a órganos humanos, como se ha hecho en la normativa de trasplante de órganos al ser el cerebro, precisamente, un órgano humano –el órgano más importante– aplicando la normativa que sobre trasplantes de órganos se ha generalizado y se recoge entre otros en el Convenio del Consejo de Europa sobre la lucha contra el tráfico de órganos humanos[36]; convenio que responde a los mismos principios que el relativo a los derechos humanos y la biomedicina de Oviedo[37].

Roma; importante el trabajo de Hottois, G. (2014). "Le transhumanisme est-il un humanisme?", Academie Royal de Bélgica, con un acercamiento muy interesante a la cuestión sentando las bases del debate.

[34] *Vid.* sobre el debate las posiciones de Habermas, J. (2016). *El futuro de la naturaleza humana, ¿hacia una eugenesia liberal?*, Ed. Básica, 6.ª imp.; Sandel, M. (2007). "*Contra la perfección. La ética en la era de la ingeniería genética*", Ed. Marbot, Barcelona; Fukuyama, F. (2002). *El fin del hombre: consecuencias de la revolución biotécnológica*, Barcelona, Ed. B.

[35] *Vid.* Yuste, R. y De la Quadra-Salcedo, T. (2023). "Neuro-Rights and New Charts of Digital Rights: A Dialogue Beyond the Limits of the Law", *Indiana Journal of Global Legal Studies*, Vol. 30-1.

[36] Convenio del Consejo de Europa sobre la lucha contra el tráfico de órganos humanos, hecho en Santiago de Compostela el 25 de marzo de 2015.

[37] Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997.

Aunque el consentimiento es un elemento central de la normativa en todo lo que tiene que ver con los órganos del ser humano, lo característico de dichos convenios es que no basta con ese consentimiento que pueda dar cada persona, puesto que en definitiva no se trata de algo que afecte sólo a cada persona en particular, sino de algo que acaba afectando a la humanidad y a todos y cada uno de sus integrantes.

Por eso las demandas de potenciación y aumentación de humanistas y transhumanistas plantean el reto de las consecuencias que las mismas tienen en relación con el riesgo de sustitución de la humanidad actual por otra en que surgirían dos tipos de personas: las aumentadas y potenciadas y las demás, con afección al derecho a la igualdad (art. 14 de la Constitución), que se pretendería solventar con sistemas de ayudas que traten de equiparar la situación facilitando el acceso de todos a programas gratuitos o subvencionados de potenciación.

Pero, más allá de la igualdad, no puede ignorarse que esa potenciación y mejora de las personas –que, en determinados casos a decidir por el legislador, podría ser legítima– entraña riesgos en cuanto a la independencia y las capacidades de la persona para mantener conciencia de su propia identidad y de independencia respecto de un sistema de inteligencia artificial, quienquiera que sea el que lo maneje[38]. Capacidades que podrían quedar enervadas, perdiendo en todo o en parte la de buscar cada uno por sí mismo solución para los problemas que la vida diaria plantea con pérdida del hábito de buscar tales soluciones.

Suscita además la cuestión de la dependencia que respecto de los sistemas de IA plantea una sociedad de personas potenciadas y mejoradas habituadas diariamente a depender de tales sistemas. También la cuestión de los sesgos en las informaciones, impulsos o estímulos que se introduzcan en las personas conectadas

---

[38] Goering, S., Yuste, R. et al. (2016). "On the Necessity of Ethical Guidelines for Novel Neurotechnologies", *revista Cell*, Volume 167, Issue 4, pp. 882-885, 3 November, afirman: *"Una de las más importantes cuestiones éticas y filosóficas a afrontar es la posibilidad de cambios sustanciales en el concepto del "yo". Mientras en la actualidad tendemos a identificarnos a nosotros mismos como relativamente separados y entidades privadas limitadas por nuestros propios cuerpos el uso de las novedades de las neurotecnologías puede dirigirnos hacia una parcial disolución de las ideas tradicionales sobre el yo*". En otro orden de cosas, pero situándonos en el mundo digital y de internet, Carr Nicholas, detecta también cambios de comportamiento en "Superficiales. ¿Qué está haciendo internet con nuestras mentes?" Ed. Taurus, 4. ed., 2016, sostiene que al confiar en los ordenadores para comprender el mundo nuestra inteligencia se aplana y convierte en inteligencia artificial; pp. 269 y 270.

con tales sistemas de inteligencia artificial y las posibilidades de manipulación de la gente en el momento de ejercer sus derechos democráticos en función de quién sea el titular del sistema de inteligencia artificial con el que se conectan –a través de comunicaciones electrónicas– los interfaces cerebro ordenador que dichas personas llevan.

En esas condiciones no puede bastar con la libertad individual ni con el consentimiento para participar en proyectos de mejora o potenciación de las personas. El legislador deberá determinar con mucha cautela las eventuales condiciones en que esa mejora y potenciación puede llegar a ser posible y lícita en función de las finalidades que se pretendan, que pudieran no siempre ser estrictamente terapéuticas, y en función no solo de las garantías que se ofrezcan, sino de las que se impongan para garantizar que no se produzcan abusos o manipulaciones en la democracia[39].

No se trata pues solo de proteger a las personas frente al uso y aplicación de las neurotecnologías, sino también de proteger a la sociedad entera para mantener la democracia.

Lo mismo puede decirse en relación con el mercado y la competencia, en la medida en que las personas conectadas puedan ser inducidas –desde los sistemas de inteligencia artificial conectados con sus cerebros a través del interfaz cerebro máquina– a tomar decisiones que tienen que ver con sus preferencias en el mercado y sus inversiones.

Este es el sentido que tiene el reconocimiento de los llamados neuro derechos que no se refieren a otra cosa sino a las garantías frente al uso de estas neurotecnologías que aseguren que cada persona tenga siempre libertad para decidir, de modo que no quede condicionada por los sesgos o por estímulos y sentimientos que se les puedan inducir con mantenimiento siempre de la conciencia de sí mismos y de su identidad y de su capacidad de decidir en todo caso.

---

[39] *Vid.* Quadra Salcedo Fernández del Castillo, T. (2023). "Derechos y libertades y neurotecnologías convergentes aplicadas a la actividad cerebral", *Derecho Digital e Innovación* (La Ley), núm. 18, octubre-diciembre.

7. CONCLUSIONES

Todo el Derecho de la sociedad digital se ha ido construyendo a atención a la garantía de los derechos y libertades fundamentales de las personas, pero en la descripción de varios de los ámbitos que han sido objeto de análisis ha podido verse que no solo los derechos y libertades individuales puede estar en riesgo, sino que puede haber daños colaterales. Daños colaterales en ocasiones vinculados indirectamente a la generalización y universalidad de la sociedad digital y al aumento de sus riesgos, pues cuando riesgos y daños aumentan en una dimensión cuantitativa muy importante lo cuantitativo se hace cualitativo y salta a otra dimensión en cuanto transforma de alguna manera la sociedad misma en que vivimos al afectar a instituciones centrales de la sociedad en que vivimos. Es lo que ocurre en el caso expuesto de los precios diferenciados por discriminación algorítmica que no solo afectan a los derechos de las personas, sino al mercado y la competencia como instrumento de una economía de mercado en la que la libertad de empresa en un mercado en competencia (como límite natural de dicha libertad) no solo podría quedar afectado, sino también la democracia. La democracia en la medida en que el poder de los representantes del pueblo puede quedar comprometido en una economía monopolizada por pocos actores si la competencia desaparece y queda comprometida; tal fue el origen de las normas anti-trust en los Estados Unidos ante el temor a sus consecuencias para la democracia[40]. Sin perder de vista que las actuales tecnologías que dan soporte a la sociedad digital tienen una tendencia a la concentración y al monopolio, como se pone de relieve con los primeros puestos al que han escalado en las bolsas mundiales todas las tecnológicas y con las reacciones que tanto el Departamento de Justicia de los Estados Unidos como la Comisión

---

[40] *Vid.* Letwin, W. L. (1955). "Congress and The Sherman Antitrust Law: 1887-1890". *The University of Chicago Law Review*, núm. 23, en cuya página describe las demandas del "Movimiento Granger" [Buck, The Granger Movement 52-53 (1913) Cambridge Harvard University Press, 1913] y la resolución de una Convención de Granjeros de Illinois en 1873 en que decían de los monopolios que "*han demostrado ser perjudiciales para la prosperidad pública, corruptores en su gestión y peligrosos para las instituciones republicanas*". También Lande, R. H. en "Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged", *University of Baltimore School of Law*, cita en p. 99, nota 137, la intervención del Senador Hoar, redactor del texto final de la Sherman Act, sobre el peligro de los monopolios para las instituciones republicanas cuando dijo que *"ha inducido al Congreso a ocuparse del asunto la queja que ha llegado de todas partes y de todas las clases del país sobre estos grandes monopolios, que se están convirtiendo no sólo en algunos casos en un perjuicio real para la comodidad de la vida ordinaria, sino que son una amenaza para las propias instituciones republicanas".*

de la UE han comenzado a adoptar desde hace algún tiempo contra graves conductas contra la afecciones a la competencia de las grandes tecnológicas, llegando a adoptar medidas específicas contra algunas. La preocupación por esa dinámica de concentración se pone de relieve en el hecho de que el Reglamento de Mercados digitales haya acuñado la categoría –y la expresión– de "guardianes de acceso" (*gatekeepers*) (art. 3 del Reglamento) y clasificado ya seis como tales[41]. En ese contexto es en el que puede haber víctimas colaterales como el mantenimiento de una real y efectiva competencia condición inexcusable para la existencia de una economía de mercado que puede quedar afectada. Y con ella también la democracia que, además, puede estarlo como consecuencia de una generalizada aplicación de neurotecnologías a las personas como se ha visto más arriba que igualmente pueden afectar a la democracia y a la sociedad tal y como hasta ahora la hemos conocido.

La primera conclusión tiene pues que ver con la necesidad de no solo contemplar los riesgos para los derechos y libertades fundamentales, sino también para la democracia y el mercado y la competencia.

La segunda tiene que ver con el hecho de que el Derecho de la sociedad digital en sus diversas manifestaciones surge con algunas características propias tanto respecto de los problemas que afronta como de la forma como lo hace. No se trata de que las reglas aplicables en el mundo tradicional para articular los derechos y libertades entre sí y con otros bienes constitucionales no valgan en el mundo digital, sino de que las circunstancias cambian de tal manera que nos obligan a una aplicación distinta y, en ocasiones, aparentemente contradictoria; pero sólo aparentemente. En efecto, lo que en realidad ocurre es que se trata del problema de siempre: de articular derechos fundamentales y libertades que entran en conflicto entre sí, sin que tengamos de antemano un criterio pre-establecido de preferencia entre ellos, sino que el mismo se obtiene tras una ponderación de las circunstancias que concurren en dichos conflictos entre derechos y libertades. Ponderación que ha de hacerse a la vista de las circunstancias que concurren en cada caso descendiendo y penetrando en la lógica, las razones y los valores que subyacen a dichos derechos y libertades para llegar a la solución del conflicto de articulación entre derechos y libertades. Solución que, como se ha visto, puede ser distinta en los conflictos que se producen en la sociedad digital respecto frente a los propios de la sociedad

---

[41] Designó como tales la Comisión el 6 de septiembre de 2023 a seis: Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft.

tradicional. Respuestas diferentes dirigidas en muchos casos, sin embargo, a mantener justamente la misma lógica de primacía y prevalencia de los derechos y libertades que lo merezcan en función de las circunstancias de cada caso.

La novedad es que en la solución de esos conflictos emergen y se interfieren conceptos, ciencias, prácticas y conocimientos tecnológicos cuyo alcance y derivaciones no siempre son fáciles de interpretar, pero que pueden condicionar la solución. Por otra parte, tampoco es posible para el legislador dar de antemano la solución en el propio texto normativo, porque todo depende de matices muy importantes y de las concretas situaciones que pueden producirse en la realidad de cada caso, lo que está exigiendo que las normas no agoten todo el espacio decisional normativo *a priori* de determinación o definición de lo que se puede hacer, sino que remitan a otras autoridades que vayan completando ese espacio decisional.

Espacio que se va cubriendo no siempre con normas que a priori y con carácter general determinan lo que se puede hacer, sino con la resolución puntual en cada caso concreto de lo que es o no correcto, pero bajo el imperativo categórico de que esa solución pretenda ser regla de conducta para casos idénticos. En definitiva, erigiéndose esa solución de cada caso en criterio de solución de casos sucesivos en la medida en que los posteriores sean idénticos al primero y, si no lo fueran, adaptándolo a las nuevas circunstancias diferenciales cuando fuera necesario. Se trata de la regulación a través de la solución de los concretos conflictos concretos ("*regulation through adjudication*" en terminología anglosajona) –conflictos de articulación entre derechos y libertades– que confirmada por las decisiones de los tribunales se erigen en reglas de conducta para supuestos idénticos futuros.

La construcción en dos fases del Derecho de la sociedad digital surge como rasgo frecuente que empieza a caracterizarle: fase normativa y definidora de conductas, pero en que, junto a las reglas más clásicas de conducta, se echa mano de términos abiertos, principiales y valorativos y una fase aplicativa y resolutoria de cada conflicto, pero cuyas concretas soluciones se erigen en regla de conducta y resolución para los sucesivos.

Vemos esos rasgos en el reglamento europeo de inteligencia artificial o en los reglamentos sobre servicios digitales o mercados digitales, en que sus reglas –no siempre muy precisas y con frecuencia en tensión, o aparente contradicción, con otras del mismo texto– se complementan con referencias a principios, valores, conocimientos, ciencias, prácticas y técnicas que se erigen en elementos para la interpretación y aplicación de esas mismas reglas. Se complementan también con remisiones

a normas armonizadas, cuando no a especificaciones comunes o medidas de efectos equivalentes[42] a establecer por la Comisión o distintas autoridades competentes.

En esa segunda fase empieza a ser inevitable la remisión a autoridades competentes, en muchas ocasiones de carácter independiente que van concretando la regulación que la primera fase no puede agotar. Todo ello sin perjuicio desde luego de la última palabra que compete siempre a la Justicia. No es ajeno a esa interposición de autoridades reguladoras antes de la palabra última de la Justicia, la presencia de esas ciencias, conocimientos y prácticas *aliunde* al Derecho, pero a colonizar por él, a las que hay que acudir para completar el sistema regulatorio en la sociedad digital.

Todo ello da una cierta sensación de complejidad de la normativa –integrada por reglas y principios (definidos y reconocidos en fases diversas)– a aplicar a situaciones diferentes, entreveradas y en hibridación y articulación con distintas prácticas, técnicas y conocimientos *aliunde*; complejidad que determina la morfología del Derecho en nuestros días y de las normas en estos escenarios digitales. Frente al Derecho clásico, codificado y silogístico basado en reglas claras que establecían lo que se puede o no hacer y las consecuencias de no hacerlo, surge en estos contextos tecnológicos más complejos la regulación como técnica y paradigma para la ordenación jurídica.

Es sintomático que fue en el ámbito de la economía donde por primera vez, en cierto modo, se desplegó una forma de primitiva regulación (bien es verdad que *ex post*) como fue el Derecho de la competencia que sancionaba, una vez incurridos en ellos, los abusos y prácticas contrarias a la competencia que, posteriormente se fue extendiendo, ya como regulación propiamente dicha, a sectores de actividad cerrados inicialmente, en general, a la competencia por ser monopolios naturales, pero que luego se liberalizaron. Es la regulación la que ha hecho posible el mercado y la competencia en esos sectores, pero a costa de unas pocas reglas y, sobre todo, invocando principios y referencias a prácticas, conocimientos y técnicas en principio ajenas (*aliunde*) al Derecho. Y lo hace, además, interponiendo para la resolución de conflictos el elemento de una Administración independiente o Agencia que aplica las regulaciones normativamente establecidas y las completa con las soluciones que va dando en función de las circunstancias de cada caso y los principios, conocimientos, prácticas y técnicas ajenas al Derecho, pero colonizados por este que la misma Agencia aplica.

---

[42] *Vid.* art. 41 del Reglamento de Inteligencia Artificial.

Administraciones que al hilo de solucionar los casos concretos sientan precedentes y establece directrices ("*regulation through adjudication*") que forman un depósito regulatorio, aunque siempre bajo el control último de los tribunales[43].

Una última conclusión o reflexión sobre las consecuencias de la dislocación que producen las tecnologías digitales y la IA que determinan la reconsideración y cambio de las soluciones tradicionales del Derecho es que, en ocasiones, obligan a revelar sus ocultas raíces en los presupuestos morales o éticos pre-jurídicos sobre los que el Derecho ha ido construyendo sus reglas y principios y que podemos reconocer en algunas tan simples como el *honeste vivere*, *alterum non laedere* y *suum cuique tribuere* de Ulpiano[44]; raíces ocultas o subconsciente del Derecho mismo. Subconsciente tapado, como debe ser, por el Derecho positivo o consciente, aunque surjan destellos de tal subconsciente en los principios y valores integrantes del Derecho mismo, más allá de sus reglas. Lo llamativo de la sociedad digital y sus disrupciones es que nos obliga a recodar esas raíces morales para decidir qué límites han de ponerse a unos avances tecnológicos incorporados ya a la "naturaleza" cotidiana de nuestro tiempo –construidos sobre las "leyes" escondidas de la naturaleza– que nos invitan a aprovechar todas sus posibilidades. Desde una visión materialista, que algunos podrían considerar realista, se propondría no resistirse a a aprovechar todas las posibilidades de ese oxímoron de una "naturaleza tecnológica" desbordada dejando que el "modo de producción" que la misma permite sea el que determine nuestra conciencia, abriendo paso libre y sin obstáculos a todas sus posibles realizaciones.

Sin embargo, lo que hemos visto a lo largo del presente trabajo, en los diversos ámbitos que se han ido analizando (derecho al olvido, precios diferenciados, herencia digital o neuroderechos) es que, afortunadamente, es la conciencia –a partir de los valores morales sobre los que el Derecho se ha construido– la que, esta vez, parece determinar lo que es justo, lo que hay que hacer y cómo ha de ser el Derecho que lo regule.

---

[43] *Vid.* Quadra Salcedo Fernández del Castillo, T. (2023). "La regulación como modalidad genérica de intervención pública. La regulación en la sociedad digital", *Cuadernos de Derecho Transnacional*, octubre, Vol. 15, núm. 2.

[44] Digesto 1, 1, 10, 1.

BIBLIOGRAFÍA

Alegre Ávila, J. M. "Acerca de los derechos subjetivos: derechos fundamentales y eficacia de los derechos en las relaciones entre particulares". en *AEPDA* disponible en https://www.aepda.es/AEPDAEntrada-3385-Acerca-de-los-derechos-subjetivos-derechos-fundamentales-y-eficacia-de-los-derechos-en-las-relaciones-entre-particulares.aspx

Alfaro, J. "Precios personalizados y discriminación", en *Almacén de Derecho*, disponible en https://almacendederecho.org/precios-personalizados-discriminacion

Antón Juárez, I. (2021). "Marketplaces que personalizan precios a través del big data y de los algoritmos: ¿esta práctica es legal en atención al derecho de la competencia europeo?", *Cuadernos de Derecho Transnacional*, marzo, Vol. 13, núm. 1.

Bar-Gill, O. (2019). "Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions", *The University of Chicago Law Review*, núm. 86, march, number 2.

Beladiez Rojo, M. (2017). *"La eficacia de los derechos fundamentales entre particulares".*

Bodas Daga, Mª. E. (2007). *La defensa "post mortem" de los derechos de la personalidad*, Bosch, Barcelona.

Cámara Lapuente, S. (2019). "La sucesión mortis-causa en el patrimonio digital", El notario del siglo XXI, *Revista del Colegio Notarial de Madrid*, núm. 84.

Carr, N. (2016). *Superficiales. ¿Qué está haciendo internet con nuestras mentes?*, Ed. Taurus, 4ª edición.

Cruz Villalón, P. (1988). "Derechos fundamentales y Derecho Privado", en Academia Sevillana del Notariado.

De Asis Roig, R. y Laukytehottois, M. (2020). "Sobre el transhumanismo: Transhumanismo inclusivo", en *Soluciones tecnológicas para los problemas ligados al envejecimiento: cuestiones éticas y jurídicas*, Atienza Macías, E. (coord.) e Alkorta Idiakez, I. (dir.), Dykinson.

Díaz Alabart, S. (2020). *La protección de los datos y contenidos digitales de las personas fallecidas*, Ed. Reus.

Fukuyama, F. (2002). *El fin del hombre: consecuencias de la revolución biotécnológica*, Barcelona, Ed. B.

García Torres, J. y Jiménez Blanco, A. (1986). "Derechos fundamentales y relaciones entre particulares: la Drittwirkung en la jurisprudencia del Tribunal Constitucional", Cuadernos Civitas, Madrid.

Ginebra Molins, M. E. "Morir en la era digital. Voluntades digitales, intimidad y protección de datos personales", en *Derecho Mercantil y Tecnología*, Parra, A. (dir.) y Blanco Sánchez, M. J. (coord.), Madrid.

Goering, S. y Yuste, R. et al. (2016). "On the Necessity of Ethical Guidelines for Novel Neurotechnologies", *Revista Cell*, Volume 167, Issue 4, pp. 882-885, 3, November.

Habermas, J. (2016). *El futuro de la naturaleza humana, ¿hacia una eugenesia liberal?*, Ed. Básica, 6ª imp.

Hannak, A. et al. (2014). "Measuring Price Discrimination and Steering on E-commerce Web Sites", Proceedings of the 2014 Conference on Internet Measurement Conference 305, 316, November.

Hottois, G. (2014). "Le transhumanisme est-il un humanisme?", Academie Royal de Bélgica.

Lande, R. H. (1913). "Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged", University of Baltimore School of Law Buck, The Granger Movement 52-53, Cambridge Harvard University Press.

Letwin, W. L. (1995). "Congress and The Sherman Antitrust Law: 1887-1890", *The University of Chicago Law Review*, núm. 23.

Maggiolino, M. (2017). "Personalized Prices in European Competition Law", June 12, Bocconi Legal Studies Research, en SSRN: https://ssrn.com/abstract=2984840 or http://dx.doi.org/10.2139/ssrn.2984840

Melvin Tjon, A. (2020). "Personalized Pricing Using Payment Data: Legality and Limits under European Union and Luxembourg Law", *European Business Law Review 31*, núm. 5.

Ordelin Font, J. L. y Oro Boff, S. (2020). "Bienes digitales personales y sucesión mortis causa:la regulación del testamento digital en el ordenamiento jurídico español", *Revista de Derecho* (Valdivia), Vol. XXXIII, núm. 1, julio.

Otero Crespo, M. (2019). "La sucesión en los «bienes digitales». La respuesta plurilegislativa española", *Revista de Derecho Civil*, Vol. VI, núm. 4, octubre-diciembre.

Pastrana Esparraga, M. (2021). "Los precios personalizados como práctica anticompetitiva de discriminación mediante el uso de algoritmos", en *El sistema jurídico ante la digitalización: estudios de derecho privado*, Jonatan Cruz, Á. et al. (coord.), Tirant lo Blanch.

Quadra Salcedo Fernández Del Castillo, de la T. (1981). *El recurso de amparo y los derechos fundamentales en las relaciones entre particulares*, Ed. Civitas.

Quadra Salcedo Fernández del Castillo, de la T. (2013). "Derecho público, Derecho privado y derechos fundamentales", *Revista General de Derecho Administrativo 34*.

Quadra Salcedo Fernández del Castillo, de la T. (2023). "Derechos y libertades y neurotecnologías convergentes aplicadas a la actividad cerebral", *Derecho Digital e Innovación*, núm. 18, octubre-diciembre.

Quadra Salcedo Fernández del Castillo, de la T. (2023). "La regulación como modalidad genérica de intervención pública. La regulación en la sociedad digital", *Cuadernos de Derecho Transnacional*, octubre, Vol. 15, núm. 2.

Rubí, A. (2021). "Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores", *Revista de Educación y Derecho*, núm. 24, abril-septiembre, accesible en https://almacendederecho.org/precios-personalizados-discriminacion

Ryan, C. (2014). "Digital market manipulation", *George Washington Law Review 82*, 4.

Sandel, M. (2007). *Contra la perfección. La ética en la era de la ingeniería genética*, Ed. Marbot, Barcelona.

Santos Botelho, C. (2024). "The End of the Deception? - Counteracting Algorithmic Discrimination in the Digital Age", *The Oxford Handbook on Digital Constitutionalism*, Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4659451

Santos Morón, M. J. (2018). "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho transnacional*, Vol. 10, núm. 1.

Tena Arregui, R. (2019). "¿Son justos los precios personalizados mediante algoritmos"? Blog, "Contratos, Economía, Internet y Nuevas Tecnologías".

Yuste, R., Goering, S. et al. (2017). "Four ethical priorities for neurotechnologies and AI", *Revista Nature*, 8 noviembre, accesible en https://www.nature.com/news/four-ethical-priorities-for-neurotechnologies-and-ai-1.22960

Yuste, R. y De La Quadra-Salcedo, T. (2023). "Neuro-Rights and New Charts of Digital Rights: A Dialogue Beyond the Limits of the Law", *Indiana Journal of Global Legal Studies*, Vol. 30-1, Winter.

Zuiderveen Borgesius Frederik y Poort Joost. "Online Price Discrimination and EU Data Privacy Law", *Consum Policy*, p. 364. Disponible en SSRN: https://ssrn.com/abstract=3009188 or http://dx.doi.org/10.2139/ssrn.3009188

Capítulo 3
CÓMO ABORDAR JURÍDICAMENTE EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LOS DERECHOS FUNDAMENTALES[1]

Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional
Universidad de Valencia
Valgrai
https://orcid.org/0000-0003-2661-0010

1. CONSTITUCIONALMENTE HAY QUE GARANTIZAR, GUIAR Y CONTENER LA INNOVACIÓN EN INTELIGENCIA ARTIFICIAL

La Constitución "se forjó en un mundo analógico" y, como señala Balaguer con palabras de Benedetti, "cuando creíamos que teníamos todas las respuestas, de pronto, cambiaron todas las preguntas", de ahí que se hable de la necesidad de una "Constitución del algoritmo" para "constitucionalizar el algoritmo y digitalizar la constitución"[2]. Se ha afirmado la necesidad de "un nuevo paradigma

---

[1] El presente estudio es resultado de investigación de los siguientes proyectos: MICINN Proyecto "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-136439OB-I00) financiado por MCIN/AEI/10.13039/501100011033/; Proyecto "Algoritmic law" (Prometeo/2021/009, 2021-24 Generalitat Valenciana); "Algorithmic Decisions and the Law: Opening the Black Box" (TED2021-131472A-I00) y "Transición digital de las Administraciones públicas e inteligencia artificial" (TED2021-132191B-I00) del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1, Convenio de Derechos Digitales-SEDIA Ámbito 5 (2023/C046/00228673) y Ámbito 6. (2023/C046/00229475).

[2] Balaguer Callejón, F. (2021). "La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital", en Gomes, A. C. y otros (coords.), *Direito Constitucional: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho. Belo Horizonte: Fórum*. Ver también entre otros, La constitución del algoritmo, Fundación Manuel Giménez Abad (2022). https://www.fundacionmgimenezabad.es/publicaciones/la-constitucion-del-algoritmo

en la protección de los derechos fundamentales [...] una reorientación a consecuencia de la naturaleza de las tecnologías de las que hablamos"[3]. Este estudio profundiza en la intersección entre la inteligencia artificial (IA) y los derechos fundamentales. Obviamente, se centra la atención en algunos elementos básicos de lo que sería una parte general[4]. No se entra ahora en lo que sería la parte especial relativa a cada derecho fundamental o sector específico,[5] objeto de atención de otros estudios de esta obra. Lo mismo sucede respecto de la discriminación algorítmica en la que he profundizado en otros trabajos[6].

---

[3] Sarrión Esteve, J. (2020). "El derecho constitucional en la era de la inteligencia artificial, los robots y los drones", Pérez Miras, A. y otros (dirs.): *Setenta años de Constitución Italiana y cuarenta años de Constitución*, Vol. 5; Retos en el siglo XXI, Romboli S. (coord.), pp. 321-334, p. 328. En dicha obra una aproximación algo superficial Gascón Marcén, A., "Derechos humanos e inteligencia artificial", pp. 335-350.

[4] Por cuanto una aproximación desde la parte general, me remito a mi estudio, "Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", en *Derechos y garantías ante la inteligencia artificial*...cit pp. 69-105. Posteriormente, para la parte general destaca Presno Linera, M. Á. (2023). *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid; también en "Teoría general de los derechos fundamentales e inteligencia artificial: una aproximación", en Balaguer Callejón, F. y otros (coords.) (2023). *Derechos fundamentales y democracia en el constitucionalismo digital*, Aranzadi, Cizur Menor, pp. 461-491. Destaca también, Asís Roig, R. F. de (2022). "Ética, tecnología y derechos", en Garrido Martín, J. y otros (dirs.): *Inteligencia artificial y Filosofía del derecho*, Laborum, pp. 91-114. Una primera aproximación general en Martínez Martínez, R. "Inteligencia artificial, Derecho y derechos fundamentales", en Quadra-Salcedo, T. de la, (dir.), *Sociedad Digital y Derecho*, BOE-Red.es, pp. 259-278.

[5] Existen ya numerosos estudios particulares respecto de derechos específicos. No obstante, me permito remitir a más de 20 estudios en Cotino Hueso, L. (ed.). (2022). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Thompson-Reuters Aranzadi, Cizur y en Balaguer, F. y Cotino, L. (2023). *Derecho público de la inteligencia artificial*, F. Jiménez Abad-Marcial Pons. Acceso completo

De interés diversos de los estudios en Castellanos Claramunt, J. (coord.) (2023). *Inteligencia artificial y democracia; garantías, límites constitucionales*, Atelier, Madrid; y Arellano Toledo, W. (coord.) (2023). *Derecho, Ética e Inteligencia Artificial,* Tirant lo Blanch, Valencia.

Abordar el impacto de la IA en cada derecho parece un intento abocado a una necesaria superficialidad. No obstante, al efecto destaca sin duda la parte especial en Presno Linera, M. Á., *Derechos fundamentales ...cit.*. También, Gutiérrez García, E. (2024). *Inteligencia artificial y derechos fundamentales. Hacia una convivencia en la era digital*, Colex; Gómez Abeja, L. (2022). "Inteligencia artificial y derechos fundamentales", en Garrido Martín, J. y otros (dirs.): *Inteligencia artificial y Filosofía del derecho*, Laborum, pp. 91-114.

[6] "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", en Gamero Casado, E. (dir.) (2023), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia, acceso capítulo. Acceso obra

Y entiendo necesario que el punto de partida sea afirmar un deber de progreso e innovación tecnológica que incluso puede transformarse en un derecho o al menos en obligaciones concretas. La IA penetra hoy en nuestras vidas y lo hará aún más. Decide qué leemos, oímos y vemos en plataformas y redes, influyendo así en cómo percibimos el mundo. Determina con quiénes nos relacionamos, incluso en aspectos íntimos; qué compramos, e incluso establece precios específicos para nosotros. Decide las contrataciones de las empresas (incluso en el sector público). En muchos empleos, dicta qué hacer y cuándo, nos controla y evalúa. Pronto decidirá a qué colegio o universidad asistirán nuestros hijos, y ya elige y propone muchos tratamientos médicos o de asistencia social. También es el factor que nos preselecciona para inspecciones o sanciones directas. Si no decide directamente, lo hace a través de un ser humano que, a menudo, acepta acríticamente sus propuestas sin una revisión sustancial. Además, la IA respalda decisiones políticas y administrativas para mejorar la movilidad, la sostenibilidad, la educación, la salud, etc., y pronto, las decisiones judiciales. Por lo general, ni nosotros ni la sociedad civil somos plenamente conscientes de todo lo que ya hace, y no siempre podemos estar seguros de que el sector privado o público que utiliza la IA tenga un control y conocimiento pleno de sus acciones.

Creo que es necesario –también para el Derecho– asumir que los sistemas IA, automatizados y las tecnologías conexas pueden ser muy beneficiosos para la sociedad y los individuos. Esta dimensión beneficiosa rara vez se enfatiza desde una perspectiva jurídica constitucional, aunque se ha afirmado la cláusula de progreso tecnológico como un derecho humano[7].

Por ello, el Derecho también debe proteger el desarrollo de la IA y fomentar la innovación, al tiempo que la orienta y contiene, ya que puede ser muy positiva para toda la humanidad. Al igual que la electricidad o el propio internet, es probable que tengamos algo muy parecido a un *derecho a la IA*, con obligaciones para nuestros poderes públicos de promover, desarrollar y aplicar la IA, al menos en sectores específicos. Y si no es un derecho en sí, la IA sin duda

---

[7] Desde una perspectiva jurídica, sobre los beneficios de la tecnología como objeto de protección jurídica puede seguirse en sus diversos trabajos, afirmando la cláusula de progreso tecnológico como derecho humano. Sánchez Barrilao, J. F. (2016). "Los fundamentos del "progreso informático" ... cit. y "El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional", *Estudios de Deusto: revista de Derecho Público*, Vol. 64, núm. 2, pp. 225-258, p. 256.

está conectada con muchos derechos fundamentales. Así sucedió con el llamado derecho a internet[8]. Así, en poco tiempo podría ser impensable no exigir el uso de sistemas inteligentes en ámbitos como la investigación, la salud, el transporte, la sostenibilidad y la educación.

A pesar de las ventajas de la IA, un jurista no puede ignorar que también presenta un lado mucho más oscuro. La autonomía es una característica inherente a la IA y supone un riesgo adicional a los muchos peligros e impactos que generan el uso de software y sistemas que realizan tratamientos automatizados de datos o que integran algoritmos. Los equipos que diseñan la IA no son perfectos. Involuntariamente, pueden crear sistemas con errores y sesgos, lo que deriva en impactos estructurales sobre los principios constitucionales y los derechos fundamentales. Y, por supuesto, los desarrolladores también pueden actuar con malas intenciones. Además, la IA y los sistemas autónomos con autoaprendizaje adquieren cierta independencia de sus creadores. Estos sistemas autónomos no son infalibles y pueden convertirse en verdaderos peligros. Como afirmó James Madison en *El Federalista* 51: "Si los hombres fueran ángeles, no sería necesario ningún gobierno. Si los ángeles gobernaran a los hombres, no sería necesario ningún control, ni externo ni interno, sobre el gobierno"[9]. Trasladando esta afirmación al ámbito del Derecho, es indudable que este tiene un papel crucial frente a los nuevos riesgos[10].

La IA, los sistemas automatizados, el reconocimiento facial y tecnologías afines suponen *disparar y con fuego racheado* a los derechos fundamentales. El Reglamento por el que se establecen normas armonizadas en materia de inteligencia

---

[8] Entre otros, mis estudios "ONLINE-OFFLINE. Las garantías para el acceso a internet y para la desconexión, bloqueo, filtrado y otras restricciones de la red y sus contenidos", *Revista De Derecho Político*, núm. 1(108), pp. 13-40. https://doi.org/10.5944/rdp.108.2020.27991

[9] Madison, James, *The Federalist No. 51.* "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments", *Independent Journal*, Wednesday, February 6, 1788. https://www.constitution.org/1-Constitution/fed/federa51.htm

[10] "Riesgos e impactos del big data, la IA y la robótica y enfoques, modelos y principios de la respuesta del Derecho", Boix Palop, A. y Cotino Hueso, L. (coords.) (2019). *Monográfico Derecho Público, derechos y transparencia ante el uso de algoritmos, IA y big data RGDA Iustel*, núm. 50, febrero. Acceso en completo https://bit.ly/37RifyJ

artificial (en adelante RIA) de 2024[11], en su Considerando 48[12] menciona hasta veintiún derechos fundamentales que pueden verse afectados por sistemas de alto riesgo, además de derechos específicos de menores. Por ello, el RIA así como el "Convenio marco sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho" del Consejo de Europa también de 2024 (en adelante, Convenio IA), buscan asegurar que las "actividades dentro del ciclo de vida de los sistemas de inteligencia artificial sean plenamente coherentes con los derechos humanos, la democracia y el Estado de Derecho" (art. 1 Convenio IA)[13].

2. PREMISAS JURÍDICAS Y DOGMÁTICAS: LA DIMENSIÓN OBJETIVA DE LOS DERECHOS Y LA DIGNIDAD PARA LA GARANTÍA DE LA IA Y LOS DERECHOS FUNDAMENTALES

Desde el inicio de la atención a estas cuestiones, especialmente desde la UE, han sido numerosas las proclamaciones sobre la dignidad y los derechos fundamentales como elementos fundamentales en la ética de la IA y su marco jurídico[14],

---

[11] En este estudio se sigue la versión oficial traducida al español aprobada por Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024. Contiene la numeración final de considerandos y artículos. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf
Sobre el RIA, por todos, con más de treinta autores, me remito a Cotino Hueso, L. y Simón Castellanos, P. (coords.) (2024). *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi. Una visión general del Reglamento en Presno Linera, M. Á. (2023). "La propuesta de "Ley de Inteligencia Artificial" europea", en *Revista de las Cortes Generales*, núm. 116, pp. 81-133.

[12] Dignidad, vida privada y familiar, protección de datos, libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración. Además, los derechos específicos de menores y la salud y la seguridad de las personas y la protección del medio ambiente.

[13] Se sigue el proyecto de marzo para su adopción final por el Comité de Ministros en mayo de 2024. https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680aee411

[14] Un análisis exhaustivo lo realizo en "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho" en *Revista Catalana de Derecho Público* núm. 58, junio 2019. http://revistes.eapc.gencat.cat/index.php/rcdp/issue/view/n58 http://dx.doi.org/10.2436/rcdp.i58.2019.3303 Ver, Parlamento Europeo, *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo*, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica

destacando la necesidad de una visión "antropocéntrica" y "antropogénica"[15]. El Supervisor Europeo de Protección de Datos acertó al afirmar que es esencial situar "la dignidad en el centro de una nueva ética digital", pues "un mayor respeto de la dignidad humana y una mayor salvaguardia de la misma podrían contrarrestar la vigilancia generalizada y la asimetría de poder que enfrentan las personas"[16]. La Carta de Derechos Digitales de España, adoptada en julio de 2021[17], menciona explícitamente la dignidad en su introducción y el apartado XXV.1[18]. La UNESCO también ha resaltado esta perspectiva[19]. Recientemente, el Convenio IA dedica un artículo a afirmar que "Cada Parte adoptará o mantendrá medidas para respetar la dignidad humana y la autonomía individual en relación con las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial" (art. 7).

Más allá de las proclamaciones ocasionalmente retóricas que caracterizan todas las declaraciones éticas de IA[20] y el *soft law*, desde el punto de vista jurídico y dogmático, hay que subrayar la importancia de la dignidad y la dimensión

---

(2015/2103(INL)) letra U. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES

[15] Parlamento Europeo, *Resolución de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)),* núm. 2, y considerando 12. Su anexo incluye una propuesta de Reglamento regulatorio. Ver su artículo 7.

[16] Hoffmann-Riem, W. (2019). *Big Data. Desafíos también para el Derecho*, Civitas, Madrid, p. 98.

[17] Gobierno de España-De la Quadra, T. (coord.) (2021). *Carta de Derechos digitales, julio.* https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf Por todos, Cotino Hueso, L. (coord.) (2022). *La Carta de Derechos Digitales*, Tirant lo Blanch, Valencia. También, Ramón Fernández, F. (coord.) (2022). *Los nuevos retos de los derechos digitales,* Tirant lo Blanch, Valencia.

[18] Con acierto afirma su introducción que "La persona y su dignidad son la fuente permanente y única de los mismos y la clave de bóveda tanto para proyectar el Ordenamiento vigente sobre la realidad tecnológica, como para que los poderes públicos definan normas y políticas públicas ordenadas a su garantía y promoción". Y el XXV1 *dispone* que "La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad".

[19] Conferencia General 41ª reunión - París, 41 C/73, 22 de noviembre de 2021. Anexo. https://unesdoc.unesco.org/ark:/48223/pf0000379920_spa Entre otros, ver núm. 15, III. 1, núm. 13 y ss. y 10º.

[20] Especialmente Fjeld, J. y otros. *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, The Berkman Klein Center for Internet & Society Research, núm. 2020-1. https://cyber.harvard.edu/publication/2020/principled-ai

objetiva de los derechos fundamentales para guiar y enfrentar los desafíos jurídicos que plantea la IA, siguiendo la jurisprudencia[21] y doctrina constitucional española[22], siguiendo la alemana[23]. Buena parte de las propuestas de este estudio pueden encontrar anclaje y legitimación constitucional a partir de la dignidad y la dimensión objetiva de los derechos. Es importante recordar que, como lo demuestra la jurisprudencia europea y española, la dignidad es jurídicamente útil en múltiples aspectos relacionados con el vínculo de la IA con los derechos fundamentales.

Así, la dignidad[24] sirve como reactivo para establecer límites jurídicos claros ante los peligros estructurales para los derechos o la humanidad, señalando las barreras que deben aplicarse a la IA. La dignidad y la dimensión objetiva de los

---

[21] El Tribunal Constitucional español reconoció por primera vez esta dimensión objetiva de los derechos y libertades en la STC 25/1981, de 21 de julio (FJ 5º), STC 18/1984 /FJ 6º), como, de manera muy significativa, en la STC del aborto 53/1985, de 11 de abril (FJ 4º). Asimismo, entre otras en la STC 163/1986, de 17 de diciembre (FJ 1º), STC 129/1989, de 17 de julio, FJ 3º, STC 172/1989, de 19 de octubre (FJ 3º), o en el ATC 382/1996, de 18 de diciembre (FJ 3º), entre otros.

[22] No se trata de una materia excesivamente trabajada con rigor. Además de los trabajos que luego se mencionan de Otto o en la obra que coordina Bastida, me permito destacar especialmente los análisis de Salvador Martínez, M. (2001). "Sobre el contenido objetivo de los derechos fundamentales", en Aparicio, M. A. (coord.): *Derechos Constitucionales y Formas Políticas. Actas del Congreso sobre derechos constitucionales y Estado autonómico*, Cedecs, Barcelona, pp. 199-219; Alguacil González-Aurioles, J. (2006). "Objeto y contenido de los Derechos Fundamentales: presupuestos e implicaciones de una nueva diferenciación dogmática", en *Teoría y realidad constitucional*, núm. 18, pp. 305-320, en particular pp. 314 y ss. y de Gavara de Cara, J. C. (2007). "La vinculación positiva de los poderes públicos a los derechos fundamentales", *Teoría y realidad constitucional*, núm. 20, pp. 277-320.

[23] En palabras del Tribunal Constitucional Alemán (caso Lüth de 15 de enero de 1958, *BverfGE* 7, 198 (207)), los derechos fundamentales son normas objetivas que expresan un contenido que se irradia en todos los ámbitos del ordenamiento; este efecto de irradiación afecta las tres funciones del Estado: la conformación material de prescripciones de Derecho por el legislador o normador; a la actuación del ejecutivo en el ámbito de sus funciones, y a la interpretación y aplicación de prescripciones por parte del juez. Los poderes públicos tienen en su ámbito de actuación un deber de realización que implica en los más de los casos, un deber de actividad positiva de muy diversa índole.

[24] Milione, C. y Cárdenas Cordón, A. (2020). "Dignidad humana y derechos fundamentales", *Derechos y libertades*, núm. 42, pp. 233-265, en especial pp. 262-263. DOI: 10.14679/1159. Entre otros, recientemente, Masferrer A. (2022). *Dignidad y derechos humanos: un análisis retrospectivo de su formación en la tradición occidental*, Tirant lo Blanch. También, Chueca Rodríguez, R. L., (dir.) (2015). *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid.

derechos facilitan un lenguaje internacional común bajo la *lengua de los derechos*. Además, la dimensión axiológica de la dignidad y los derechos une la ética con el Derecho de la IA. Invocar la dignidad de la personalidad facilita dogmáticamente la actualización del contenido y garantías de los derechos existentes frente a tecnologías disruptivas, permitiendo el reconocimiento legal y especialmente jurisprudencial de nuevos contenidos y garantías de los derechos clásicos en el entorno digital. Igualmente, la dignidad y la dimensión objetiva de los derechos imponen un mandato de maximización de la eficacia de los derechos, lo que obliga a establecer garantías efectivas en el nuevo contexto de la IA, así como adoptar regulaciones y nuevos criterios jurisprudenciales. El enfoque jurídico de la dignidad y la dimensión objetiva de los derechos ayuda a superar la perspectiva individualista de los derechos subjetivos, dado que la IA y el big data afectan principalmente a la sociedad y a colectivos sin un impacto individual perceptible en los casos más significativos. También facilita legalmente la obligación de que todas las ramas del Derecho, incluyendo el Derecho de la competencia, integren entre sus objetivos la realización de los derechos. Asimismo, proporciona cobertura jurídica a la cláusula de progreso tecnológico como protegida por los derechos, así como a los objetivos sociales del uso de la IA, como la sostenibilidad y la IA para el bien común, adoptando formas jurídicas de prestación o subvención (por ejemplo, para la financiación del desarrollo de la IA o para compensar las desigualdades o impactos que genera, y para la educación e inclusión en IA).

Además, recurrir a estas categorías jurídicas proporciona garantías contra los riesgos que la IA supone para la sociedad, grupos y colectivos, y permite crear y regular respuestas y mecanismos de tutela efectivos, incluyendo acciones colectivas para la protección de intereses difusos o colectivos. La dimensión objetiva de los derechos también sirve de base para la creación de nuevas instituciones y organismos específicos de protección de los derechos fundamentales frente a la IA. También, el alcance jurídico de la dignidad es relevante para exigir que la IA no ponga en riesgo a futuras generaciones ni a la humanidad en general. La dignidad y la dimensión objetiva de los derechos justifican legalmente la intervención pública con políticas y regulaciones dirigidas al sector privado, tan relevante para la IA, así como fomentar la autorregulación y códigos de conducta para asegurar y efectivizar los derechos fundamentales desde los sectores industriales, tecnológicos y profesionales relacionados con la IA y el big data. La dimensión objetiva de los derechos en el contexto de la IA también justifica extender el modelo de extraterritorialidad en la aplicación del RGPD o, más recientemente, en el RIA.

Por último, la dignidad y la dimensión objetiva proporcionan protección contra la IA en el ámbito de la protección entre particulares, especialmente frente a las "big tech"[25]. Como señala Balaguer, "las grandes compañías tecnológicas que convierten en letra muerta gran parte de las previsiones constitucionales relativas a los derechos fundamentales de la persona"[26]. Recordemos que esta dimensión objetiva del derecho se configura como un elemento externo al contenido del derecho subjetivo, impulsando necesariamente una "política de derechos fundamentales" definida en líneas generales por el legislador en la regulación del ejercicio de los mismos, como indica Aláez[27] e inicialmente Otto[28].

3. CLAVES, DESAFÍOS Y DEFICIENCIAS DE LA PROTECCIÓN DE DATOS COMO RÉGIMEN GENERAL APLICABLE A LA IA

El Derecho de protección de datos ha sido clave para abordar la falta de regulación de tecnologías disruptivas, sustentado en los "principios", fundamentales según el art. 5 RGPD, que se han demostrado útiles y sólidos. Esto es aplicable a la IA, siempre que trate datos personales durante su ciclo de vida. Si es así y, en consecuencia, se ha de dar una aplicación integral y en bloque de estos principios y todo el régimen jurídico pertinente. Además, la IA a menudo realiza perfiles y toma decisiones automatizadas basadas en datos directos, observados o inferidos[29]. En tales casos, además, se aplican las garantías específicas

---

[25] En especial, Hoffmann-Riem, W.: *Big Data... cit.* También Quintiá Pastrana, A. (2019). "Reforma del derecho y revolución digital. Las garantías sociales en la economía de plataformas", en Puentes Cociña, B. y Quintiá Pastrana, A., (coords.): *El derecho ante la transformación digital: oportunidades, riesgos y garantías*, Atelier, pp. 105-126, p. 111, cita p. 112.

[26] Balaguer Callejón, F. (2020). "Crisis sanitaria y Derecho Constitucional en el contexto global", *Teoría y Realidad Constitucional*, núm. 46, pp. 121-140, p. 123. Antes, con más profundidad "Redes sociales, compañías tecnológicas y democracia", *Revista de Derecho Constitucional Europeo*, núm. 32, julio-diciembre de 2019. Sobre las limitaciones del Derecho constitucional en el ámbito tecnológico, también el ya mencionado Sánchez Barrilao, J. F. (2004). "El Derecho constitucional ... *cit*.

[27] Bastida, F. J. y otros: *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, capítulo 8 (B. Aláez Corral), pp. 182 y ss. https://www.unioviedo.es/constitucional/miemb/pdf/librodf.PDF

[28] Martín Retortillo, L. y de Otto Y Pardo, I. (1988). *Derechos fundamentales y Constitución*, Civitas, Madrid, pp. 163 y ss.

[29] Grupo del Artículo 29: *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 3 de octubre de 2017 y revisadas el 6 de febrero de 2018, pp. 7-8.

del artículo 22 RGPD de decisiones automatizadas. La ausencia de regulación específica para IA ha motivado que las autoridades de protección de datos hayan sido muy proactivas y hayan creado y derivado obligaciones detalladas de gobernanza, calidad de datos, protección contra la discriminación y sesgos algorítmicos, transparencia, explicabilidad de los algoritmos, minimización y limitación de datos, y ciberseguridad[30].

Sin embargo, aplicar el régimen de protección de datos a la IA conlleva dificultades estructurales. Es difícil mantener la finalidad de uso de los datos (art. 5.1.b RGPD), dado que continuamente los algoritmos descubren nuevas correlaciones, haciendo impredecibles los usos futuros de los datos. También es complejo establecer y cumplir con un plazo de conservación (art. 5.1.e RGPD) debido a las investigaciones continuas. El principio de minimización de datos (art. 5.1.c RGPD) contrasta con la necesidad general de grandes volúmenes de datos para investigaciones de calidad[31]. Además, por cuanto, a la legitimación, obtener el consentimiento informado y cumplir con las obligaciones de transparencia e información (arts. 5.1.a y 14.5.b RGPD) son retos significativos. Y como se analiza al final del estudio, el legislador no está cumpliendo su función de legitimar y regular con garantías el impacto y restricciones que implica la IA.

Además de estas dificultades estructurales, entre las cuestiones clave, Jaume[32], Floridi y el grupo de Tilburg[33] y con profundidad Castillo[34], abordan especialmente la "privacidad de grupo en la era de los datos". La IA forma grupos por afinidades, a menudo sin el conocimiento de los individuos afectados. Aunque

---

[30] En especial, AEPD: *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, en especial, pp. 30-48 y, con más claridad en AEPD: Requisitos para Auditorías de Tratamientos que incluyan IA, 2021.

[31] Recuero Linares, M. (2019). *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*, Premio AEPD, pp. 21 y ss. https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf

[32] Jaume Palasí, L. "Cómo la inteligencia artificial..." *cit*. p. 28.

[33] En particular, Kammourieh, L. y otros. "Group privacy in the age of big data", en Taylor. L.; Van der Sloot, B.; Floridi, L. (eds.). *Group Privacy... cit.* Capítulo 3, pp. 48-83, ver p. 54. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

[34] Castillo Parrilla, J. A. (2023). "Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial", *Derecho Privado y Constitución*, núm. 43, pp. 53-88, doi: https://doi.org/10.18042/cepc/dpc.43.02

la AEPD sugiere que estos casos carecen de protección legal[35], entiendo que habrá un tratamiento de datos personales en el momento que desprenden efectos y se aplican a una persona concreta, por lo que será aplicable la normativa. Además, el uso de datos proxies puede eludir las garantías para datos especialmente protegidos (art. 9 RGPD), infiriendo características como orientación sexual o salud a partir de datos no protegidos específicamente. la IA infiere fácilmente orientación sexual, posición política, salud, etc. a partir de datos de geolocalización, consumo, hábitos, etc. En consecuencia, hay que atender más a los resultados y datos inferidos que a los datos que se utilizan y vigilar y analizar posibles "enmascaramientos" y la elección intencional de factores cerca de los prohibidos o de datos afines a los especialmente protegidos[36]. Apunta Van der Sloot que hoy día basar la protección jurídica en la naturaleza de los datos "no es la mejor manera de avanzar"[37].

Y quizá la cuestión más importante: la IA genera datos de salida, datos inferidos que pueden revelar información personal de manera indirecta o detallada[38]. Por lo general, de estos datos no se tiene conocimiento por el interesado al tiempo que pueden fluir a terceros. Aunque estos datos no son proporcionados directamente por los usuarios, han de considerarse como personales, pues obviamente son relativos a personas identificables. Sin duda alguna así es para el Grupo del Artículo son datos personales[39]. Sin embargo, el RGPD se centra más en los datos de entrada[40] y el TJUE no es tan claro que respecto de estos datos

---

[35] AEPD (2020). *Privacidad de grupo*, 19 de octubre. https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

[36] Entre otros, Terry Nicolas, "Big Data Proxies and Health Privacy Exceptionalism", en *Health Matrix* núm. 24, pp. 65-108, 2014. Sobre el enmascaramiento de datos especialmente prohibidos, Barocas, S. y Selbst, A. D. (2016). *Big Data's Disparate Impact*, 104 *CAL. L. REV.* 671, 692-93.

[37] Van der Sloot, B. "Regulating non-personal data in the age of Big Data", en Tzanou, M. (Ed.): *Health data privacy under the GDPR: Big Data challenges and regulatory responses,* Routledge pp. 85-105; p. 16 de la versión SSRN.

[38] Sobre el tema, Palma Ortigosa, A. (2022). *Decisiones automatizadas y protección de datos personales. Especial atención a los sistemas de inteligencia artificial*, Dykinson. Sobre la noción, Wachter, S. y Mittelstadt, B. D. (2019). "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, Vol. 2019, núm. 2, 2019, pp. 494-620, p. 2. https://ssrn.com/abstract=3248829

[39] Grupo del Artículo 29, *Directrices sobre decisiones... cit*. p. 10.

[40] Soriano Arnanz, A. *Decisiones automatizadas... cit*.

inferidos pueda ejercerse el derecho de acceso o rectificación[41]. Sería necesaria una regulación o criterios interpretativos de las autoridades regulatorias o judiciales al respecto.

Otra cuestión clave que requiere claridad es el alcance y las garantías del artículo 22 RGPD sobre decisiones sólo automatizadas[42]. A este respecto, hay que tener en cuenta la muy valiosa posición del Grupo del Artículo 29[43] desde hace años o la doctrina[44]. La reciente STJUE del 7 de diciembre de 2023 (caso SCHUFA c. Alemania) que he analizado[45] extiende las obligaciones de este artículo a los terceros encargados que hacen el tratamiento automatizado para el responsable. También, brinda las garantías del artículo 22 RGPD a supuestos en los que la decisión (sólo automatizada materialmente) formalmente parece humana o es adoptada por otro sujeto. Se trata de criterios interpretativos claramente proyectables para el uso de IA.

Tras exponer estas dificultades estructurales o cuestiones clave sobre la proyección del RGPD a sistemas IA, cabe afirmar que la convivencia del RGPD y el RIA van a convivir y por mucho tiempo, y hay que señalar que no resulta nada

---

[41] Así, no consideró que procediera reconocer estos derechos respecto de un análisis jurídico que se había realizado sobre un permiso de residencia; STJUE de 17 de julio de 2014, asuntos acumulados, C-141/12 y C-372/12, caso YS. y M. y S. (ver apartados 45 y 48). En cambio, respecto de los datos de evaluación de un examen sí que considero que sí que procedía el acceso, pero la rectificación no amparaba, obviamente, a rectificar a posteriori las respuestas incorrectas. STJUE de 20 de diciembre de 2017, asunto, C-434/16, caso Nowak, apartados 43, 44, 52 y 54.

[42] Así como regulaciones afines como el artículo 11 de la Directiva (UE) 2016/680 o el nuevo artículo 9. 1º Convenio 108 del Consejo de Europa que reconoció en 2018 también este "derecho".

[43] En especial hay que tener en cuenta Grupo del Artículo 29, *Directrices sobre decisiones individuales...cit.*

[44] Palma Ortigosa, A.: *Decisiones automatizadas... cit. y* Roig I Batalla, A. (2021). *Las garantías frente a las decisiones automatizadas del Reglamento general de Protección de Datos a la gobernanza algorítmica*, J.M. Bosch, Barcelona. He analizado en particular este precepto en "Derechos y garantías ante el uso público y privado de inteligencia artificial, robótica y big data", en Bauzá, M. (dir.) (2019). *El Derecho de las TIC en Iberoamérica*, FIADI, La Ley-Thompson-Reuters, Montevideo, pp. 917-952, acceso en http://links.uv.es/BmO8AU7.

[45] He realizado el primer estudio de la misma en "La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial", *Diario La Ley*, enero de 2024. https://ir.uv.es/V14YNLl

sencillo ni superponer las dos normas, ni gestionar el cumplimiento conjunto de las mismas[46].

4. LA ACELERACIÓN DE LA REGULACIÓN Y EL CONVENIO EUROPEO DE IA

La regulación de la IA ha estado en la agenda de la UE desde 2016, inicialmente con documentos de *soft law*[47] y más notablemente con el Libro Blanco de la IA[48] en 2020. Este esfuerzo continuó con la propuesta del RIA en 2021 que culminó con un acuerdo político el 9 de diciembre de 2023 y su aprobación en 2024. Este proceso ha incentivado el interés regulatorio de la IA globalmente. Por ejemplo, el 16 de junio de 2022, Canadá presentó la *Digital Charter Implementation Act*[49] de 2022 dentro de la *Artificial Intelligence and Data Act*, "AIDA"[50]. En diciembre de 2022, Brasil comenzó a tramitar el proyecto de ley núm. 2338 en el Senado para regular la IA[51], mientras que el Reino Unido ha adoptado un enfoque de regulación más laxo post-Brexit[52].

---

[46] Puede seguirse el régimen superpuesto de ambos regímenes en mi estudio "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en Balaguer, F. y Cotino, L. *Derecho público de la inteligencia artificial... cit.*

[47] Se sigue la evolución en "Ética en el diseño..." *cit.*

[48] *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza,* COM(2020) 65 final, Bruselas, 19.2.2020, https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

[49] https://www.parl.ca/legisinfo/en/bill/44-1/c-27

[50] El texto en https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading El estado de tramitación en https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act y https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

[51] *Projeto de lei nº 2338 do Senado, que regulamenta a IA*, texto inicial en https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1702407086098&disposition=inline&_gl=1*1ifop8*_ga*MTg0Njk3ODg3MS4xNzA1Mzk4MDU2*_ga_CW3ZH25XMK*MTcwNTM5ODA1Ni4xLjAuMTcwNTM5ODA1Ni4wLjAuMA. Procedimiento en https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

[52] Así, destaca Gobierno de Reino Unido: *A pro-innovation approach to AI regulation*, Department for Science, Innovation and Technology and Office for Artificial Intelligence, 29 de marzo 2023, actualización 3 de agosto. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

La aparición de tecnologías como ChatGPT a finales de 2022 aceleró estos desarrollos. Destacan, por ejemplo, las "Medidas provisionales para la gestión de servicios de IA generativa" en China, implementadas el 13 de julio de 2023[53]. Canadá anunció en septiembre de 2023 el "Código de Conducta Voluntario para el Desarrollo y Gestión Responsable de Sistemas Generativos Avanzados de IA"[54]. Desde el G7, destacó el "Proceso de Hiroshima", culminando en el "Código Internacional de Conducta para el Desarrollo de Sistemas Avanzados de IA" el 30 de octubre de 2023[55]. El mismo día Estados Unidos adoptó la importante Orden ejecutiva sobre el desarrollo y la utilización seguros y fiables de la inteligencia artificial, de 30 de octubre de 2023[56]. Con carácter más parcial, el 3 de enero de 2024 California ha regulado su *Artificial Intelligence Accountability Act*[57] o Illinois cuenta con su *Artificial Intelligence Video Interview Act* (820 ILCS 42/)[58]. En Iberoamérica existen múltiples propuestas legislativas[59].

Además del RIA, hay que prestar atención al nuevo Convenio IA del Consejo de Europa, ambos de 2024 sobre el cual he tenido ocasión de hacer el primer estudio[60]. Su elaboración comenzó con el Comité Ad hoc sobre IA

---

[53] http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

[54] Lanzado por el Ministro de Innovación, Ciencia e Industria: *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems.* https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

[55] https://www.mofa.go.jp/files/100573473.pdf

[56] *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. Cabe seguir también la nota informativa https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

[57] California Senate Bill 896, https://legiscan.com/CA/text/SB896/id/2868456

[58] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68#:~:text=An%20employer%20may%20not%20use,use%20of%20artificial%20intelligence%20analysis

[59] Existen propuestas normativas de legisladores particulares y otras vinculadas a estrategias nacionales en la materia como en Perú, Chile, Colombia, por mencionar algunos.

[60] Cabe seguir mi estudio, "The Council of Europe's Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law", en *CERIDAP Journal*, Issue núm. 2/2024, https://ceridap.eu/en/issues/ En español, "El Convenio sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho del Consejo de Europa", *Revista Administración &*

(CAHAI) en septiembre de 2019. El Comité de Ministros instauró el Comité Ad hoc sobre Inteligencia Artificial (CAHAI)[61] el 11 de septiembre de 2019. Posteriormente, se otorgó un mandato al Comité sobre Inteligencia Artificial (CAI) desde enero de 2022 hasta diciembre de 2024[62], con unos "Términos de Referencia del CAI"[63] para crear un "instrumento jurídico vinculante de carácter transversal" [64] que promueva la innovación y establezca principios "sólidos y claros" para el diseño, desarrollo y aplicación de sistemas de IA en relación con los derechos humanos, la democracia y el Estado de Derecho"[65]. Hubo un "Borrador Cero" de 6 de enero 2023[66], un Borrador consolidado de 7 de julio de 2023[67], un Proyecto base de 18 de diciembre de 2023[68] y Finalmente el Convenio fue adoptado el 17 de mayo de 2024 en la 133ª Sesión del Comité de Ministros (Estrasburgo, 17 de mayo de 2024). El Convenio figura como el núm. 225 de las series de tratados y se abre a la firma el 5 de septiembre de 2024 durante la Conferencia de Ministros de Justicia en Vilnius[69].

Cidadanía, EGAP, 2024, actualizado en https://papers.ssrn.com/sol3/Delivery.cfm/4942383.pdf?abstractid=4942383&mirid=1

También, Ziller, J.: "El Convenio del Consejo de Europa de Inteligencia Artificial frente al Reglamento de la Unión Europea: dos instrumentos jurídicos muy diversos", en Cotino Hueso, L. y Simó Castellanos, P. (coords.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, 2024.

[61] Así, en la 353.ª reunión del Comité de Ministros, Decisión CM/Del/Dec(2019)1353/1.5, 11 de septiembre de 2019.

[62] https://www.coe.int/en/web/artificial-intelligence/cai

[63] Mandato de Comité ad hoc (CM(2021)131-addfinal), *Terms of reference.* https://rm.coe.int/terms-of-reference-of-the-committee-on-artificial-intelligence-for-202/1680a74d2f

[64] Puede seguirse al respecto, entre otros, https://dig.watch/processes/convention-on-ai-and-human-rights-council-of-europe-process. También, ver https://www.law.kuleuven.be/citip/blog/the-council-of-europes-road-towards-an-ai-convention-taking-stock/

[65] Parte II y III. 11. CAHAI, *Possible elements... cit.*

[66] CAI, *Revised zero draft [framework] convention on artificial intelligence, human rights, democracy and the rule of law*, Estrasburgo, 6 de enero 2023. https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

[67] CAI, *Consolidated Working Draft of the Framework Convention*, Estrasburgo, 7 de julio 2023. https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66

[68] CAI, *Consolidated working draft*, 18 de diciembre de 2023. https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043

[69] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680aee411

Este Convenio es extenso y comprende diecisiete considerandos y treinta y seis artículos distribuidos en ocho capítulos[70]. Representa un esfuerzo significativo para armonizar y establecer un marco común mínimo para Europa, orientado hacia una ambición mundial centrada en los derechos humanos, la democracia y el Estado de Derecho, más que en la economía y el mercado. Europa aspira a posicionarse como un *faro luminoso* y una piedra angular en el paisaje normativo de la IA, no solo para el continente sino también a nivel global. Para los Estados no miembros de la UE, el Convenio de IA puede desempeñar un papel normativo y jurídico importante. Para la UE y sus Estados miembros que ratifiquen el Convenio, este tiene el potencial de complementar y hasta elevar y fortalecer la protección de los derechos. Cabe destacar que, a diferencia del RIA, el Convenio de IA no se limita a los sistemas de IA de alto riesgo. Además, para las partes que lo ratifiquen, sirve para integrar en el ámbito jurídico y normativo como "principios" aquello que hasta ahora no eran más que principios éticos consensuados de la IA. Estos principios jurídicos poseen un gran potencial en manos de los operadores jurídicos para derivar normas y obligaciones concretas, continuando la tradición de las últimas décadas en los principios de protección de datos. Además, el Convenio de IA otorga a los sujetos afectados por la IA ciertos derechos y garantías, y establece mecanismos para la defensa de estos derechos ante autoridades que han de ser independientes. Es especialmente relevante el enfoque basado en el riesgo del Convenio de IA, particularmente en su artículo 16, que exige una evaluación y mitigación continuas de los riesgos e impactos adversos de cualquier tipo de sistema de IA.

Así pues, el Convenio IA puede complementar al RIA de la UE. Más allá de esta perspectiva, el valor del Convenio va más allá. Si se me permite, *el Convenio pone la lírica a la prosa que supone el RIA*. El RIA establece las bases y estructuras de un ecosistema de IA seguro y confiable, el Convenio centra en su impacto en las personas y la sociedad democrática. El RIA es metódico, detallado y preciso, trazando un camino claro a través de la complejidad técnica y jurídica, estableciendo estándares firmes y obligaciones concretas para los proveedores y usuarios o implantadores de sistemas de IA. En contraste, el Convenio introduce la lírica,

---

[70] Un Preámbulo con diecisiete Considerandos y treinta y seis artículos estructurados en ocho capítulos: Disposiciones generales (I); Obligaciones generales (II); Principios (III); Recursos (IV); Evaluación y Mitigación de Riesgos e Impactos adversos (V) y los relativos a Aplicación (VI); Mecanismo de seguimiento y cooperación (VII) y Cláusulas finales (VIII).

se eleva para integrar normativamente los valores fundamentales, los principios éticos y los derechos humanos que deben guiar la evolución de la IA. El Convenio no sólo tiene un valor simbólico y metajurídico, sino que es un instrumento normativo, con capacidad de integración casi constitucional en los ordenamientos jurídicos de los Estados parte y cuenta con gran potencial interpretativo. Es por ello que el Convenio IA supera a decenas de instrumentos declarativos y de *soft law* que ya resultaban superfluos, inocuos e incluso tediosos. Obviamente habrá que estar a su proceso final de aprobación, ratificación y el despliegue de sus efectos.

5. MÁS ALLÁ DE LA RETÓRICA: LA RELEVANCIA DE LOS PRINCIPIOS JURÍDICOS EN LA IA

Desde hace años, entre decenas de declaraciones y documentos, se han ido visibilizando y destilando unos principios éticos esenciales de la IA. Desde Harvard se analizaron más de treinta de las principales declaraciones internacionales y corporativas de ética de la IA y se sintetizaron en privacidad, rendición de cuentas, seguridad, transparencia y explicabilidad, equidad y no discriminación, control humano, responsabilidad profesional, valores humanos y sostenibilidad. Hoy por hoy están más que consensuados toda una serie de principios que se proclaman en códigos, declaraciones y otros instrumentos no normativos. Considero que es necesario pasar ya –si se me permite– de las *musas* de la ética al *teatro* del Derecho. Y en este sentido, hay que destacar el interés jurídico de los principios. Como es sabido, los principios desempeñan un papel esencial en la configuración y estructuración del ordenamiento jurídico, informan el ordenamiento y son herramientas clave para interpretación y aplicación de las normas, son fuente de inspiración para resolver conflictos y derivar nuevas interpretaciones. Y ello tiene particular relevancia en sectores digitales y disruptivos, donde se da una considerable incertidumbre, como es el caso de la IA. Además, no olvidemos que en un ámbito tan relacionado como el de la protección de datos, durante más de treinta años, los "principios" (art. 5 RGPD) han desempeñado y continúan desempeñando estas funciones generales, siendo los pilares fundamentales. Es más, los "principios" de la protección de datos han constituido reglas concretas aplicables a los tratamientos. Tan es así que su mero incumplimiento directamente implica la comisión de infracciones.

En el caso del RIA de la UE finalmente no se han regulado unos principios en el articulado y su proclamación ha quedado limitada a un Considerando. No había principios ni en la propuesta de la Comisión de 2021 ni en el texto

del Consejo de diciembre de 2022. Sin embargo, el Parlamento de la UE en junio de 2023 (Enmienda 213) incluyó en un nuevo artículo 4 bis los "Principios generales aplicables a todos los sistemas de IA" con cierto detalle: a) "intervención y vigilancia humanas"; b) "solidez y seguridad técnicas"; c) "privacidad y gobernanza de datos"; d) "transparencia"; e) "diversidad, no discriminación y equidad"; y f) "bienestar social y medioambiental". Estos principios alcanzaban a todo sistema IA –de alto riesgo o no– y también a los modelos fundacionales. Hay que decir que esta versión del Parlamento regulaba estos principios, pero "sin crear nuevas obligaciones" (art. 4 bis. 2º), aunque sí que debían inspirar los procesos de normalización y las orientaciones técnicas (art. 4 bis. 2º). Finalmente, sólo se afirman en el Considerando 14 bis pero expresamente dejándolos fuera de "los requisitos jurídicamente vinculantes del presente Reglamento".

Así las cosas, cabe subrayar la importancia que puede tener la inclusión de los principios en el Convenio IA. Y es que, pese a que la regulación de este convenio es flexible y abierta, caracterizada por mandatos amplios o remisiones a la normativa existente, la inclusión de los principios tiene una potencialidad normativa importante, especialmente por cuanto el RIA no los ha regulado finalmente y en manos de los operadores jurídicos nacionales pueden tener un importante potencial.

Desde hace años, entre decenas de declaraciones y documentos, se han ido visibilizando y destilando principios éticos esenciales de la IA[71]. A través de más de treinta declaraciones internacionales y corporativas analizadas en Harvard[72], los ordena desde la privacidad, rendición de cuentas, seguridad, transparencia y explicabilidad, equidad y no discriminación, control humano, responsabilidad profesional, valores humanos y sostenibilidad. Estos principios, ahora ampliamente consensuados, se proclaman en numerosos códigos, declaraciones y otros

---

[71] La Declaración del Parlamento de la UE de 2017 sobre robótica es una clara manifestación de estos principios. Destacan sin duda las Directrices éticas para una IA fiable desde la UE, la Recomendación del Consejo sobre Inteligencia Artificial de la OCDE del 22 de mayo de 2019 y la Recomendación sobre la ética de la inteligencia artificial de la UNESCO de noviembre de 2021. Ya en 2018, el proyecto *AI4People contabilizó 47 principios éticos proclamados internacionalmente y los destiló en cinco puntos: beneficencia ("hacer el bien"), no maleficencia ("no hacer daño"), autonomía o acción humana ("human agency") ("respeto por la autodeterminación y elección de los individuos") y justicia ("Trato justo y equitativo para todos").*

[72] Fjeld, J. y otros (2020). "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI", Berkman Klein Center for Internet & Society Research at Harvard University, enero. https://dash.harvard.edu/handle/1/42160420

instrumentos no normativos. Considero que es necesario pasar ya –si se me permite– de las *musas* de la ética al *teatro* del Derecho. Los principios desempeñan un papel esencial en la configuración del ordenamiento jurídico, informando y sirviendo como herramientas clave para la interpretación y aplicación de las normas, además de ser fuente de inspiración para resolver conflictos y derivar nuevas interpretaciones. Esta función es especialmente relevante en sectores disruptivos como la IA. Además, en el ámbito de la protección de datos, los "principios" (art. 5 RGPD) han sido fundamentales durante más de treinta años, constituyendo reglas concretas cuyo incumplimiento implica directamente la comisión de infracciones.

Aunque la regulación es flexible, tienen un gran potencial interpretativo para operadores jurídicos nacionales siendo, además, que el RIA no los ha regulado. Así, cada "Parte adoptará o mantendrá medidas para garantizar" los principios establecidos en el Capítulo III, aplicables de manera adecuada al ordenamiento jurídico interno. Estos principios abarcan desde la dignidad humana y autonomía individual hasta la fiabilidad y confianza, destacando obligaciones específicas como la detección y transparencia del contenido generado por sistemas de IA. En el mismo los principios se integran bajo la fórmula de que cada "Parte adoptará o mantendrá medidas para garantizar" los principios que "establece" en el Capítulo III "principios generales comunes que cada Parte deberá aplicar [...] de manera adecuada a su ordenamiento jurídico interno" (como "nota explicativa"). Ocho artículos (arts. 6 a 13) expresan y afirman tales "principios": dignidad humana y autonomía individual (art. 6), transparencia y supervisión (art. 7), rendición de cuentas y responsabilidad (art. 8), igualdad y no discriminación (art. 9), privacidad y protección de datos personales (art. 10), preservación de la salud [y del medio ambiente] (art. 11), fiabilidad y confianza (art. 12), innovación segura (art. 13). Son pocos los elementos normativos más específicos como la obligación de la "detección y transparencia del contenido generado por sistemas de inteligencia artificial" (art. 7); la mención de "estándares y marcos nacionales e internacionales aplicables en materia de protección de datos personales y [gobernanza de datos]" (art. 10)[73] o de "la seguridad, la protección, la exactitud, el rendimiento, la calidad [...] requisitos de integridad, seguridad de los datos, gobernanza, ciberseguridad y solidez" (art. 12). Destaca

[73] El SEPD, *Opinion 20/2022... cit.* recomienda una referencia explícita al cumplimiento de la normativa UE (3.3) y que haya un enfoque de protección de datos desde el diseño y por defecto (apartado 6, p. 13 y ss., núm. 36 y ss.).

que se "anime" (*encouraged*) a las partes a "fomentar la innovación" y, para ello, "el establecimiento de] [un] entorno[s] [reglamentario] controlado[s] para [el desarrollo y la experimentación] / [pruebas]" (art. 13).

6. ¿NUEVOS DERECHOS EN LA ERA DE LA IA? CARTA DE DERECHOS DIGITALES, CONVENIO IA Y EL RIA

Desde hace décadas, en el contexto de los denominados derechos de cuarta o última generación, se pretende dar respuestas a los continuos desafíos que plantea la sociedad postindustrial y digital[74]. Van cristalizando o se van afirmando nuevos "derechos digitales"[75]. Expresión de ello es la Carta de Derechos Digitales de España, de 2021, y sus proyecciones en la Unión Europea e Iberoamérica, como la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01), de 15 de diciembre de 2022[76] o la Carta Iberoamericana de Principios y Derechos en Entornos Digitales, de 25 de marzo de 2023[77].

De la Carta de Derechos Digitales y la Inteligencia Artificial, destaco los derechos relacionados con la actuación administrativa (artículo XVIII.6º)[78], pues incluye innovaciones y concreciones que deberían inspirar al legislador nacional

---

[74] Bustamante Domas, J. (2001). "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica". *Revista Interamericana de Ciencia, Tecnología, Sociedad e Innovación* (septiembre / diciembre) y Riofrío Martínez-Villalba, J. C. (2014). "La cuarta ola de derechos humanos: los derechos digitales". *Revista Latinoamericana de Derechos Humanos* Volumen 25 (1), I Semestre, pp. 15-45.

[75] Entre otros, Rallo Lombarte, A. "Una nueva generación de derechos digitales", *Revista de Estudios Políticos*, núm. 187, pp. 101-135. https://doi.org/10.18042/cepc/rep.187.04. O mi trabajo "La necesaria actualización de los derechos fundamentales como derechos digitales ante el desarrollo de internet y las nuevas tecnologías", en AA. VV. (2028). *España constitucional (1978-2018). Trayectorias y perspectivas*, Vol. III, CEPC, Madrid, pp. 2347-2361. Acceso en www.cotino.es

[76] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)

[77] Aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. https://www.segib.org/wp-content/uploads/Carta_iberoamericana_derechos_digitales_ESP_web.pdf.

Sobre la misma, Costa, J., Ávila, R. y Fernández Aller, C. (2023). *Derechos digitales en Iberoamérica: situación y perspectivas*, Fundación Carolina y Telefónica. https://www.fundacioncarolina.es/wp-content/uploads/2023/03/DERECHOS-DIGITALES_FC-2.pdf

[78] Puede seguirse mi estudio, "Derechos ante la administración digital y la inteligencia artificial (XVIII Y XV)", en Cotino Hueso, L. (editor). *La Carta de Derechos Digitales*, cit..., pp. 251-284. Acceso.

prontamente, tal como lo evidencia el artículo 25.1º de la Ley 15/2022, de 12 de julio. El tratamiento de la IA en el apartado XXV recuerda la centralidad de la persona, su dignidad, el bien común y el principio de no maleficencia (1º). Se proclaman una serie de mandatos "en el desarrollo y ciclo de vida de los sistemas" "no discriminación", "transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza" y que deberá "garantizarse la accesibilidad, usabilidad y fiabilidad" (2º). Finalmente, se proyecta en la IA el artículo 22 RGPD sobre "decisiones automatizadas", si bien, ampliando su aplicación más allá de las decisiones "únicamente" automatizadas, reconociendo el derecho a la revisión humana ex post y a impugnarlas (3º). La IA también se destaca en los "Derechos en el ámbito laboral" (artículo XIX), la salud (artículo XXIII) y las neurotecnologías (artículo XV).

Hay que explorar las capacidades interpretativas de los derechos existentes antes de dejarse llevar por la tentación del reconocimiento de nuevos derechos[79], siempre atractivo, algo siempre atractivo. Acudir a derechos preexistentes facilita contar con las garantías que ya gozan. Sin embargo, el reconocimiento de nuevos derechos también tiene un impacto simbólico y pedagógico significativo. Ya sean derechos nuevos o la expansión de los existentes, es vital la precisión en la definición de nuevas facultades y garantías, y el establecimiento de mecanismos efectivos para su protección.

Hay que evitar las deficiencias como las observadas en la Ley Orgánica 3/2018, cuyos derechos digitales[80], a pesar de su reconocimiento legal, carecen de efecto práctico. El Convenio IA y el RIA destacan por su enfoque en los derechos, aunque generalmente no establecen nuevos derechos subjetivos, con más de cuarenta referencias a "derechos humanos" ya reconocidos".

---

[79] En general, sobre nuevos derechos en razón de nuevas necesidades y amenazas, Escobar Roca, G.: *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid, 2018, en especial pp. 99 y ss. Asimismo, Masferrer, A. (2017). "Derechos de nueva generación", en Enríquez, J. M., *Derechos humanos: un análisis multidisciplinar de su teoría y praxis*, pp. 331-358.

[80] Al respecto cabe remitir al análisis sistemático y por artículos en Rodríguez Ayuso, J. F. (coord.) (2023). *Retos, desafíos y oportunidades en materia de derechos digitales en un contexto de pandemia: visión multidisciplinar*, Thompson-Reuters Aranzadi, Cizur Menor; y Troncoso Reigada, A. (dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales*.

Es fundamental destacar la regulación de derechos y en su caso nuevos derechos en el Convenio IA y el RIA. A pesar de que se menciona que uno de los "aspectos clave" del Convenio IA es su enfoque en los derechos[81], en términos generales, no establece nuevos derechos subjetivos. Existen más de cuarenta referencias a los "derechos humanos" o a "derechos", pero ya reconocidos anteriormente. También se incluyen menciones específicas a la "igualdad y no discriminación" (arts. 9 y 17), la "privacidad y protección de datos" (art. 10) y los "derechos de las personas con discapacidad y de los niños" (art. 18), pero sin regular ningún contenido sustantivo ni establecer nuevos derechos. Como excepción, si pueden considerarse como derechos específicos en el Convenio IA algunas obligaciones de documentación, registros y otras medidas para garantizar los "recursos" efectivos del artículo 14, así como las garantías de supervisión y notificación del artículo 15, como a continuación se expone.

Respecto de los "Recursos" del artículo 14 del Convenio IA, ya en 2014 en EE. UU., Crawford y Shultz introdujeron el "data due process" para redefinir las garantías del debido proceso en el contexto de las decisiones algorítmicas. Este nuevo derecho incluye la garantía de que se proporcione a los afectados información mínima sobre lo que predijo el algoritmo, con qué datos y la metodología utilizada. [82] Siguiendo esta línea, el artículo 14 obliga a los Estados a "adoptar medidas" que garanticen recursos efectivos. Se asegura la generación de documentación, registros y evidencias accesibles para los afectados. Se enfatiza que "los sistemas de inteligencia artificial [...] estén adecuadamente documentados, y que se facilite información pertinente sobre el uso [...] operaciones realizadas [...] y que esta información se registre, se facilite a los organismos autorizados conforme a su Derecho interno para acceder a esta información y, cuando proceda y sea aplicable, se ponga a disposición o se comunique a las personas afectadas" (art. 14 a). Además, esta información debe ser "suficiente y proporcionada para que las personas afectadas impugnen" (artículo 14 b). Esta obligación a las partes de regular expresamente garantías es del todo positiva. Sin embargo, estas

---

[81] Así, Brandusescu, A. y Sieber, R. (2023). "*omments on Preliminary Discussions with the Government of Canada on Council of Europe Treaty Negotiations on Artificial Intelligence* (31 de agosto). https://ssrn.com/abstract=4559139. p. 3 sobre los "Mecanismos de derechos" (*Rights mechanisms).*

[82] Crawford, K. y Schultz, J. (2014). *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV., p. 125.

obligaciones no deberían generalizarse a todos los sistemas de IA, considero que procede una interpretación restrictiva de la referencia del artículo 14 a sistemas que puedan "afectar significativamente" ("significantly affecting") a los derechos humanos[83].

Asimismo, el artículo 15 regula las "Garantías procesales" ("Procedural safeguards"). Su primer apartado destaca "la importancia de la revisión humana" y la necesidad de garantías efectivas en casos en los que un sistema de IA "informe o adopte decisiones o actos que afecten sustancialmente a los derechos humanos" (art. 15. 1º). Aunque la formulación podría ser más precisa, el artículo 15 establece claras conexiones con las garantías reconocidas por el Derecho europeo para decisiones automatizadas. Además, estas garantías no se limitan a decisiones "basadas únicamente en el tratamiento automatizado", sino que se extienden también a decisiones influenciadas significativamente por sistemas de IA. Esta aproximación es coherente con la reciente decisión del TJUE en diciembre de 2023 sobre la Carta de derechos que se ha expuesto. Aunque no es posible detallar en este momento, en la versión final del RIA, se consideran de alto riesgo aquellos sistemas que puedan "influir sustancialmente en el resultado de la toma de decisiones" (art. 6.3 RIA), incluyendo criterios bien definidos.

El artículo 15.2º del Convenio IA introduce la obligación, y potencialmente el derecho, a la "notificación", especificando que "se notificará a las personas que interactúan con un sistema de inteligencia artificial y no con un ser humano". Desde 2018 en la UE, el HLEG incluyó en la transparencia el derecho a la "comunicación", esencialmente como "derecho a saber que [las personas] están interactuando con un sistema de IA" (núm. 78). El artículo 52 del RIA contempla esta notificación entre las "Obligaciones de transparencia para determinados sistemas de IA". Así, el artículo 15 del Convenio IA parece alinearse con el *soft law* internacional, donde la comunicación se divide en un derecho u obligación

[83] No son de alto riesgo los sistemas IA para: a) "una tarea procedimental limitada"; b) si el sistema de IA "pretende mejorar el resultado de una actividad humana realizada previamente"; y c) tampoco es de alto riesgo si el sistema detecta patrones o desviaciones de patrones "y no está destinado a sustituir o influir en la evaluación humana previamente completada, sin la debida revisión humana". Finalmente, no se aplican las garantías de alto riesgo del RIA si el sistema está "destinado a realizar una tarea preparatoria de una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III" (art. 6. 2 bis RIA).

a la "notificación cuando se interactúa con un sistema de IA"[84] y en las garantías frente a decisiones automatizadas del artículo 15.1º.

Finalmente, respecto del Convenio IA, en el contexto de los recursos efectivos, el artículo 13 CEDH reconoce el derecho a un recurso interno efectivo ante una instancia nacional para garantizar los derechos del propio CEDH (y no otros)[85]. Este recurso debe permitir que una autoridad independiente, no necesariamente judicial, examine el fondo de la petición y, si procede, otorgue la reparación adecuada[86]. En esta línea, el artículo 15 del Convenio IA sobre "Recursos" en su apartado 3º prevé que se regule "una posibilidad efectiva para las personas afectadas de presentar una reclamación [ante las autoridades públicas, incluido, en su caso,] ante el mecanismo de supervisión a que se refiere el artículo 26, conforme a su Derecho interno]" [87]. Y como luego se analiza, debe tratarse de una autoridad independiente.

En relación con el reconocimiento de nuevos derechos en el RIA de la UE, es importante reconocer que se dirige a fabricantes (proveedores) e implantadores de productos de IA. Ha sido criticado por ignorar completamente a los afectados por un sistema de IA, que ni siquiera se mencionan[88]. Respecto al reconocimiento de derechos, desde las enmiendas 628 y 629 de junio de 2023 se propuso la inclusión de algunos derechos, y finalmente, se expresa el derecho a presentar una reclamación ante una autoridad de vigilancia del mercado y el derecho a explicación de decisiones tomadas individualmente en los artículos 85-87. Cabe señalar que el texto finalmente aprobado diluye la propuesta del

---

[84] Así, cabe seguir el ya referido estudio de Harvard, Fjeld y otros: "Principled Artificial Intelligence... cit.

[85] Consejo de Europa (2001). *Guide on Article 13 of the European Convention on Human Rights. Right to an effective remedy*, actualizado el 31 de agosto. https://ks.echr.coe.int/web/echr-ks/article-13

[86] La sentencia TEDH, de 3 de abril de 2001, Keenan contra Reino Unido, párr. 122 resume el contenido de este precepto.

[87] En la versión de 18 de diciembre se señala la letra c) como posibilidad (en color rojo).

[88] Hasta junio de 2023 no se incluyó entre las definiciones la de "persona afectada", junto con diversos derechos en las enmiendas del Parlamento (Enmienda 174, art. 3. 1º, 8 bis). Las "personas afectadas" finalmente no se definen, pero sí que forman parte del "alcance" del artículo 2.1.g) RIA "personas afectadas que estén establecidas en la Unión".

Parlamento. Como señala López-Tarruella[89], queda más bien en el ámbito de las buenas intenciones. Así, en cuanto al derecho a presentar una reclamación, a diferencia del derecho reconocido en el artículo 77 del RGPD, el RIA regula un derecho a presentar una petición ante la autoridad de vigilancia del mercado que se tendrá en cuenta para adoptar acciones o investigaciones. Además, como señala este autor, estas peticiones se verán obstaculizadas por la compleja distribución de competencias entre las autoridades de vigilancia del mercado que se deriva del artículo 74 del RIA. Por cuanto al derecho a explicación de decisiones tomadas individualmente, este quedará limitado a algunos sistemas de alto riesgo y, en el caso de las personas físicas, la obtención de explicaciones deberá ejercerse a partir de las vías habilitadas por el artículo 22 RGPD.

7. EL IMPACTO COLECTIVO O SUPRAINDIVIDUAL DE LA IA REQUIERE NUEVOS MODELOS DE GARANTÍA Y PARTICIPACIÓN

Un tema más relevante es el reconocimiento y la protección de colectivos y grupos afectados por la IA. He sostenido que es imperativo superar la visión tradicional que limita los derechos fundamentales a impactos individuales directos[90]. Un enfoque centrado en los derechos individuales es insuficiente frente a los extensos impactos sociales de las tecnologías que soportan decisiones en ámbitos públicos y privados. Es fundamental adoptar una perspectiva más amplia que contemple los efectos colectivos y las consecuencias para la sociedad en su conjunto, reconociendo el alcance estructural del uso de sistemas de IA. Para los colectivos, como pueden ser los colectivos vulnerables[91], es relevante fomentar la transparencia específica y asegurar la participación de la sociedad civil en las diversas aplicaciones de sistemas de IA. El Supervisor Europeo señala

---

[89] El primer estudio sobre el tema López-Tarruella Martínez, A. "Vías de recurso para los particulares en el reglamento de inteligencia artificial", en Cotino Hueso, L. y Simón Castellanos, P. (coords.). *Tratado sobre el Reglamento ... cit.*

[90] Ver "Nuevo paradigma en las garantías ...cit. Sobre el tema recientemente, Castillo Parrilla, J. A.: "Privacidad de grupo...cit.

[91] Castellanos Claramunt, J. "Una reflexión acerca de la influencia de la inteligencia artificial en los derechos fundamentales", en Ramón Fernández, F. (2023). *Ciencia de datos y perspectivas de la inteligencia artificial*, Tirant lo Blanch, Valencia, pp. 271-300, en especial, pp. 279 y ss. sobre colectivos vulnerables. También, Valle Escolano, R. (2023). "Inteligencia artificial y derechos de las personas con discapacidad", en *Revista Española de Discapacidad (REDIS)*, Vol. 11, núm. 1, pp. 7-28.

que "Se van dejando caer "migas digitales" a cada minuto, que se combinan para clasificar a las personas físicas en tiempo real y para crear perfiles múltiples y, en ocasiones, contradictorios"[92]. Como afirma Jaume "El daño social, al igual que el daño medioambiental, son problemas existentes que no se dejan evaluar desde un enfoque individual"[93]. Con este enfoque destacan especialmente los análisis de gran calado en esta dirección de Hoffmann-Riem[94] y especialmente Mantelero[95], de Tullio[96] con apoyo de Vedder, Rodotà, Peña Gangadharan, Crawford, Faleiros, Luers, Meier, Perlich y Thorp.

Al momento de una valoración jurídica y constitucional de los riesgos, daños y restricciones, es necesario realizar un "recalibrado"[97], como sugirió Citron en relación al debido proceso. Es imprescindible evaluar no solo casos individuales, sino también el impacto masivo de las operaciones continuadas de algoritmos, sistemas de IA o el manejo extensivo de datos.

En la Carta de Derechos Digitales, propuse incluir un apartado sobre "Garantías de impacto social"[98], inspirado en parte por Mantelero[99]. La Recomendación

---

[92] Supervisor Europeo de Protección de Datos, SEPD (2015). *Dictamen 4/2015. Hacia una nueva ética digital. Datos, dignidad y tecnología*, 11 de septiembre, p. 15.

[93] Jaume Palasí, L. (2020). "Cómo la inteligencia artificial está impactando en las sociedades", Cerrillo i Martínez, A. y Peguera Poch, M. (coords.): *Retos jurídicos de la inteligencia artificial*, Aranzadi, Cizur, pp. 27-39, pp. 32 y 34.

[94] Hoffmann-Riem, W.: *Big Data...cit.*

[95] Mantelero, A. *El big data en el marco del Reglamento General de Protección de Datos*, marzo, UOC, Barcelona, pp. 1-46. Su obra de interés para el enfoque de este estudio es muy amplia, cabe seguir especialmente Mantelero, A. (2016). "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection". *Computer Law & Security Rew*, Vol. 32, núm. 2, pp. 238-255, 2016 DOI:10.1016/j.clsr.2016.01.014; y Mantelero, A. (2017). "From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era", en Taylor. L.; Van der Sloot, B.; Floridi, L. (eds.). *Group Privacy: New Challenges of Data Technologies*, Springer, capítulo 8. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

[96] De Tullio, M. F. (2016). "La privacy e i big data verso una dimensione costitizionale collettiva", *Politica del diritto*, Vol. 47, núm. 4, pp. 637-696.

[97] Citron, D. K. (2007). "Technological Due Process", *85 Wash. U. L. Rev*. pp. 1249-1313, pp. 1254 y ss., p. 1286. http://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2

[98] Ver mi aportación en RED DAIA (2020). *Aportación DAIA a consulta pública Carta de derechos digitales, diciembre.* https://bit.ly/3paF0H0

[99] Además de la obra reseñada, por ejemplo, "From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era", en Taylor. L., Van Der Sloot, B. y Floridi, L. (eds.) (2017), cap. 8.

sobre IA de la UNESCO subraya la importancia de un enfoque colectivo y la inclusión de mecanismos de participación social en el uso de sistemas de IA[100]. Ya hace décadas por la evolución tecnológica y social se incrementa el reconocimiento de los derechos de última generación, enfocados en la protección de intereses colectivos y supraindividuales, que desafían el marco centrado en intereses individuales[101]. Asimismo, se están reforzando las garantías y regulaciones para acciones colectivas efectivas del consumidor[102], particularmente en la protección contra la acumulación y tratamiento masivo de datos por grandes plataformas tecnológicas. En 2022, el Tribunal de Justicia de la Unión Europea ha interpretado favorablemente la normativa de protección de datos en este contexto[103].

A diferencia del Reglamento General de Protección de Datos (RGPD), el Reglamento de IA (RIA) no ha sido diseñado con un enfoque centrado en los afectados ni con un régimen de garantías. No obstante, el Convenio IA reconoce la importancia de esta perspectiva colectiva. El Supervisor Europeo de Protección de Datos ha instado a "la especificación de que los riesgos sociales o de grupo que plantean los sistemas de IA deben también ser evaluados y mitigados" en el convenio IA (núm. 6)[104]. Aunque las garantías no están detalladas con precisión, representan un avance significativo, alentando a los Estados a desarrollar y perfeccionar estos mecanismos de protección colectiva.

Por ejemplo, el artículo 15 del Convenio IA exige la identificación y evaluación de riesgos considerando todas las partes interesadas, incluidas aquellas cuyos derechos podrían verse afectados.

---

[100] En especial apartados 28, 30 (igualdad), 46 y 47 (Gobernanza), 50, 52, 53, 60 y 64 (impacto ético) o en el núm. 91 (género).

[101] Gidi, A. y Ferrer Mac-Gregor, E. (2003). *Procesos colectivos. La tutela de los derechos difusos, colectivos e individuales en una perspectiva comparada*, México, Porrúa, p. 203.

[102] En España cabe recordar la acción colectiva indemnizatoria del artículo 11 de la LEC; la acción de cesación del artículo 53 y ss. Real Decreto Legislativo 1/2007; las acciones colectivas de cesación, retractación y declarativa de condiciones generales (arts. 12 y ss. Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación).

[103] La Directiva (UE) 2020/1828, de 25 de noviembre de 2020 amplía las medidas y garantías (medidas resarcitorias como indemnización, reparación, resolución), sólo se debe probar el incumplimiento normativo, sin necesidad de dolo o culpa. Y, por lo que ahora interesa, explícitamente incluye la protección de datos en su anexo (núm. 56). El artículo 80 RGPD sobre "representación de los interesados" ha sido interpretado favorablemente por la STJUE de 28 de abril de 2022, l asunto C 701/20.

[104] SEPD, *Opinion 20/2022... cit.* núm. 6, apartado 8 de "Conclusiones", p. 15.

Así, el artículo 15 regula la necesidad de identificar y evaluar riesgos e "integrar la perspectiva de todas las partes interesadas pertinentes, incluida cualquier persona cuyos derechos puedan verse potencialmente afectados" (art. 15. 2º c). La participación de la sociedad civil se menciona en el artículo 5 sobre "Integridad de los procesos democráticos y respeto del Estado de Derecho". En su apartado 2º "en el contexto de las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial" obliga a adoptar medidas, en su caso, para "proteger la participación [de las personas] en los procesos democráticos, el acceso justo al debate público [y la capacidad de las personas para tomar decisiones libres de influencias o manipulaciones externas indebidas / [perjudiciales y malintencionadas]". Es más destacable si cabe que el artículo 20 sobre "consulta pública" disponga que "Cada Parte se esforzará por garantizar que las cuestiones importantes [...] sean, según proceda, objeto de debate público y de consulta a las múltiples partes interesadas a la luz, en particular, de las implicaciones sociales, económicas, jurídicas, éticas y medioambientales pertinentes.". Incluso hay algunas referencias más indirectas de interés.

8. LA INDEPENDENCIA DE LAS (NUEVAS) AUTORIDADES DE IA Y LA AESIA EN ESPAÑA

Como ocurrió con la protección de datos y el derecho de acceso a la información pública, parece necesaria una garantía frente a la IA a través de instituciones o autoridades regulatorias específicas y en su caso nuevas. La dimensión objetiva de los derechos es un instrumento dogmático importante para impulsar la legitimación constitucional de estas nuevas autoridades o, en su caso, nuevas facultades de instituciones ya existentes.

Es importante señalar que en el RIA se establecen diversos nuevos organismos. Por ejemplo, el 24 de enero de 2024 se creó la Oficina Europea de la IA[105]. Además, el RIA regula el Consejo Europeo de Inteligencia Artificial y se crean dos órganos consultivos: el grupo científico de expertos y el foro consultivo. En cada Estado miembro, habrá autoridades de supervisión del mercado (art. 59) encargadas de monitorear el correcto funcionamiento de los sistemas

[105] *Decisión de la Comisión de 24.1.2024 por la que se crea la Oficina Europea de Inteligencia Artificial*, Bruselas, 24.1.2024C(2024) 390 final. https://ec.europa.eu/newsroom/dae/redirection/document/101625

IA en el mercado, incluidos los sistemas de IA de alto riesgo, identificando riesgos emergentes, incidentes u otras circunstancias que requieran intervención. También deben existir organismos de evaluación de conformidad, responsables de realizar las pruebas de conformidad y que deben estar habilitados por una autoridad notificante, que debe existir al menos una por país y puede ser la autoridad de supervisión del mercado. Cada Estado puede establecer nuevas instituciones o asignar estas competencias a diversas autoridades, que en algunos casos podrían ser la Agencia Española de Protección de Datos o, para el uso jurisdiccional de algoritmos (Anexo III.8º), el Consejo General del Poder Judicial[106]. España ha sido el primer país de la UE en establecer una Autoridad Española de Supervisión de la IA, AESIA[107].

Cabe plantearse la necesidad de independencia de estas autoridades de IA, especialmente cundo su actuación se vincule a derechos fundamentales y a la posibilidad de resolver las reclamaciones o recursos efectivos. Por un lado, el artículo 26 del Convenio IA sobre "Mecanismos de supervisión eficaces" es muy relevante, ya que cada parte "garantizará que dichos mecanismos ejerzan sus funciones de manera independiente e imparcial y que tengan los poderes, la experiencia y los recursos necesarios para cumplir eficazmente sus tareas de supervisar el cumplimiento de las obligaciones del Convenio" (2º). Se trata de una regulación valiente y suficientemente concreta.

Por otro lado, el RIA originalmente no requería la independencia e imparcialidad de la "autoridad de vigilancia del mercado". Sin embargo, la enmienda 123 del Parlamento al considerando 77 y la enmienda 558 con el nuevo artículo 59, apartado 4, ahora exigen la "total independencia", caracterizándola como "independiente, imparcial y objetiva". En la versión final, la "independencia" se aclara en los considerandos (76, 77 bis y 80-x) y en el artículo 59. 2.

---

[106] Para el caso de sistemas de identificación biométrica utilizados por Fuerzas y Cuerpos de Seguridad del Estado, en migración o en Administración de Justicia, las autoridades de supervisión serán, las autoridades de protección de datos competentes en esos ámbitos, pudiendo ser en algunos supuestos la AEPD.

[107] La creación legal y habilitación fue por la Ley 28/2022, de 21 de diciembre, en concreto, su D.A 7ª reguló la creación. Asimismo, según Ley 28/2022, la AESIA está adscrita orgánica al Ministerio de Asuntos Económicos y Transformación Digital, a través de su Secretaria o SEDIA. El Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto.

Pues bien, considero que la AESIA no cumple completamente con los criterios de independencia establecidos tanto en el RIA, como en el Convenio IA. La AESIA se creó como un organismo público bajo el artículo 91 de la Ley 40/2015 y no como una agencia estatal independiente de acuerdo con los artículos 108 bis y siguientes de la Ley 40/2015. En sus estatutos regulados por el Real Decreto 729/2023, de 22 de agosto, el artículo 8 menciona como "Principios de actuación de la Agencia" la "Autonomía" y la "Independencia técnica" y señala que "la Agencia actuará con plena autonomía"[108]. No obstante, estas afirmaciones parecen insuficientes, especialmente dada una evidente falta de independencia orgánica que afecta a la independencia funcional. Incluso se establece explícitamente la "dependencia" de la Dirección de un órgano político como el Secretario de Estado, quien es el Presidente y desempeña algunas funciones materiales (art. 23.1º).

El estándar máximo de independencia de una autoridad regulatoria es el de las de protección de datos, que ha alcanzado estatus "constitucional" en el derecho de la UE[109]. El RGPD establece una regulación muy exhaustiva[110], resultado de una doctrina del TJUE muy exigente en la materia, especialmente en la sentencia del 3 de diciembre de 2009, Comisión/Alemania (C-424/07), apartados 80 a 83. No son pocos los casos en los que el derecho de la UE exige la "independencia" de las autoridades por diversos motivos, como evitar conflictos de interés, asegurar la imparcialidad y promover la confianza en los procesos regulatorios y de supervisión. Esto ocurre en contextos como la Autoridad Bancaria Europea y otras autoridades de supervisión financiera, en el ámbito de la competencia, autoridades nacionales de regulación de medios y telecomunicaciones,

---

[108] "a) Autonomía, entendida como la capacidad de la Agencia de gestionar, en los términos previstos en su Estatuto, los medios puestos a su disposición para alcanzar los objetivos comprometidos".
"b) Independencia técnica, basada en la capacitación, especialización, profesionalidad y responsabilidad individual del personal al servicio de la Agencia que deberá observar los valores de competencia, ética profesional y responsabilidad pública que son de aplicación. En el desempeño de sus funciones y en el ejercicio de sus competencias, la Agencia actuará con plena autonomía".

[109] Artículo 8 Carta de derechos fundamentales UE, "3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[110] Capítulo VI. Autoridades de control independientes, Sección 1, Independencia: artículo 51 Autoridad de control; artículo 52 Independencia; artículo 53: Condiciones generales aplicables a los miembros de la autoridad de control, artículo 54, Normas relativas al establecimiento de la autoridad de control.

la Agencia Europea de Medicamentos y la Autoridad Europea de Seguridad Alimentaria y las Autoridades Reguladoras de Energía. En el ámbito tecnológico también es importante considerar las autoridades nacionales relacionadas con la DSA o la detección de contenidos terroristas, por ejemplo.

No obstante, es necesario evaluar cada caso concreto y la especificación de la "independencia" en la regulación aplicable, ya que hay variaciones. Se puede afirmar que cuanto más vinculada esté una autoridad al ámbito de los derechos fundamentales o a la protección del consumidor, mayor independencia se requiere, hasta el nivel exigido para la protección de datos[111]. Aunque no exista una doctrina jurisprudencial muy consolidada en casos que no involucran derechos fundamentales, se puede afirmar que el TJUE es bastante exigente en cuanto a la independencia y que "El sistema del Derecho de la Unión privilegia una concepción amplia de la independencia respecto a las competencias específicas asignadas a las autoridades independientes"[112].

En el caso de España se ha optado por un modelo concentrado de autoridad para el Reglamento IA, ello haría pensar en la necesidad de mayor independencia. No obstante, la AESIA va a cohabitar con autoridades sectoriales que, aunque actúan en áreas relacionadas con la vida o la integridad de las personas (ascensores, vehículos, juguetes, etc.), también carecen de independencia y, hasta ahora, no han presentado problemas significativos por ello. Además, en los terrenos en los que hay una mayor afinidad a derechos fundamentales (áreas de aplicación de la ley o justicia) la competencia recaerá en la AEPD o el CGPJ cuya independencia no está puesta en duda. Igualmente, es poco probable que

---

[111] Así lo afirma el abogado General del TJUE: "125. Por lo demás, también en otros sectores del Derecho de la Unión en los que ha sido necesario instituir autoridades independientes con obligaciones destinadas a crear un mercado competitivo que sea capaz de tutelar de forma simultánea otros objetivos, expresamente indicados y regulados por el legislador europeo, como por ejemplo la protección de derechos fundamentales específicos y de los derechos del consumidor, la interpretación del concepto de independencia proporcionada por el Tribunal de Justicia ha sido lo más amplia posible." Conclusiones del Abogado General Giovanni Pitruzzella, presentadas el 14 de enero de 2021, Asunto C-718/18, Comisión Europea contra República Federal de Alemania, para un supuesto no relativo a protección de datos, con análisis de diversas sentencias sobre la independencia de las autoridades independientes. https://curia.europa.eu/juris/document/document.jsf?text=%2522autoridades%2Bindependientes%2522%2B%2522independencia%2Bfuncional%2522%2B%2522derechos%2Bfundamentales%2522&docid=236435&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=1817917#ctx1

[112] Cabe acudir a las Conclusiones referidas, ver en especial 104, 105, 127 y la cita de 128.

la AESIA tenga que resolver sobre el ejercicio de derechos de personas. Estos motivos pueden llevar a disminuir la intensidad de exigencia de una autoridad independiente. Pero, aun así, el carácter centralizado de la AESIA y su proximidad a no pocos derechos fundamentales llevan a pensar que habría de garantizarse un mayor estándar de independencia que actualmente no se cumple con su regulación. En todo caso, habrá que estar atentos a la evolución e interpretación de este marco normativo y los ámbitos reales de actividad.

9. GESTIÓN DE RIESGOS Y LA DOBLE PROYECCIÓN PARA LA IA DEL MODELO PREVENTIVO DE LA PROTECCIÓN DE DATOS

Ante la IA, es fundamental adoptar técnicas de responsabilidad "proactiva", "demostrada" o "accountability" desde el diseño, siguiendo el principio jurídico de "más vale prevenir que curar"[113]. Inspirándose en las leyes de la robótica de Asimov, esto implica la integración del cumplimiento ético y legal directamente en el "Código", conforme a los términos expuestos por Lessig. Este enfoque, conocido como compliance o cumplimiento normativo de origen anglosajón, comienza a ser reconocido en el Derecho continental europeo, aplicándose en áreas como el medio ambiente o los estudios de impacto de género en disposiciones generales[114], y extendiéndose para incluir la discriminación algorítmica pública. Este modelo se generaliza en la UE en diversos ámbitos digitales[115]

---

[113] Sobre la aplicación del principio de responsabilidad proactiva y el diseño para el ámbito de la IA y el big data mi estudio (2022 a). Destaca, Hernández Peña, J. C. (2022). *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cízur, pp. 119-172 y también con especial atención a la gobernanza, pp. 173-206.
Hernández Peña, J. C. (2022). *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cízur, pp. 119-172 y también con especial atención a la gobernanza, pp. 173-206. Cabe seguir: Alberto González, P. (2017). "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata*, núm. 24, pp. 115-129; Navas Navarro, S. (2017). "Derecho e inteligencia artificial desde el diseño. Aproximaciones", Navas Navarro, S. (coord.). *Inteligencia artificial: tecnología, derecho*, Tirant lo Blanch, Valencia, pp. 23-72; Martínez Martínez, R. (2019). "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista catalana de dret públic*, núm. 58, pp. 64-81.

[114] Impuestos a nivel estatal por artículos 22.2 para leyes y 24.1.b para reglamentos, Ley 50/1997, de 27 de noviembre, del Gobierno; artículo 19 Ley Orgánica 3/2007 para disposiciones de carácter general y los planes de especial relevancia económica y artículos 26. 3 f) Ley 40/2015. Existe abundante normativa autonómica.

[115] Barrio Andrés, M. (2023). *El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo*, Real Instituto Elcano, ARI 34/2023, 20 abril. https://

y en la legislación europea sobre comercialización de productos potencialmente peligrosos.

Este enfoque es particularmente relevante en el modelo regulatorio de protección de datos. Su proyección a la IA es doble. De un lado hay que aplicarlo respecto de los sistemas de IA que procesan datos personales. De otro lado, este modelo proactivo de la protección de datos influye también en la nueva regulación del RIA. En España, la Carta de Derechos Digitales establece generalmente el "principio de cumplimiento normativo desde el diseño" para todos los campos (I.4)[116]. Y para la Administración, "será necesaria una evaluación de impacto en los derechos digitales al diseñar algoritmos para decisiones automatizadas o semiautomatizadas" (XVIII.7º). En desarrollo de la Carta, el artículo 23.1º Ley 15/2022 afirma con cierta *suavidad* que "se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio".

En primer término, cuando un sistema de IA maneja datos personales, el modelo de cumplimiento normativo promueve la responsabilidad proactiva (art. 5, Considerando 78 del RGPD), lo que implica numerosas obligaciones[117], como el registro interno de actividades de procesamiento, la identificación del riesgo en cada proceso (art. 30 y art. 31 de la Ley Orgánica 3/2018, conectado con el inventario de actividades del sector público, art. 77.1º). Especialmente relevante es la obligación de proteger los datos desde el diseño y por defecto (art. 25 RGPD) antes del procesamiento inicial de datos, y en particular, la realización de evaluaciones de impacto (art. 35 RGPD), que supone el análisis y descripción de todas las operaciones, su necesidad, proporcionalidad

media.realinstitutoelcano.org/wp-content/uploads/2023/04/el-cumplimiento-basado-en-el-riesgo-o-risk-based-compliance-pieza-cardinal-del-nuevo-derecho-digital-europeo-real-instituto-elcano.pdf

[116] "Declara que el principio de cumplimiento normativo desde el diseño es de aplicación íntegramente al desarrollo de los entornos digitales y por ello los desarrollos científicos, tecnológicos y su despliegue contemplarán en la determinación de sus requerimientos un análisis sobre el cumplimiento de tal principio".

[117] Entre otras, la diligente elección de un encargado, las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas (art. 28) y la necesidad de decidir cuáles son las adecuadas según los riesgos (art. 32 RGPD), la designación de un delegado de protección de datos (art. 36), la notificación de una violación de la seguridad a las autoridades (art. 33) y su comunicación a los interesados (art. 34).

y evaluación de riesgos. Según la AEPD desde 2019[118] este análisis de impacto es obligatorio en casi todos los casos de uso de IA con datos personales. Para facilitar el cumplimiento de estas medidas, se han desarrollado instrumentos desarrollados las autoridades europeas[119] y españolas[120] de protección de datos. Por último, hay que llamar la atención de que todas estas exigencias se intensifican cuando se manejan datos especialmente protegidos bajo el artículo 9 del RGPD y en casos de decisiones "exclusivamente automatizadas" (art. 22 RGPD).

10. EL MODELO PREVENTIVO DE PROTECCIÓN DE DERECHOS DEL REGLAMENTO IA PARA LOS SISTEMAS DE ALTO RIESGO Y EN EL CONVENIO DE EUROPA

El modelo de responsabilidad proactiva se ha proyectado claramente en la UE como el "Ethics & Rule of law by design X-by design", insignia de la "IA confiable" "Made in Europe"[121], que fundamenta las políticas y normativas de IA en la UE[122]. Además, el alto grupo de expertos de la UE adoptó un modelo

---

118 Afirma que se han de dar al menos dos de estos supuestos: toma de decisiones automatizadas; perfilados de comportamiento; uso de datos a gran escala; asociación, combinación o enlace de registros de bases de datos para varias finalidades o utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, AEPD: *Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4),* 2019. https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

119 Así, Grupo del Artículo 29. *Directrices sobre la evaluación del impacto de la protección de datos (DPIA) y determinar si el procesamiento es "probable que genere un alto riesgo" a los efectos del Reglamento 2016/679*, WP248 rev. 01, Revisadas por última vez y adoptadas el 4 de octubre de 2017. https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

120 AEPD: *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, 2021* https://www.aepd.es/es/node/46578; AEPD: *Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas, 2019.* https://www.aepd.es/es/node/816; Autoridad Catalana de Protección de Datos: *Guía práctica sobre la evaluación de impacto relativa a la protección de datos, 2017.* https://apdcat.gencat.cat/es/documentacio/guies_basiques/Guies-apdcat/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/; AEPD: *Guía práctica para las evaluaciones de impacto en la protección de datos personales, 2018.* https://www.lopdencastellon.com/wp-content/uploads/2018/02/Gu%C3%ADa-Evaluaci%C3%B3n-de-impacto-protecci%C3%B3n-de-datos.pdf

121 HLEG, *op.cit.*, en versión 2018, pp. 19, 21, 29.

122 Un análisis exhaustivo en mi estudio "Ética en el diseño... *cit*.

de ética en el diseño con su exhaustiva lista de evaluación[123], su modelo ALTAI de evaluación o FUTURE-AI para salud[124]. El Libro Blanco de la IA de 2020 clarificó el modelo de riesgos, que se concretaría un año después en el RIA. Este enfoque supone un aumento de obligaciones y garantías en proporción al impacto o riesgo del sistema de IA. Es notable destacar las contribuciones de Mantelero[125] y Simón en España[126] en el ámbito de la protección de datos y posteriormente para los sistemas de IA.

El RIA, en su fase final y tras el surgimiento de ChatGPT y similares, reguló los sistemas de IA de propósito general y les impuso diversas obligaciones generales: elaboración de documentación técnica, diseño de políticas de cumplimiento sobre derechos de autor y un resumen detallado del contenido utilizado durante el entrenamiento del sistema de IA. Las obligaciones se intensifican para sistemas considerados de riesgo sistémico: evaluaciones para identificar y mitigar riesgos sistémicos, documentación y notificación de incidentes graves y un adecuado nivel de ciberseguridad. Bajo la dirección de la nueva Oficina de IA de la UE, se establecerán códigos de conducta para precisar estas obligaciones.

El RIA implica esencialmente que los sistemas de IA de alto riesgo (artículo 6, anexo I y III) deben cumplir ciertos requisitos. "La clasificación de un sistema de IA como "de alto riesgo" debe limitarse a aquellos sistemas de IA que tengan un efecto perjudicial importante en la salud, la seguridad y los derechos fundamentales de las personas de la Unión" (Considerando 46). Como se señaló al inicio, el Considerando 48 menciona veintiún derechos fundamentales afectados por estos sistemas, además de derechos específicos de

---

[123] HLEG, *Directrices éticas para una IA fiable, 2019, en especial Capítulo III y listado,* pp. 33-41.

[124] Portal ALTAI https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal

[125] Respecto del ámbito de los datos Mantelero, A. "Toward a New Approach to Data Protection in the Big Data Era", en Gasser U. y otros (dir.): *Internet Monitor 2014: Reflections on the Digital World.* Cambridge (MA), Berkman Center for Internet and Society at Harvard University, pp. 84 y ss. Para la IA, Mantelero, A. *Beyond Data. Human Rights, Ethical and Social Impact Assessment*, Springer, Information Technology and Law Series IT&LAW 36, 2022. https://link.springer.com/book/10.1007/978-94-6265-531-7

[126] Simón Castellano, Pere (2023). *La evaluación de impacto algorítmico en los derechos fundamentales*, Aranzadi, Cízur. También, "Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial", *Revista de Derecho Político*, núm. 117, 2023, pp. 153-196.

menores. Por una parte, será de alto riesgo la integración de IA en productos ya peligrosos, sujetos a la normativa de la UE dentro del "nuevo marco legislativo" de la UE (Anexo I). Por otra parte, son de alto riesgo los sistemas IA utilizados para "influir sustancialmente en el resultado de la toma de decisiones" (art. 6.3 RIA) para hasta 25 finalidades enumeradas en el Anexo III agrupadas en: 1) Biometría; 2) Infraestructuras críticas; 3) Educación y formación profesional; 4) Empleo, gestión de los trabajadores y acceso al autoempleo; 5) Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones; 6) Aplicación de la ley; 7) Migración, asilo y gestión del control fronterizo; y 8) Administración de justicia y procesos democráticos.

En caso de sistemas de alto riesgo, se requiere cumplir con un conjunto de obligaciones preventivas que, de verificarse, permiten una evaluación de conformidad. Ello permite que el sistema IA de alto riesgo se incluya en un registro y pueda ponerse en el mercado bajo el marcado "CE" de la UE. Las obligaciones incluyen que el proveedor o fabricante realice evaluaciones y mitigaciones de riesgos (art. 9 RIA), use datos de alta calidad (art. 10 y 16 RIA). Se parte de que los datos deben "estar libres de errores y ser completos en vista de la finalidad prevista del sistema" (Considerando 67). Si los datos de los que se alimenta la IA son basura, sus resultados necesariamente serán basura. El proveedor de un sistema de alto riesgo ha de generar documentación técnica que demuestra el cumplimiento de los requisitos y los elementos técnicos del sistema, para ponerla a disposición de las autoridades (art. 11).

También se ha de diseñar la IA de alto riesgo para que genere registros y logs de funcionamiento (art. 12). Se trata de que los sistemas de IA más peligrosos estén localizados y que se puedan vigilar, así como trazar exactamente cómo han funcionado, así como verificar que cumplen las obligaciones preventivas. Asimismo, al menos para los sistemas peligrosos, se hace preciso diseñar el sistema algorítmico de manera que pueda ser auditable, esto es, creando registros entendibles para que se pueda investigar si funcionó bien en todo momento. Y obviamente el sistema de IA ha de estar bien diseñado y comprobarse que funciona bien en todo momento. También hay obligaciones de "transparencia y comunicación de información a los responsables del despliegue" (art. 13), esto es, que los sistemas tengan buenos "manuales de instrucciones" y las empresas o administraciones –los implementadores– que los utilicen los conozcan y puedan también dar suficiente información a la ciudadanía, que son los afectados últimos por la IA. Las medidas proactivas pasan

también en general por las obligaciones de supervisión humana (art. 14). De igual modo, los sistemas de IA evitarán los sesgos y la discriminación si están diseñados con "solidez" técnica, cumpliendo obligaciones para prevenir o minimizar "errores, fallos, incoherencias, situaciones inesperadas" (Considerando 75) y la eliminación o reducción de resultados sesgados una vez comercializados (art. 15. 3º), además de requisitos de ciberseguridad –que no sean *hackeables*–.

Todas estas exigencias serán desarrolladas además por todo un armazón de normas técnicas y de armonización, que serán acompañadas de la normalización técnica de la IA que está actualmente en fase de desarrollo. Para los sistemas que no son de alto riesgo, todas estas obligaciones serán los referentes de las buenas prácticas a seguir voluntariamente en códigos, sellos o certificaciones a las que se sumen (Considerandos 165-166) los proveedores públicos o privados de esos sistemas de IA.

El Convenio IA del Consejo de Europa también adopta un modelo de gestión de riesgos. Desde su inicio, establece la obligación general de implementar "medidas legislativas, administrativas o de otro tipo", que deben ajustarse según la necesidad, en función de la gravedad y la probabilidad de que se produzcan impactos adversos sobre los derechos humanos, la democracia y el Estado de Derecho (art. 1). De hecho, lo más importante del Convenio, es el artículo 16 (Capítulo V), que obliga a adoptar medidas "para la identificación, evaluación, prevención y mitigación de los riesgos e impactos" (art. 16.1º). "Dichas medidas tendrán en cuenta el enfoque basado en el riesgo a que se refiere el artículo 1" (art. 16. 2º). Entre las obligaciones concretas, hay que tener: a) "debidamente en cuenta el contexto y el uso previsto de los sistemas"; b) "la gravedad, duración y reversibilidad de los posibles riesgos"; c) "integrar la perspectiva de todas las partes interesadas relevantes, incluida cualquier persona cuyos derechos puedan verse potencialmente afectados"; d) también se incluye "el registro, seguimiento y la debida consideración de los impactos"; e) que de manera continua se lleven a cabo "procesos de gestión de riesgos e impactos"; y f) que estos análisis de riesgos se plasmen en "la documentación adecuada". Incluso se afirma g) "en su caso, la publicación de información sobre los esfuerzos" adoptados.

Como consecuencia lógica de la identificación y evaluación de los riesgos, el Convenio también estipula la mitigación de estos, es decir, h) "la aplicación de medidas preventivas y paliativas suficientes para abordar los riesgos e impactos adversos detectados, incluyendo, cuando sea apropiado, la realización de pruebas

previas del sistema antes de su uso inicial". Adicionalmente, si los riesgos se consideran "incompatibles", se exige "establecer mecanismos de moratoria, prohibición u otras medidas apropiadas" (art. 16.3º).

11. ANÁLISIS DE RIESGOS Y ESTUDIOS DE IMPACTO DE DERECHOS FUNDAMENTALES PARA SISTEMAS IA DE ALTO RIESGO

Cabe centrar ahora en dos instrumentos de evaluación de riesgos y prevención del RIA: la obligación que el artículo 9 impone a los proveedores o fabricantes de IA de implementar sistemas de gestión de riesgos y el estudio de impacto sobre derechos fundamentales que deben realizar aquellos que implementan sistemas de alto riesgo (art. 27)[127]. En primer lugar, el análisis de riesgos debe incluir aspectos relacionados con los derechos fundamentales (art. 9.2.a), enfocándose especialmente en menores y otros grupos vulnerables (art. 9.9. concepto que la oficina europea de IA y la AESIA española tendrán que matizar y delimitar). Las etapas clave del análisis de riesgos involucran la identificación y evaluación de riesgos, considerando tanto el uso previsto como un mal uso razonablemente previsible. Las pruebas se basan en parámetros y umbrales de tolerancia definidos previamente. Además, tras la comercialización del producto se evalúan riesgos adicionales y se implementan medidas específicas de gestión de riesgos. Es un proceso de mejora continua a lo largo del ciclo de vida del sistema de IA de alto riesgo, que requiere revisiones y actualizaciones periódicas. El proveedor tiene la flexibilidad de poder seguir diferentes modelos y estándares internacionales[128], adaptándolos a las particularidades de cada entidad y tipo de sistema de IA. Además, el análisis de riesgos podrá coordinarse con otros sistemas de gestión de riesgos regulados, como los ambientales y de sostenibilidad, así como de seguridad de la información (ENISA y ENS o los específicos para infraestructuras críticas).

---

[127] Cabe remitir a los estudios de Chaveli Donet, E. "Evaluaciones de impacto de derechos fundamentales sobre sistemas de inteligencia artificial" y Simón Castellano, P. "Los sistemas de gestión de riesgos como obligación específica para los sistemas de IA de alto riesgo", ambos en *Tratado sobre el Reglamento... cit.*

[128] Así, cabe recordar la ISO/IEC 42001:2023, la ISO/IEC TR 24030:2021 y la ISO/IEC TR 5469:2024; o los modelos de la norma técnica NIST 800 218 PW.I.I y NIST 800 218RV.1.I.; o el modelo de gestión de riesgos de IA de la OCDE: *High-level AI risk-management interoperability framework.* https://oecd.ai/en/accountability

Si, por un lado, el proveedor debe realizar un análisis de riesgos del sistema IA de alto riesgo que fabrica (art. 9), por el otro lado, el usuario que adquiere y utiliza el sistema está obligado a realizar un estudio de impacto sobre derechos fundamentales antes de su implementación (art. 27 RIA). Este estudio, introducido en las últimas etapas de aprobación del RIA, es obligatorio solo para los sistemas de alto riesgo empleados por el sector público, así los sistemas IA bancarios usados para solvencia de personas físicas y en situaciones de emergencia por policía, bomberos y servicios médicos. Debe evaluarse si hay necesidad de implantar el sistema IA de alto riesgo por la entidad y, fundamentalmente, identificar y mitigar riesgos que tiene para los derechos fundamentales que sean aceptables. Todo esto debe documentarse adecuadamente. También es importante mantener un sistema de control y evaluación de riesgos una vez que el sistema está implementado y en uso.

Dado que es probable que también se requiera un estudio de impacto sobre protección de datos (art. 35 RGPD), se recomienda la colaboración entre las partes responsables de uno y otro, aunque no sea obligatoria. Existen diversas metodologías y herramientas de evaluación[129] relacionadas con los derechos fundamentales previas al RIA[130], y la Oficina de la IA de la UE también desarrollará y propondrá herramientas para que las entidades las adopten y adapten. Esto representa una garantía preventiva adicional para evitar violaciones de los derechos fundamentales.

12. LA CALIDAD DE LA LEY COMO GARANTÍA ANTE EL IMPACTO DE LA IA EN LOS DERECHOS FUNDAMENTALES

Sin duda que la IA impacta en el sistema de fuentes, con un papel cada vez más protagonista del *soft law*, la normalización técnica y la autorregulación[131].

---

[129] Por ejemplo, HRESIA o EISDH (evaluación de impacto social, ético y de los Derechos Humanos), la PIA (P*rivacy Impact Assessment*) o DPIA *(Data Privacy Impact Assessment*), la SIA (*Social Impact Assessment*) y la *EtIA Ethical Impact Assessment*).

[130] Como recuerda Chaveli, existen ciertas metodologías como el *Algorithmic Impact Asssessment Tool* en Canadá; la herramienta AIA del Gobierno de Estados Unidos, en los Países Bajos el modelo FRIAA o el modelo PIO (Principios, Indicadores y Observables) de la OEIAC, o las propuestas del Ada Lovelace Institute y el Model Rules del European Law Institute.

[131] En particular, Álvarez García, V. J. y Tahirí Moreno, J. (2023). "La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque", en *Revista General de Derecho Administrativo*, núm. 63. Una reflexión de interés, Sánchez Barrilao, J. F. (2023). "Inteligencia artificial y fuentes del derecho", en *Revista de derecho constitucional europeo*, núm. 39.

Ahora bien y por lo que aquí interesa, por su impacto los derechos fundamentales la IA necesita de regulación, legal y de calidad. Un legislador de calidad es fundamental para garantizar que la IA impacte los derechos fundamentales adecuadamente. El desarrollo, regulación del ejercicio y los límites directos e indirectos de los derechos fundamentales en razón de la IA ha de ser regulado a través de ley de que cumpla con el mandato de calidad legislativa. Recordemos que materia digital, de privacidad y protección de datos, tanto el TJUE como el TC han sido particularmente exigentes. Por ejemplo, la STJUE (Gran Sala) del 8 de abril de 2014 en los Asuntos C-293/12 y C-594/12 (*Digital Rights*), y en especial las Conclusiones de Pedro Cruz (núm. 108 y ss.), resaltan la exigencia de calidad normativa, aplicable incluso a Directivas, que son por naturaleza más genéricas que el Derecho nacional que las transpone. En España, la protección de datos ha provocado las sentencias más estrictas sobre calidad legislativa. Quien suscribe precisamente participó en la petición al Defensor del Pueblo del recurso de inconstitucionalidad respecto de la Ley Orgánica 3/2018, que dio lugar a la sentencia más exigente en materia de calidad de la ley. La legislación restrictiva debe no solo detallar la restricción y sus presupuestos, sino también incluir garantías concretas *compensatorias*. Este estándar se extiende a la normativa de protección de datos, especialmente en tratamientos de datos especialmente protegidos y en tratamientos automatizados.

En el ámbito de regulación de los sistemas automatizados e inteligentes, en 2020 ya advertí sobre una situación similar con la sentencia del Tribunal de Distrito de La Haya del 5 de febrero de 2020 (C / 09/550982 / HA ZA 18-388), que encontró inconstitucionales las garantías en la normativa neerlandesa, pese a ser amplias, en el sistema Systeem Risicoindicatie (SyRI). Sentencias con un alto nivel de exigencia se han dado también en Francia y Eslovaquia, y eso que las leyes que examinaban ofrecen garantías superiores a las de España. Es decir, en otros países se declara inconstitucional una normativa con garantías que no se alcanzan ni de lejos en España respecto de los tratamientos masivos de datos que se llevan a cabo por la AEAT, la TGSS, CNMC o inspección de trabajo, entre otras[132].

---

[132] Olivares Olivares, B. D. "Law and Artificial Intelligence in the Spanish Tax Administration: the Need for a Specific Regulation", *European Review of Digital Administration* & Law-ERDAL 1 (1-2), pp. 227-234.

En 2023, la sentencia del Tribunal Constitucional alemán del 16 de febrero (1 BvR 1547/19, 1 BvR 2634/20) estableció requisitos y estándares de calidad legislativa muy altos (incluso excesivos) para tratamientos automatizados de datos en la prevención del delito, prohibiendo además el uso de sistemas de IA. Nuestras autoridades de protección de datos reconocen la falta de cobertura normativa en casos de sistemas automatizados o de reconocimiento facial, y la FRA (Agencia de la Unión Europea para los Derechos Fundamentales) también insiste en requisitos exhaustivos de habilitación, cobertura y calidad normativa.

La falta de un legislador que cumpla con sus *deberes* nos priva de poder usar legítimamente estas tecnologías en áreas como la seguridad, fraude, salud, educación, laboral, personalización de servicios públicos, marketing y un largo etcétera. Aún es peor, bajo una situación de falta de regulación o mala regulación se compromete la efectividad de estos sistemas, pudiendo anular actuaciones públicas por violaciones de derechos fundamentales. Ahora bien, creo que no debe orillarse o directamente prohibirse la regulación del uso de IA y los sistemas autónomos como hace sin excesiva justificación el TC alemán. La regulación del RIA ofrece una oportunidad para adoptar estas tecnologías, siempre y cuando se cumplan los estándares y garantías necesarias. A estos efectos, las garantías y medidas técnicas que regula en un reglamento europeo sí que sirven para cumplir con la regulación de garantías en una ley. Ahora bien, como advierte expresamente el Considerando 63 del RIA, "El hecho de que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea legal con arreglo a otros actos del Derecho de la Unión o del Derecho nacional compatible con el Derecho de la Unión [...] No debe entenderse que el presente Reglamento constituye un fundamento jurídico [...] salvo que el presente Reglamento disponga específicamente otra cosa." (Considerando 63). Así pues, el RIA no vale como norma legal habilitadora o legitimadora de sistemas que restringen derechos fundamentales. Si la Constitución española o el mismo RGPD exige una ley que legitime, seguirá siendo necesaria pese a que se trate de un sistema de alto riesgo de los regulados con carácter general en el RIA. De ahí, que habrá de ser la ley nacional o Reglamento europeo el que habilite expresamente y con calidad los usos que impliquen la regulación del ejercicio de derechos, límites directos o indirectos y desarrollos de derechos fundamentales en razón de los sistemas IA. Asimismo, la ley habrá de regular las garantías especiales que puedan corresponder a ese caso concreto.

13. CONCLUSIONES

Este estudio ha centrado su atención en elementos claves de una parte general una comprensión general de los derechos fundamentales frente a la IA. Es necesario adaptar nuestra dogmática y categorías analógicas a las realidades tecnológicas emergentes, en especial la IA. La defensa de los derechos en este nuevo entorno digital requiere, más que nunca, redefinir, innovar e incluso forzar categorías y conceptos, así como los propios contornos de los derechos fundamentales y la creación de nuevas instituciones.

Las cuestiones esenciales identificadas contarían con la palanca legitimadora de la dignidad de la persona y la dimensión objetiva de los derechos fundamentales.

Se destaca la necesidad de configurar un deber constitucional de progreso e innovación en IA por los beneficios públicos (y en su caso privados) que conlleva. Se parte de que la "Constitución del algoritmo" debe estimular y dirigir la innovación y establecer también garantías y limitaciones adecuadas. El régimen de protección de datos continuará siendo fundamental para los tratamientos de datos con IA, no obstante, se han señalado sus insuficiencias estructurales y cuestiones clave, respecto de las que se han señalado líneas de respuesta. También se ha resaltado que la flexibilidad del régimen de protección de datos ya no es suficiente como marco general para abordar todos los desafíos que presenta la IA.

Se ha descrito el actual panorama de aceleración en la regulación de la IA en el mundo. En todo caso, destaca el RIA y el más reciente Convenio de IA del Consejo de Europa. Aunque en segundo plano, este último sirve para enfocar la atención en los derechos fundamentales y apuntalar al RIA con un marco sólido y coherente de los derechos fundamentales a nivel europeo y global. He afirmado que positivamente estamos desde las "musas" de la ética y el *soft law* de la IA hacia una regulación más concreta. Y en este sentido se apuesta por la regulación de principios jurídicos a los que someter el uso de IA para guiar su desarrollo y aplicación. El Convenio IA va en una buena línea que, desafortunadamente el RIA no se ha atrevido en su versión final.

En cuanto a los nuevos derechos y garantías relacionados con la IA, se argumenta que es preferible una regulación efectiva a la tentación a veces frívola de proclamar nuevos derechos, que a menudo quedan en declaraciones vacías sin efecto jurídico, como ha sucedido con los "derechos digitales" de la Ley Orgánica 3/2018. Se ha insistido en la importancia de avanzar en la protección

de los colectivos en los que impacta la IA, con nuevos modelos de garantía y de participación.

El modelo emergente es el de cumplimiento normativo y gestión de riesgos con un enfoque preventivo y proactivo: más vale prevenir que curar. Se ha explicado cómo el enfoque proactivo de la protección de datos se proyecta doblemente a la IA. También, que el RIA regula principalmente los sistemas que más afectan a los derechos fundamentales, es decir, los sistemas de alto riesgo imponiéndoles todo un régimen de obligaciones preventivas. Se detalla que este está basado en un sistema de evaluación de conformidad y que cuenta con concretos instrumentos preventivos como el análisis de riesgos (también de derechos fundamentales) por los proveedores y la obligación del estudio de impacto de derechos fundamentales para ciertos implementadores de sistemas de IA de alto riesgo. También se ha revisado la regulación de gestión de riesgos del Convenio IA.

Se ha puesto en duda si es suficiente la independencia de las nuevas instituciones de garantía de la IA en España, como la AESIA, en contraste con lo que exigen el RIA y el Convenio IA. Finalmente se ha recordado que los altos tribunales demandan un legislador de calidad que regule tanto los impactos en los derechos fundamentales como las garantías específicas compensatorias. Sin embargo, se observa que este legislador no ha actuado adecuadamente en España.

El desafío futuro no es otro que lograr un equilibrio donde la innovación tecnológica de la IA y la protección de los derechos fundamentales se fortalezcan mutuamente, asegurando que la tecnología de IA promueva bienes e intereses constitucionales y privados, respetando la dignidad y los derechos de individuos y colectivos afectados de forma masiva. El Derecho no es la única pieza en este tablero, y posiblemente no es la más importante frente a elementos tecnológicos, económicos, políticos o geoestratégicos, pero sí que tiene los instrumentos para acercarse e incluso lograr este equilibrio de manera más concreta. Se trata de uno de los retos más importantes, sino el que más, de este siglo XIX.

BIBLIOGRAFÍA

AEPD (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos personales*. https://www.lopdencastellon.com/wp-content/uploads/2018/02/Gu%C3%ADa-Evaluaci%C3%B3n-de-impacto-protecci%C3%B3n-de-datos.pdf

AEPD (2020). *Privacidad de grupo*, 19 de octubre. https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

AEPD (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*.

AEPD (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. https://www.aepd.es/es/node/46578

AEPD (2019). *Listas de tipos de tratamientos de datos que requieren EIPD (art. 35.4)*. https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

AEPD (2019). *Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas*. https://www.aepd.es/es/node/816

AEPD (2021). *Requisitos para Auditorías de Tratamientos que incluyan IA*.

Alberto González, P. (2017). "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata*, núm. 24, pp. 115-129.

Alguacil González-Aurioles, J. (2006). "Objeto y contenido de los Derechos Fundamentales: presupuestos e implicaciones de una nueva diferenciación dogmática", en *Teoría y realidad constitucional*, núm. 18, pp. 305-320.

Álvarez García, V. J. y Tahirí Moreno, J. (2023). "La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque", en *Revista General de Derecho Administrativo*, núm. 63.

Arellano Toledo, W. (coord.) (2023). *Derecho, Ética e Inteligencia Artificial,* Tirant lo Blanch, Valencia.

Asís Roig, R. F. de (2022). "Ética, tecnología y derechos", en Garrido Martín, J. et al. (dirs.): *Inteligencia artificial y Filosofía del derecho*, Laborum, pp. 91-114.

Autoridad Catalana de Protección de Datos (2017). *Guía práctica sobre la evaluación de impacto relativa a la protección de datos*. https://apdcat.gencat.cat/es/documentacio/guies_basiques/Guies-apdcat/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

Balaguer Callejón, F. (2020). "Crisis sanitaria y Derecho Constitucional en el contexto global", *Teoría y Realidad Constitucional*, núm. 46, pp. 121-140.

— (2021). "La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital", en Gomes, A. C. y otros (coords.). *Direito*

Constitucional: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho. Belo Horizonte: Fórum.

— (2022). *La constitución del algoritmo*, Fundación Manuel Giménez Abad. https://www.fundacionmgimenezabad.es/publicaciones/la-constitucion-del-algoritmo

Balaguer, F. y Cotino, L. (2023). *Derecho público de la inteligencia artificial, F. Jiménez Abad-Marcial Pons.* Acceso completo.

Barocas, S. y Selbst, A. D. (2016). *Big Data's Disparate Impact*, 104 *CAL. L. REV.* 671, 692-93.

Barrio Andrés, M. (2023). *El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo*, Real Instituto Elcano, ARI 34/2023, 20 abril. https://media.realinstitutoelcano.org/wp-content/uploads/2023/04/el-cumplimiento-basado-en-el-riesgo-o-risk-based-compliance-pieza-cardinal-del-nuevo-derecho-digital-europeo-real-instituto-elcano.pdf

Bastida, F. J. y otros (2004). *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, capítulo 8 (B. Aláez Corral), pp. 182 y ss. https://www.unioviedo.es/constitucional/miemb/pdf/librodf.PDF

Brandusescu, A. y Sieber, R. (2023). "Omments on Preliminary Discussions with the Government of Canada on Council of Europe Treaty Negotiations on Artificial Intelligence", 31 de agosto. https://ssrn.com/abstract=4559139.

Bustamante Domas, J. (2001). "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica", *Revista Interamericana de Ciencia, Tecnología, Sociedad e Innovación* (septiembre / diciembre).

Castellanos Claramunt, J. (2023) (coord.). *Inteligencia artificial y democracia; garantías, límites constitucionales*, Atelier, Madrid.

— (2023). "Una reflexión acerca de la influencia de la inteligencia artificial en los derechos fundamentales", en Ramón Fernández, F. *Ciencia de datos y perspectivas de la inteligencia artificial*, Tirant lo Blanch, Valencia, pp. 271-300.

Castillo Parrilla, J. A. (2023). "Privacidad de grupo: un reto para el derecho a la protección de datos a la luz de la evolución de la inteligencia artificial",

Derecho Privado y Constitución, núm. 43, 2023, pp. 53-88. https://doi.org/10.18042/cepc/dpc.43.02

Chaveli Donet, E. "Evaluaciones de impacto de derechos fundamentales sobre sistemas de inteligencia artificial", en *Tratado sobre el Reglamento... cit.*

Chueca Rodríguez, R. L. (dir.) (2015). *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid.

Citron, D. K. (2007). "Technological Due Process", *85 Wash. U. L. Rev*. pp. 1249-1313, pp. 1254 y ss., p. 1286. http://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2

Comisión Europea (2020). *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza, COM(2020)* 65 final, Bruselas, 19.2.2020. https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

Consejo de Europa (2022). *Guide on Article 13 of the European Convention on Human Rights. Right to an effective remedy, actualizado el 31 de agosto de 2022.* https://ks.echr.coe.int/web/echr-ks/article-13

Costa, J., Ávila, R. y Fernández Aller, C. (2023). *Derechos digitales en Iberoamérica: situación y perspectivas, Fundación Carolina y Telefónica.* https://www.fundacioncarolina.es/wp-content/uploads/2023/03/DERECHOS-DIGITALES_FC-2.pdf

Cotino Hueso, L. (2018). "La necesaria actualización de los derechos fundamentales como derechos digitales ante el desarrollo de internet y las nuevas tecnologías", en AA. VV. *España constitucional (1978-2018). Trayectorias y perspectivas*, Vol. III, CEPC, Madrid, pp. 2347-2361. Acceso en www.cotino.es

— (2019). "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho" en *Revista Catalana de Derecho Público,* núm. 58, junio. http://revistes.eapc.gencat.cat/index.php/rcdp/issue/view/n58

— (2019). "Riesgos e impactos del big data, la IA y la robótica y enfoques, modelos y principios de la respuesta del Derecho", Boix Palop, Andrés y Cotino Hueso, L. (coords.). *Monográfico Derecho Público, derechos y transparencia*

ante el uso de algoritmos, IA y big data, RGDA Iustel, núm. 50, febrero. Acceso en completo https://bit.ly/37RifyJ

— (2019). "Derechos y garantías ante el uso público y privado de inteligencia artificial, robótica y big data", en Bauzá, M. (dir.), *El Derecho de las TIC en Iberoamérica*, FIADI, La Ley-Thompson-Reuters, Montevideo, pp. 917-952. http://links.uv.es/BmO8AU7.

— (2020). "ONLINE-OFFLINE. Las garantías para el acceso a internet y para la desconexión, bloqueo, filtrado y otras restricciones de la red y sus contenidos", *Revista De Derecho Político*, núm. 1(108), pp. 13-40. https://doi.org/10.5944/rdp.108.2020.27991

— "Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", en *Derechos y garantías ante la inteligencia artificial*...cit, pp. 69-105.

— (2023). "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", en Gamero Casado, E. (dir.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia. Acceso capítulo. Acceso obra.

— "Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en Balaguer, F. y Cotino, L., *Derecho público de la inteligencia artificial*... cit.

— "The Council of Europe's Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law", en *CERIDAP Journal*, Issue núm. 2/2024, https://ceridap.eu/en/issues/

— (2024). "El Convenio sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho del Consejo de Europa", *Revista Administración y Cidadanía*, EGAP, actualizado en https://papers.ssrn.com/sol3/Delivery.cfm/4942383.pdf?abstractid=4942383&mirid=1

— (2024). "La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial", *Diario La Ley*, enero. https://ir.uv.es/V14YNLl

— (2022). (coord..). *La Carta de Derechos Digitales*, Tirant lo Blanch, Valencia.

Cotino Hueso, L. (ed.) (2022). *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Thompson-Reuters Aranzadi, Cizur.

Cotino Hueso, L. y Simón Castellanos, P. (coords.) (2024). *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi.

Cotino Hueso, L. "Derechos ante la administración digital y la inteligencia artificial (XVIII y XV)", en Cotino Hueso, L. (ed.): *La Carta de Derechos Digitales*, cit..., pp. 251-284. Acceso.

Crawford, K. y Schultz, J. (2014). *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV., p. 125.

De Tullio, M. F. (2016). "La privacy e i big data verso una dimensione costitizionale collettiva", *Politica del diritto*, Vol. 47, núm. 4, pp. 637-696.

Escobar Roca, G. (2018). *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid.

Fjeld J. et al. (2020). "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI", Berkman Klein Center for Internet & Society Research at Harvard University, enero. https://dash.harvard.edu/handle/1/42160420

Gascón Marcén, A. (2020). "Derechos humanos e inteligencia artificial", en Pérez Miras, A. y otros (dirs.), *Setenta años de Constitución Italiana y cuarenta años de Constitución*, Vol. 5, Retos en el siglo XXI, Romboli, S. (coord.), pp. 335-350.

Gavara de Cara, J. C. (2007). "La vinculación positiva de los poderes públicos a los derechos fundamentales", *Teoría y realidad constitucional*, núm. 20, pp. 277-320.

Gidi, A. y Ferrer Mac-Gregor, E. (2003). *Procesos colectivos. La tutela de los derechos difusos, colectivos e individuales en una perspectiva comparada*, México, Porrúa, p. 203.

Gobierno de España-De la Quadra, T. (coord.) (2021). *Carta de Derechos digitales*, julio. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Gobierno de Reino Unido (2023). *A pro-innovation approach to AI regulation*, Department for Science, Innovation and Technology and Office for Artificial Intelligence, 29 de marzo, actualización 3 de agosto. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

Gómez Abeja, L. (2022). "Inteligencia artificial y derechos fundamentales", en Garrido Martín, J. y otros (dirs.), *Inteligencia artificial y Filosofía del derecho*, Laborum, pp. 91-114.

Grupo del Artículo 29, (2017). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, 3 de octubre, versión final 6 de febrero de 2018, Doc WP251rev.01. https://www.aepd.es/documento/wp251rev01-es.pdf

— *Directrices sobre la evaluación del impacto de la protección de datos (DPIA) y determinar si el procesamiento es "probable que genere un alto riesgo" a los efectos del Reglamento 2016/679, WP248 rev.01, Revisadas por última vez y adoptadas el 4 de octubre de 2017.* https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

Gutiérrez García, E. (2024). *Inteligencia artificial y derechos fundamentales. Hacia una convivencia en la era digital*, Colex.

Hernández Peña, J. C. (2022). *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cízur, pp. 119-172 y también con especial atención a la gobernanza, pp. 173-206.

Hoffmann-Riem, W. (2019). *Big Data. Desafíos también para el Derecho*, Civitas, Madrid.

Jaume Palasí, L. (2020). "Cómo la inteligencia artificial está impactando en las sociedades", en Cerrillo i Martínez, A. y Peguera Poch, M. (coords.), *Retos jurídicos de la inteligencia artificial*, Aranzadi, Cizur, pp. 27-39, pp. 32 y 34.

Kammourieh, L et al. "Group privacy in the age of big data", en Taylor. L., Van der Sloot, B. y Floridi, L. (eds.), *Group Privacy... cit.,* capítulo 3, pp. 48-83. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

López-Tarruella Martínez, A. "Vías de recurso para los particulares en el reglamento de inteligencia artificial", en Cotino Hueso, L. y Simón Castellanos, P. (coords.), *Tratado sobre el Reglamento ... cit.*

Madison, J. (1788). *The Federalist No. 51,* "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments", *Independent Journal*, Wednesday, February 6. https://www.constitution.org/1-Constitution/fed/federa51.htm

Mantelero, A. "Toward a New Approach to Data Protection in the Big Data Era", en Gasser U. y otros (dir.): *Internet Monitor 2014: Reflections on the Digital World,* Cambridge (MA), Berkman Center for Internet and Society at Harvard University, pp. 84 y ss.

— (2017). "From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era", en Taylor. L., Van der Sloot, B. y Floridi, L. (eds.), *Group Privacy: New Challenges of Data Technologies*, Springer, capítulo 8. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

— (2016). "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law & Security Rew,* Vol. 32, núm. 2, pp. 238-255. DOI:10.1016/j.clsr.2016.01.014

— (2022). *Beyond Data. Human Rights, Ethical and Social Impact Assessment*, Springer, Information Technology and Law Series IT&LAW 36. https://link.springer.com/book/10.1007/978-94-6265-531-7

— *El big data en el marco del Reglamento General de Protección de Datos*, marzo, UOC, Barcelona, pp. 1-46.

Martín Retortillo, L. y de Otto y Pardo, I. (1988). *Derechos fundamentales y Constitución*, Civitas, Madrid, pp. 163 y ss.

Martínez Martínez, R. "Inteligencia artificial, Derecho y derechos fundamentales", en Quadra-Salcedo, T. de la (dir.), *Sociedad Digital y Derecho*, BOE-Red.es, pp. 259-278.

— (2019). "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista catalana de dret públic*, núm. 58, pp. 64-81.

Masferrer, A. (2017). "Derechos de nueva generación", en Enríquez, J. M., *Derechos humanos: un análisis multidisciplinar de su teoría y praxis*, pp. 331-358.

— (2022). *Dignidad y derechos humanos: un análisis retrospectivo de su formación en la tradición occidental*, Tirant lo Blanch.

Milione, C. y Cárdenas Cordón, A. (2020). "Dignidad humana y derechos fundamentales", *Derechos y libertades*, núm. 42, pp. 233-265, en especial pp. 262-263. DOI: 10.14679/1159. Entre otros, recientemente, Masferrer A. (2022), *Dignidad y derechos humanos: un análisis retrospectivo de su formación en la tradición occidental*, Tirant lo Blanc.

Ministro de Innovación, Ciencia e Industria. *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems.* https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

Navas Navarro, S. (2017). "Derecho e inteligencia artificial desde el diseño. Aproximaciones", Navas Navarro, S. (coord..): *Inteligencia artificial: tecnología, derecho*, Tirant lo Blanch, Valencia, pp. 23-72.

OCDE. *High-level AI risk-management interoperability framework*. https://oecd.ai/en/accountability

Olivares Olivares, B. D. "Law and Artificial Intelligence in the Spanish Tax Administration: the Need for a Specific Regulation", *European Review of Digital Administration* & Law-ERDAL 1 (1-2), pp. 227-234.

Palma Ortigosa, A. (2022). *Decisiones automatizadas y protección de datos personales. Especial atención a los sistemas de inteligencia artificial*, Dykinson.

Parlamento Europeo, (2017). *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo*, de 16 de febrero, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)) letra U. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES

— *Resolución de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)),* núm. 2 y considerando 12. Su anexo incluye una propuesta de Reglamento regulatorio. Ver su artículo 7.

Presno Linera, M. Á. (2023). "Teoría general de los derechos fundamentales e inteligencia artificial: una aproximación", en Balaguer Callejón, F. y otros

(coords.), *Derechos fundamentales y democracia en el constitucionalismo digital*, Aranzadi, Cizur Menor, pp. 461-491.

— (2023). *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid.

— (2023). "La propuesta de "Ley de Inteligencia Artificial" europea", *Revista de las Cortes Generales*, núm. 116, pp. 81-133.

Quintiá Pastrana, A. (2019). "Reforma del derecho y revolución digital. Las garantías sociales en la economía de plataformas", en Puentes Cociña, B. y Quintiá Pastrana, A., (coords.), *El derecho ante la transformación digital: oportunidades, riesgos y garantías*, Atelier, pp. 105-126, p. 111, cita p. 112.

Rallo Lombarte, A. "Una nueva generación de derechos digitales", *Revista de Estudios Políticos*, núm. 187, pp. 101-135. https://doi.org/10.18042/cepc/rep.187.04

Ramón Fernández, F. (coord.) (2022). *Los nuevos retos de los derechos digitales,* Tirant Lo Blanch, Valencia.

Recuero Linares, M. (2019). *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado, Premio AEPD.* https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf

RED DAIA (2020). *Aportación DAIA a consulta pública Carta de derechos digitales*, diciembre. https://bit.ly/3paF0H0

Riofrío Martínez-Villalba, J. C. (2014). "La cuarta ola de derechos humanos: los derechos digitales", *Revista Latinoamericana de Derechos Humanos,* Vol. 25 (1), I Semestre, pp. 15-45.

Rodríguez Ayuso, J. F. (coord.) (2023). *Retos, desafíos y oportunidades en materia de derechos digitales en un contexto de pandemia: visión multidisciplinar*, Thompson-Reuters Aranzadi, Cizur Menor.

Roig I Batalla, A. (2021). *Las garantías frente a las decisiones automatizadas del Reglamento general de Protección de Datos a la gobernanza algorítmica*, J. M. Bosch, Barcelona.

Salvador Martínez, M. (2001). "Sobre el contenido objetivo de los derechos fundamentales", en Aparicio, M. A. (coord.), *Derechos Constitucionales y Formas*

Políticas. Actas del Congreso sobre derechos constitucionales y Estado autonómico, Cedecs, Barcelona, pp. 199-219.

Sánchez Barrilao, J. F. (2016). "El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional", *Estudios de Deusto: revista de Derecho Público*, Vol. 64, núm. 2, pp. 225-258, p. 256.

— (2017). "Los fundamentos del "progreso informático" en la Unión Europea", *Revista de Derecho Político*, núm. 98, pp. 335-368. DOI: 10.5944/rdp.98.2017.18658

— (2023). "Inteligencia artificial y fuentes del derecho", *Revista de Derecho Constitucional europeo*, núm. 39.

Sarrión Esteve J. (2020). "El derecho constitucional en la era de la inteligencia artificial, los robots y los drones", Pérez Miras, A. y otros (dirs.), *Setenta años de Constitución italiana y cuarenta años de Constitución*, Vol. 5, Retos en el siglo XXI, Romboli, S. (coord.), pp. 321-334.

Simón Castellano, P. (2023). "Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial", *Revista de Derecho Político*, núm. 117, pp. 153-196.

— (2023). *La evaluación de impacto algorítmico en los derechos fundamentales*, Aranzadi, Cízur.

— "Los sistemas de gestión de riesgos como obligación específica para los sistemas de IA de alto riesgo", en *Tratado sobre el Reglamento... cit.*

Supervisor Europeo de Protección de Datos, SEPD (2015). *Dictamen 4/2015. Hacia una nueva ética digital. Datos, dignidad y tecnología*, 11 de septiembre, p. 15.

Terry Nicolas (2014). "Big Data Proxies and Health Privacy Exceptionalism", *Health Matrix nº 24*, pp. 65-108.

Troncoso Reigada, A. (dir.) (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales.*

Valle Escolano, R. (2023). "Inteligencia artificial y derechos de las personas con discapacidad", *Revista Española de Discapacidad (REDIS)*, Vol. 11, núm. 1, pp. 7-28.

Van der Sloot, B. "Regulating non-personal data in the age of Big Data", en Tzanou, M. (ed.), *Health data privacy under the GDPR: Big Data challenges and regulatory responses,* Routledge, pp. 85-105.

Wachter, S. y Mittelstadt, B. D. (2019). "A right to reasonable inferences: rethinking data protection law in the age of big data and AI", *Columbia Business Law Review*, Vol. 2019, núm. 2, pp. 494-620. https://ssrn.com/abstract=3248829

Ziller, J. "El Convenio del Consejo de Europa de Inteligencia Artificial frente al Reglamento de la Unión europea: dos instrumentos jurídicos muy diversos", en *Tratado sobre el Reglamento... cit.*

Capítulo 4
DERECHO PENAL Y DESAFÍOS DE LA INTELIGENCIA ARTIFICIAL (EN EL CONTEXTO DEL NUEVO MARCO REGULATORIO EUROPEO)[1]

Fernando Miró Llinares
Catedrático de Derecho Penal
Universidad Miguel Hernández de Elche
https://orcid.org/0000-0001-6379-5857

1. PRESENTE Y FUTURO DEL DERECHO PENAL ANTE LAS PROMESAS Y AMENAZAS DE LA IA

1.1. Tres desafíos para el Derecho penal derivados de la IA

No parece nada arriesgado afirmar que la Inteligencia Artificial (en adelante, IA), llegó para quedarse. Por decirlo de otro modo, su uso y su carácter de tecnología que va a marcar el desarrollo económico y social de las próximas décadas ya no está en discusión, lo único que aún desconocemos es su alcance y su impacto. Hoy podemos anticipar, también sin temor a errar, que sistemas de de IA como los vehículos sin conductor o la IA generativa cambiarán nuestras vidas, pero tampoco es difícil imaginar que vendrán muchos más cambios con la popularización de esta tecnología. Según la OCDE la IA, como conjunto de tecnologías que pretende desarrollar software y máquinas capaces de simular el actuar humano, tiene el potencial de mejorar el bienestar de las personas, contribuir a una actividad económica mundial sostenible y positiva y ayudar a responder a los principales retos mundiales debido a su potencial para aumentar

[1] Esta publicación es parte del proyecto de I+D+i TED2021-129356B-I00, financiado por MICIU/AEI/10.13039/501100011033 y por la "Unión Europea NextGenerationEU/ PRTR", y cuyo acrónimo es Ius_machinA.

innovación y la productividad[2]. Por ello se ha considerado necesaria para el desarrollo de sectores de gran impacto, como el sector público, las finanzas, la movilidad, los asuntos de interior y la agricultura, y particularmente para dar respuesta a retos como el de la crisis climática[3]. Las esperanzas sobre lo que esta tecnología puede aportar a la sociedad, a veces rayanas en un tecno optimismo cercano a la utopía, se basan en su potencial capacidad para mejorar la toma de decisiones, reduciendo el tiempo necesario para adoptarlas y otros costes, y minimizando los errores y sesgos inherentes al ser humano.

Estas promesas explican, también, al menos en parte, el enorme interés que el surgimiento de la tecnología de la Inteligencia Artificial causa en quienes se interesan por el ser y el deber ser del Derecho y la justicia penal. Cualquier tecnología con tanta capacidad transformadora a nivel social y fundada en promesas de eficiencia y mejora en la toma de decisiones, como es esta, interesa a una disciplina jurídica que se supone responsable de disuadir conductas lesivas o peligrosas para los intereses más relevantes para la sociedad y de hacerlo por medio de decisiones que deben suponer la aplicación del poder punitivo del Estado de forma adecuada y proporcionada. Es comprensible, pues, que ya se haya planteado su uso en la administración de justicia penal ante el augurio de mejores decisiones tanto para reducir la delincuencia como para responder justamente frente a ella.

Pero hay otro ángulo que da sentido al interés de la ciencia penal por los impactos de esta tecnología, uno que está en el reverso de las promesas asociadas a esta tecnología. Se relaciona con sus amenazas o con los riesgos que, desde la propia constatación de que la IA podía ser una realidad pronta, se asociaron a tales sistemas. Ya hace mucho aprendimos que desarrollo tecnológico y progreso no son sinónimos y que toda tecnología conlleva riesgos nuevos y también malos usos que producen daños. Y si nos fijáramos detenidamente en la evolución del interés académico por la IA desde la perspectiva del Derecho penal podremos ver cómo ha sido, precisamente, la sucesiva aparición de potenciales

---

[2] OCDE, *Recomendación del Consejo sobre Inteligencia Artificial*, adoptada el 22 de mayo de 2019.

[3] Exposición de motivos del Reglamento de Inteligencia Artificial (Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión, COM(2021)0206 – C9-0146/2021 – 2021/0106(COD).

riesgos asociados a la IA y el desarrollo de la inquietud sobre los mismos lo que ha ido trazando los intereses de la ciencia penal en estos sistemas. Con los primeros desarrollos robóticos y particularmente con la conducción autónoma, surgió la preocupación por la responsabilidad penal ante los resultados lesivos perpetrados por Robots o máquinas más o menos autónomas[4]. Con la aparición de sistemas algorítmicos predictivos y su uso, primero en el ámbito policial y luego a nivel judicial, y el riesgo de que estos sistemas estuvieran sesgados y pudieran ser discriminatorios, comenzó el interés académico por lo que se denominó *predictive policing*[5], y con el caso Loomis por el denominado *predictive sentencing*[6]. Luego la aparición de fenómenos claramente ligados al uso de tecnologías de IA en el ciberespacio como la desinformación y la propagación de bulos por medio de *bots* programados y los consiguientes riesgos para la democracia y otros intereses protegidos, generó un interés por la tecnología que se ha acrecentado en los últimos años debido al desarrollo de la IA generativa, la irrupción de los *Deep fakes* y, en particular, los primeros casos de ultrafalsificaciones de tipo sexual que afectaban a menores[7]. Al fin y al cabo, es esta una tecnología en evolución y conforme nuevos desarrollos de la misma van dando lugar a nuevos riesgos, el interés va mutando. De hecho, el mayor interés en los últimos años lo vuelven a suscitar de nuevo los robots y sus potenciales resultados lesivos, por un lado debido a los nuevos desarrollos de las armas letales autónomas y la posibilidad de brechas de responsabilidad ante los daños causados por drones armados y similares[8] y, por

---

[4] Hallevy, G. (2010). "The criminal liability of artificial intelligence entities – from science fiction to legal social control", en *Akron Intellect Property Journal, 4:171-201;* Quintero Olivares, G. (2017), "La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas", en *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS*, núm. 1, p. 1. De la Cuesta Aguado, P. (2016), La ambigüedad no es programable: racionalización normativa y control interno en inteligencia artificial. Revista de Derecho y Proceso Penal 44:165-194.

[5] Miró Llinares, F. (2020). "Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement", *IDP: Revista de Internet, derecho y política= revista d'Internet, dret i política*, núm. 30, p. 5.

[6] Martínez Garay, L. (2018). "Peligrosidad, algoritmos y due process: El caso State vs. Loomis", *Revista de Derecho Penal y Criminología* 20, 485-502.

[7] Simó Soler, E. (2018). "Retos jurídicos derivados de la inteligencia articial generativa", *InDret*, Santisteban Galarza, M. (2024). "La criminalización de las ultrafalsificaciones (con especial atención a las implicaciones de la normativa europea de servicios digitales e inteligencia artificial)", en *Revista de Derecho Penal y Criminología, 3ª época, núm. 31, págs. 211-249*

[8] Del Rosal Blasco, B. (2023). "¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial?", *REDEPEC: Revista*

otro, por la aparición de una potencial necesidad de proteger penalmente a los primeros robots con apariencia humana o de criminalizar los malos tratos a los mismos u otros actos relacionados con ellos[9].

Pero más allá de esa razonable tendencia reactiva de la academia ante las promesas y, particularmente, las amenazas, derivadas de la popularización de esta tecnología, hay otro tipo de razón que justifica sobradamente una reflexión profunda desde el Derecho penal sobre la IA. Se trata, de la constatación de que esta tecnología supone un reto para el Derecho penal tal y como se entiende y aplica en la actualidad, y tanto para la disciplina teórica como para su aplicación práctica. Y, aunque son muchas y diversas las transformaciones que vendrán con estos sistemas que podrían obligar a una adaptación de los esquemas y modelos teóricos y prácticos del Derecho penal, y aunque sólo podamos anticipar algunas de ellas, creo que ya pueden anticiparse al menos tres desafíos evidentes.

El primero de ellos tiene que ver con la aparición de un agente nuevo como potencial implicado en la determinación de responsabilidad penal. La IA, como disciplina científico-tecnológica que busca el desarrollo de máquinas que sean capaces de actuar de forma similar a los seres humanos, está en desarrollo y aunque ya ha servido para crear software y máquinas capaces de desarrollar acciones concretas ordenadas por humanos (IA débil), anuncia la posibilidad de crear en el futuro sistemas que actúen de forma autónoma con capacidades equivalentes o muy similares a la actuación humana (IA general) e incluso superiores (superinteligencia). El sistema penal está pensado como forma de comunicación normativa con los seres humanos motivándolos y disuadiéndoles de la realización de conductas que socialmente han sido consideradas disvaliosas y peligrosas o lesivas de intereses individuales o colectivos. La aparición de un agente nuevo que no sea considerado persona humana pero que interaccione en la causación de daños o en la creación de riesgos supone un reto para un sistema de responsabilidad como el penal. Si, con la responsabilidad de las personas jurídicas, ya se tuvo que adaptar un paradigma de la responsabilidad penal, el de *societas delinquere non potest*, la posibilidad de que haya entes que tomen decisiones de las que no pueda respon-

---

Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance 2.2: 4.

[9] Véase, entre otros, Darling, K. (2016). "Extending legal protection to social robots: The effects of anthropomorphism, empathy, and violent behavior towards robotic objects." *Robot law*. Edward Elgar Publishing, 213-232, y Mamak, K. "Should criminal law protect love relation with robots?", *AI & SOCIETY* (2022): 1-10.

sabilizarse a personas físicas o jurídicas y, sin embargo, resulten lesivas de bienes jurídicos dignos de protección, plantea un evidente desafío para el sistema penal que deberá quizás establecer las condiciones que hagan que una IA sea agente del derecho penal cuando merezca serlo y, mientras, dotarse de las estrategias necesarias para seguir sirviendo como sistema de responsabilidad que actúa con capacidad preventiva y atendiendo al merecimiento frente a lo causado.

Independientemente de que el desarrollo tecnológico de la IA en un futuro más o menos cercano determine la adaptación general, más o menos profunda, del sistema general de responsabilidad penal, el Derecho penal se enfrentará en los próximos años a un segundo desafío: el de adaptar el catálogo de figuras delictivas para dar respuesta adecuada a los nuevos riesgos y daños relacionados con los desarrollos ya existentes de esta tecnología. No es arriesgado predecir que la IA llevará, en las próximas décadas, a múltiples reformas de los códigos penales nacionales. Esencialmente porque tanto en sus desarrollos futuros como en los presentes tiene enormes potencialidades de ser usada para la perpetración de delitos. Todo desarrollo tecnológico novedoso es susceptible de ser usado para cometer o para facilitar la perpetración de actividades delictivas, y habrá que revisar que los sistemas penales, anclados bajo la necesaria exigencia de taxatividad derivada del principio de legalidad penal, den adecuada respuesta a nuevas formas de comisión de delitos por medio de IA. También que lo hagan de forma proporcionada a la nueva gravedad que el uso de esta tecnología puede suponer. De hecho, el reto incluye que la criminalización de nuevas conductas sea sólo el estrictamente necesario para que no dificulte el desarrollo de unas tecnologías que pueden producir cambios sociales positivos.

Hay, a mi parecer, un último desafío particularmente evidente que plantea la Inteligencia Artificial al Derecho penal. La IA también puede dar lugar a la aparición de nuevos intereses y valores dignos de tutela que, antes de que esta tecnología les diera sentido, no requerían una protección por medio del Derecho penal. Más allá de la funcionalidad y del valor económico de esta tecnología, es evidente que la transformación que supone la IA está cambiando la relevancia de los datos, otorgando un significado social a lo que sólo parecía un valor individual. También es claro que conforme los sistemas de IA se acerquen a aquello a lo que se aspira en el desarrollo de esta tecnología, la autonomía y la separación del actuar humano, comenzaremos a plantearnos la consideración como entes dignos de tutela de nuevos entes artificiales. Y probablemente surgirán muchos otros intereses, relacionados con la dignidad humana o con valores sociales diversos, conforme esta

tecnología vaya siendo parte de nuestras vidas. El desafío, por tanto, es que el sistema penal sea capaz de adecuar sus preceptos para dar una respuesta proporcionada a los nuevos daños a intereses nuevos o a manifestaciones nuevas de bienes jurídicos similares a los ya existentes. Y este reto incluye, al igual que sucedía con el desafío anterior, que el sistema penal sea capaz de responder a tales necesidades manteniendo su carácter de instrumento último, por ser el más lesivo, de los del estado para la tutela de los bienes jurídicos dignos de protección, sin caer, como en tantas otras ocasiones, en excesos de criminalización.

El presente trabajo pretende dar una visión de estos desafíos que la IA plantea para el Derecho penal. El objetivo, sin embargo, no es, como en otros trabajos, el de llevar a cabo una mera descripción de los problemas, ni tampoco el de aportar una introducción general a los mismos. Hay elementos para ir más allá y tratar de aportar una primera visión comprensiva de los posibles efectos que esta tecnología tendrá en cada uno de ellos. Por un lado, la tecnología está más madura y ya ha aportado muestras de sus posibilidades y de algunos de sus riesgos. Por otro, el proceso regulatorio ha comenzado, y aunque no haya entrado en vigor, el Reglamento 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial ya ha sentado bases normativas muy relevantes que pueden marcar la deriva de los procesos de criminalización que más pronto o más tarde llegarán. El hecho de que esta normativa europea ya establezca prohibiciones administrativas de usos de algunos sistemas de IA nos obliga a plantearnos cuál será el rol del Derecho penal en todo ello y cómo nuestro sistema se nutrirá de esta primera regulación, y de otras que vendrán, para tratar de evitar los peligros de la IA. Este es el principal objetivo de un trabajo que, por tanto, trata de centrarse en el impacto de la IA en el propio Derecho penal a la luz de las primeras formas de regulación extrapenal.

Antes de todo ello, sin embargo, resulta esencial cerrar una cuestión sólo aparentemente sencilla y de relevantes implicaciones para todo lo posterior, la de la definición de Inteligencia Artificial precisamente a la luz del citado texto normativo.

1.2. A vueltas con la definición de IA (y sus implicaciones para el alcance del impacto en el sistema penal)

Es llamativo que exista consenso acerca del enorme impacto económico y social que tendrá en un futuro próximo la IA, también sobre los muchos riesgos que su uso puede conllevar y que, en cambio, no lo haya acerca de su definición.

Hay varias razones que explican el disenso, relacionadas con que estemos ante una tecnología en evolución y con el hecho de que, a nivel normativo, la definición puede determinar qué sistemas son objeto de prohibición y cuáles ni siquiera están regulados. Pero lo cierto es que existe y es problemático. Aunque la discrepancia procede ya del nivel académico en el que las definiciones e interpretaciones sobre el alcance de la tecnología son diversas[10], y también los organismos internacionales ofrecen definiciones similares pero con matices distintos entre sí[11], donde más claramente se ha mostrado el "problema de la definición de IA" es en la tramitación del Reglamento Europeo de IA, con la discrepancia definitoria entre las propuestas de la Comisión Europea y las enmiendas a la misma que proponía el Parlamento europeo.

La Comisión definía sistema de IA como "el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I[12] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"; mientras que el parlamento proponía como definición de IA "un sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y capaz, para objetivos explícitos o implícitos, de generar información de salida –como predicciones, recomendaciones o decisiones– que influya en entornos reales o virtuales". Las diferencias se hacen explícitas en el considerando 6 de la propuesta, y en la idea de autonomía: mientras que la comisión entiende entre

---

[10] Véase, por todos, Zanol, J., Buchelt, A., Tjoa, S. y Kieseberg, P. (2022). What is "AI"? Exploring the scope of the "artificial intelligence act". https://jusletter-it.weblaw.ch/dam/publicationsystem_leges/iris2022/zanoal_et_al_what_is_ai.pdf

[11] Por su parte el Grupo de Expertos de Alto Nivel de la Unión Europea define la IA como sistemas de software y, potencialmente, hardware, creados por humanos que, con un fin complejo, actúan en entornos físicos o digitales a través de la recolección e interpretación de datos, razonando y decidiendo las acciones más adecuadas para alcanzar el objetivo establecido. Estos sistemas pueden aprender de la experiencia y modificar su comportamiento.

[12] Concretamente el anexo se refiere a las siguientes técnicas y estrategias de inteligencia artificial: a) Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo; b) Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico); y c) Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización.

los sistemas de IA aquellos software con capacidad para generar predicciones y recomendaciones y sostiene que los mismos pueden diseñarse para operar con distintos niveles de autonomía "y utilizarse de manera independiente o como componentes de un producto", la propuesta del parlamento hace expresa mención a que la autonomía exige que los sistemas de IA deben tener "al menos cierto grado de independencia de las acciones de los controles humanos y ciertas capacidades para operar sin intervención humana. A nivel de la discusión en el propio seno de la Unión Europea, la diferencia entre la propuesta de definición de la comisión y la del parlamento se centra, pues, en la introducción de la idea de la autonomía de los sistemas (que variaría en su nivel y adaptación, pero sería consustancial a la IA). Existe, por tanto, un acuerdo claro en que los sistemas de IA son máquinas que proponen y actúan a través de cálculos y operaciones, software a los que se les introduce inputs y que generan outputs en forma de recomendaciones o decisiones en la realidad. Hasta ahí el consenso. El potencial disenso se sitúa en la idea de autonomía, introducida para diferenciar estos sistemas "de otros sistemas de software o enfoques de programación más sencillos"[13]: la IA, por su particular capacidad de aprendizaje, razonamiento o modelización, tiene algún nivel mínimo de autonomía en el sentido "que tengan, al menos, cierto grado de independencia en sus acciones respecto de los controles humanos y cierta capacidad para operar sin intervención humana".

Pese a que pueda parecer que estamos ante una diferencia de matiz, creo que es obvio que uno u otro entendimiento de lo que es IA tiene repercusiones de cara a lo que una u otra tecnología supone en relación con el sistema penal. Es obvio que a nivel de lo que la IA puede implicar en cuanto a una necesaria adaptación del sistema de responsabilidad, no es lo mismo que estemos hablando de sistemas con autonomía que de sistemas sin capacidad de operar sin intervención humana. Es cierto, en todo caso, que, como ha señalado Chesterman, cuando hablamos de la autonomía de la IA no buscamos atribuir, "a la Kant", una relación íntima, libre o racional entre acción y agente, sino simplemente describir que hay partes de la acción en las que no ha participado el ser humano. Para determinar si hay autonomía y cuánta hay, habrá, pues, que responder "a un conjunto variado de preguntas acerca de cómo y con qué salvaguardas se está transfiriendo la autoridad humana para la toma de decisiones a una máquina". De ahí

[13] Ammendment 18 of the parlament to the recital 6 of the commission.

la idea de "diferentes niveles" en las definiciones de la OCDE y el Parlamento Europeo y de ahí también la tradicional diferenciación entre IA débil, IA general e IA fuerte o Superinteligencia.

Finalmente, el Reglamento de IA ha acabado definiendo sistema de IA en su artículo 3 como "un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales". Más allá de que parece evidente, tanto por el texto del citado precepto como por el del considerando que extiende el sentido del mismo, que se ha acabado imponiendo una visión más cercana a lo pretendido por el Parlamento Europeo, estamos ante una definición amplia que aún tendrá que ser desarrollada y precisada en la práctica y que puede dar cabida a desarrollos actuales y futuros, englobando: a) IA débil o específica, que aprende automáticamente para ejecutar tareas concretas; b) IA general, inexistente hasta la fecha, que comprendería cualquier tarea humana; y c) IA fuerte o Super IA, que excede las capacidades humanas. Por ello, a los efectos de este trabajo se adoptará, también, una interpretación amplia de la propia definición de IA que ha llevado a cabo la UE en el Reglamento de Inteligencia artificial. Es claro que los cambios más significativos en el sistema de justicia penal serán impuestos por las tecnologías de IA más avanzadas. También que los sistemas autónomos conllevarán más impactos al sistema de responsabilidad. Pero los desafíos y amenazas de la IA contemporánea, incluso de aquella sobre la que se podría discutir si realmente actúa autónomamente o de forma automatizada, ya son suficientemente relevantes como para que no sean obviados. Y puesto que el objetivo de este trabajo es aproximarnos a la comprensión de la posible transformación del Derecho penal ante el desarrollo tecnológico, adoptar un entendimiento amplio nos permitirá concretar en cada supuesto si será una u otra tipología o una u otra característica asociada a la tecnología la que tendrá uno u otro impacto para el Derecho penal.

2. DELITO, RESPONSABILIDAD PENAL E IA

2.1. Daños y peligros causados por/mediante el uso de sistemas de IA

Los beneficios potenciales de la IA se han asumido y hoy el uso de sistemas automatizados basados en esta tecnología parece imparable en muchos ámbitos

sociales. Y todo ello es, a su vez, compatible con que cada vez sean más evidentes también los riesgos individuales y colectivos que el uso de esa tecnología puede conllevar. El Comité de Ministros del Consejo de Europa ha reconocido la necesidad de supervisar las aplicaciones algorítmicas, debido al papel que desempeñarán en la sociedad, y la Unión Europea ha reconocido que algunos usos de la IA pueden poner en riesgo bienes y derechos fundamentales y en el Reglamento de Inteligencia Artificial se explicitan usos directamente prohibidos de esta tecnología. El reglamento considera sistemas de IA de riesgo inaceptable, por entenderlos una amenaza para los seres humanos, los que permiten la alteración conductual a través de la cognición; también los sistemas de identificación biométrica y de reconocimiento facial obtenidos de la web o cámaras de seguridad; los sistemas de detección de emociones en entornos laborales y educativos; los sistemas de calificación de los ciudadanos; o sistemas de categorización biométrica para deducir datos sensibles como la preferencia sexual o convicciones religiosas; y ciertas formas de supervisión predictiva por parte de las autoridades policiales.

Y esto son sólo sistemas de IA, potencialmente nocivos, que podrían ser comercializados y que la UE quiere prohibir. Pero, más allá de ellos, la observación de la realidad ya nos muestra que la IA puede causar múltiples daños y peligros y que, de hecho, puede ser usada para perpetrar delitos de todo tipo. En el informe general de la Asociación Internacional de Derecho penal múltiples países han reportado numerosos crímenes perpetrados con el uso de IA[14]. Por citar algunos significativos, en China ya ha habido cibercrímenes afectando a la intimidad y a otros intereses sociales perpetrados con el uso de la IA, como en 2018 cuando los cibercriminales usaron programas basados en IA para entrometerse en un sistema de información informático o cuando utilizaron sistemas de IA para recopilar los números de teléfono de los clientes y cotejar los nombres y otra información de los propietarios a través de medios técnicos para identificar a las personas violando los datos personales de múltiples usuarios[15]; en Ucrania se creó un chatbot para, a través de la red social Telegram,

---

[14] Miró-LLinares, F. (2024). "General Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds).: RIDP, Vol. 94 issue 3, Penal law and criminalization of AI offences, International Colloquium Section II, Bucharest, 13-16 June.

[15] Wang, X, Bai, L. (2024). "Chinese Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C y Tudorel, T. (eds.). (2024), *RIDP,*

facilitar la venta automática de sustancias psicotrópicas y droga generando automáticamente información para el comprador sobre el lugar, la forma de pago, el tipo y el número de drogas y sustancias psicotrópicas[16]; y en múltiples países se han reportado ya casos de accidentes de tráfico en los que se vieron implicados vehículos autónomos[17]. También la desinformación, íntimamente ligada con el uso de sistemas de IA, se ha convertido en una amenaza evidente en los últimos años para bienes jurídicos tan importantes como el propio orden democrático o la salud pública durante la pandemia[18] y la tecnología de los Deep fakes podría profundizar el problema. De hecho, la irrupción durante el último año de la IA generativa ha dado lugar a la aparición de relatos sobre conductas suicidas relacionadas con el uso de chatbots, atentados terroristas en grado de tentativa donde el chatbot incitaba a la comisión de magnicidio, y aún más supuestos de creación de ultrafalsificaciones[19]. Los denominados deepfakes, tal y como ha señalado Santisteban Galarza, han sido usados según Europol para llevar a cabo varios fraudes y para perpetrar extorsión[20], o para atentar contra el honor y/o la libertad sexual contra personalidades musicales[21]

Vol. 94, issue 3, *Penal law and criminalization of AI offences*, International Colloquium Section II, Bucharest, 13-16 June.

[16] Karchevskyi, M. y Radutniy, A. (2023). "Ukranian Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds). (2023), *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences*, International Colloquium Section II, Bucharest, 13-16, June.

[17] Miró Llinares, F. (2024). "General Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds).: *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences*, International Colloquium Section II, Bucharest, 13-16 June.

[18] Miró-Llinares, F, y Aguerri, J. C. (2023). "Misinformation about fake news: A systematic critical review of empirical studies on the phenomenon and its status as a 'threat'." *European Journal of Criminology* 20.1: 356-374.

[19] Véase, Santisteban Galarza, M. (2024). "La criminalización de las ultrafalsificaciones...", ob. cit., con especial atención a las implicaciones de la normativa europea de servicios digitales e inteligencia artificial, en *Revista de Derecho Penal y Criminología, 3ª época, núm. 31, enero, pp. 211-249.*

[20] Miró Llinares, F. (2024). "General Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds.), *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences*, International Colloquium Section II, Bucharest, 13-16 June.

[21] https://www.eldiario.es/blog/micromachismos/rosalia-fotos-manipuladas-mostraban-desnuda-cuerpo-mujer-no-mercancia-estrategia-marketing_132_10235525.html

o contra menores de edad como en el conocido caso de la generación de imágenes sexuales en Extremadura.

Estos, y otros muchos, son ejemplos de una realidad que aún podría considerarse casi testimonial pero que, en breve, cuando se generalice aún más el uso de estos sistemas, dejará de serlo. Ante estos nuevos daños y riesgos surge la cuestión de si el sistema penal, entendiendo por el mismo tanto el conjunto de sistemas normativos que aplican el *ius puniendi* estatal como las instituciones formales que aplican el mismo, responde adecuadamente a estos nuevos daños y peligros. En este apartado me ocuparé de lo primero, de la cuestión de si el Derecho penal está adaptado, o si debe adaptarse, a los nuevos retos que plantea la IA. Ello implica analizar cuestiones como si el sistema penal debe ser reformado de cara a escenarios en los que los sistemas de IA puedan ser considerados autónomos y deban ser hechos responsables de sus actos; o de cómo responden los sistemas de responsabilidad penal actuales a los daños ya producidos causados por la IA; y también si es necesario adaptar las concretas figuras delictivas del Código Penal o incluir nuevas para dar respuestas a los nuevos daños causados por la IA o a la necesidad de tutela de nuevos intereses. Estas y otras cuestiones están íntimamente relacionadas entre sí pero pueden ser agrupadas en, por un lado, la cuestión de la adaptación del sistema general de responsabilidad, aquello que tradicionalmente se ha denominado la parte general del Derecho penal y que incluye la teoría general del delito y, por otro, la cuestión de la adaptación del catálogo de delitos de cada Código Penal a las necesidades de protección penal derivadas del escenario que plantea la irrupción de la IA.

2.2. Responsabilidad penal e Inteligencia artificial

2.2.1. La cuestión de la adaptación del sistema general de responsabilidad

Todas las revoluciones tecnológicas que han existido en los últimos años, desde la del tráfico rodado, la revolución genética o la digital con la aparición de Internet, han supuesto adaptaciones de la legislación penal, pero ninguna de ellas ha llevado a que se sugiriera la necesidad de adaptar el sistema general de responsabilidad. La de la IA sí lo ha hecho, aunque, como veremos, más como un escenario a futuro que de presente. La razón de que, al menos, se plantee una transformación del sistema, una palingenesia del Derecho penal tradicional y de sus categorías, tal y como Picotti ha inquirido (para luego responder negativamente), tiene que ver, como he dicho anteriormente, con la potencial irrupción de un nuevo sujeto

potencial de responsabilidad penal, la IA o la máquina, como agente separado del ser humano[22]. Siendo, como es la IA, una tecnología real pero también aspiracional que trata de imitar las capacidades de los seres humanos y de crear sistemas que pueden interactuar con cierta autonomía con los humanos (IA débil) y, más allá, entes que actúen con total autonomía frente a estos (IA general), es razonable que el Derecho penal, centrado en la prevención de conductas humanas que pongan en peligro intereses sociales dignas de tutela, se plantee su adecuación a uno y otro escenario. Estamos, por tanto, ante la cuestión de la autonomía de la IA, la singularidad de esta tecnología que cuestiona la capacidad del sistema tradicional de responsabilidad penal para responder adecuadamente a daños y peligros asociados a esta tecnología. Pero, puede advertirse claramente, a mi parecer, que el problema tiene dos dimensiones distintas según estemos hablando de una u otra IA. Por un lado, tendríamos el problema de la posible consideración de una agencia moral-penal en el sistema de IA, pensando en sistemas de IA general o de superinteligencias a las que pueda atribuirse aquello que las convirtiera en auténticos agentes morales capaces de responsabilidad penal. El otro sería el problema atribucional al único agente moral-penal por la introducción de la actuación de un no-agente moral que pueda afectar a la previsibilidad del primero. Dado que los sistemas de IA son cada vez más autónomos y su funcionamiento, aún no siendo considerado totalmente autónomo del actuar de quienes lo diseñan o producen, puede resultar imprevisible para quienes lo desarrollan, programan, producen, distribuyen y utilizan, se trata de valorar si la aparición de estos entes conlleva un problema para el modelo de responsabilidad penal pensado para estos últimos. Voy a prestar atención a ambos problemas por separado.

a) La IA, ¿Agente susceptible de responsabilidad penal?

Dado el estado actual en el que se encuentra la tecnología de la IA existe un total consenso entre la comunidad científica del Derecho penal en considerar que no existe fundamento para el reconocimiento de personalidad jurídico-penal a ningún sistema actual de IA[23]. Pese a que son muchos quienes aseguran que pronto se darán las condiciones de posibilidad para la existencia de sistemas

---

[22] Picotti, L. (2022). "General Report on Traditional Criminal Law Categories and AI", Picotti, L. y Panattoni, B. (eds.). *RIDP,* Vol. 94 issue i, *Traditional Criminal Law Catyegories and AI: Crisis or Palingenesis?* International Colloquium Section I, Siracusa, 15-16, September 2022.

[23] AIDP, Resolution on Traditional Criminal Law categories and AI, pp. 54 y ss.

artificiales capaces de asimilar los procesos mentales humanos y de actuar conforme a aprendizajes propios, o incluso generar otros diferentes a los existentes hoy en día en las personas[24], lo cierto es que hoy las IA débiles funcionan básicamente como modelos matemáticos sin capacidad para el razonamiento complejo y apenas para aprender autónomamente del entorno y adaptarse a él[25]. Como señalé en otro lugar, la autonomía no es una cualidad dicotómica sino una dimensión continua, por lo que no será sencillo determinar cuándo el actuar de un sistema de IA es autónomo con respecto al del agente humano[26]. Sin embargo, ninguno de los tres modelos de IA en la actualidad atendiendo al grado de interacción hombre-máquina, se corresponden con una máquina autónoma, en el sentido de un agente moral capaz de merecer algún tipo de responsabilidad penal. Ni el caso de *Man in the loop*, en el que la IA necesita aportes humanos para la toma de decisiones, ni el modelo *Man on the loop*, cuando la máquina es capaz de actuar por sí misma a partir de una programación pero el humano puede intervenir interrumpiendo o modificando las acciones del robot en cualquier momento, como tampoco el modelo *Man out of the loop,* en el que la máquina actúa de manera independiente durante ciertos períodos de tiempo y, en estos intervalos, el ser humano no tiene influencia sobre las acciones del robot[27]. La autonomía moral pertenecería a un modelo distinto, digamos "*No man on the loop",* en el que las decisiones de la IA se originarían no a partir de intervenciones humanas, sino del aprendizaje autónomo de la propia máquina o de otra máquina que actúa como "maestra", o en el que el actuar de la IA se independizaría de enseñanzas y decisiones preprogramadas y respondería a factores intrínsecos al sistema. En la mayoría de los sistemas de IA contemporáneos, es el humano quien configura el proceso de aprendizaje, eligiendo las situaciones específicas a las que se enfrenta la IA y su

---

[24] Holland, O. (2004). "The future of embodied artificial intelligence: Machine consciousness?", en Lida, F., Pfeifer, R., Steels, L. y Kuniyoshi, Y. (eds.): *Embodied artificial intelligence,* Springer, Berlin, pp. 37-53.

[25] Lida, F., Pfeifer, R., Steels, L. y Kuniyoshi, Y. (eds.) (2004). *Embodied artificial intelligence,* Springer, Berlin, pp. 1-26.

[26] Miró Llinares, F. "AI and criminal law reform: notes on the inadequacy of a criminalization model based on a substantive principle", en prensa.

[27] El otro modelo es *Man in the loop,* cuando la IA necesita aportes humanos a intervalos de tiempo regulares para poder llevar a cabo sus acciones, Harbers, M., Peeters, M. M. y Neerincx, M. A., "Perceived autonomy of robots: Effects of appearance and context", en Aldinhas Ferreira, M. I., Silva Sequeira, J., Tokhi, M. O., Kadar, E., y Virk, G. S. (eds.) (2017), *A World with Robots,* Springer, Cham, pp. 19-33.

respuesta a un conjunto limitado de estímulos, y es también el ser humano quien omite ciertas consideraciones en la programación de la máquina, aunque, como veremos, algunos modelos de aprendizaje autónomo apuntan en otra dirección. En todo caso la posibilidad de interacción humana en tiempo real tan sólo es una parte de lo que podríamos denominar autonomía la cual, en el sentido que le estamos otorgando, sólo provendría de la capacidad real de adaptar las decisiones a un contexto distinto de aquel para el que ha sido programada.

Y es que, efectivamente, hay una dimensión de la autonomía ligada con la actuación moral que puede llevar a un reproche penal que, por lo menos con lo que existe ahora, no se da en los sistemas de IA: su falta de autoconciencia y, por tanto, de capacidad de actuar "en libertad" conforme a distintos escenarios. Este sería el problema ontológico de los sistemas de IA para ser considerados agentes morales susceptibles de responsabilidad penal: el tratarse de sistemas que carecerían de conciencia y de capacidad de autodeterminación a la hora de elegir y evaluar las posibles soluciones a un problema y también a un mandato normativo[28]. Es esto lo que los hace imposibles para la consideración de actores capaces de actuar en libertad y, por tanto, capaces de reproche moral y penal. Esto está relacionado, a su vez, con las funciones del Derecho penal y, en particular, las funciones de la pena. Sin entrar en la discusión profunda sobre el debate actual de la función de la pena, difícilmente se puede decir, sin retorcer en exceso el sentido de cada una de las teorías, que los sistemas de IA puedan darle sentido como agentes a ninguna de las funciones que se han atribuido a la sanción penal. Desde la perspectiva de la retribución o de las modernas teorías comunicativas normativas cercanas a ellas[29], los sistemas de IA carecen de la conciencia y la dignidad exigidas para que puedan merecer el reproche por el daño que puedan haber causado; y desde la perspectiva de las teorías preventivas los sistemas de IA no son capaces de motivarse autónomamente ante la amenaza de un castigo o ante la conformación individual de cuál debe ser el modelo correcto de actuación ante un supuesto caso. La IA no tiene capacidad de merecimiento ni de prevención general, ni positiva ni negativa, ni especial.

---

[28] Véase en este sentido la Recomendación 4 de la Resolution on traditional..., ob. cit., p. 55.

[29] Miró Llinares, F. M. (2021). "La salud del debate sobre la pena: Primeros síntomas tras una revisión sistemática de la literatura (2000-2020)", en VV. AA.: *El Derecho penal ante lo "empírico": Sobre el acercamiento del Derecho penal y la Política Criminal a la realidad empírica,* pp. 43-72, Ediciones Jurídicas y Sociales.

Es verdad que esto podría cambiar en el futuro. La evolución del aprendizaje profundo, de la IA generativa y de otros modelos matemáticos complejos sugiere la potencial emergencia de sistemas informáticos capaces de aprender y funcionar de manera autónoma y de contemplar la eventual realidad de una IA con capacidades de superinteligencia que nos llevaría a repensar su capacidad para actuar con conciencia y autodeterminación. Más allá de si esa IA de nivel humano podría ser una realidad en unos 20, 50 o 100 años, será esa evolución tecnológica de las capacidades de aprendizaje de esos sistemas lo que podría determinar que en un futuro las sociedades consideren que hay máquinas capaces de actuar como entidades con libre albedrío o incluso con capacidad moral y lo que, por consiguiente, llevaría a un reconocimiento potencial de una forma de identidad (artificial) para las IA autónomas lo que podría llevar a hacerlas responsables en el ámbito penal. Esto iría en paralelo, además, a la protección de estas entidades de IA, en cuanto que cuando sean consideradas capaces de cometer actos delictivos y ser reprochadas por ello probablemente también se considere que tales sistemas sean dignos de una tutela especial y se les dote de derechos similares a los de los seres humanos separados de su potencial económico o funcional-social.

Pero creo que estamos aún lejos de lo que realmente constituiría una IA autónoma. La IA actual, aquella que realiza recomendaciones y automatiza algunas decisiones previamente determinadas por seres humanos a partir de un conjunto de datos existente y de la identificación en ellos de patrones y probabilidades[30], no exige un replanteamiento del sistema penal como sí podría hacerlo un ente idealmente "autónomo. Y, sin embargo, esta IA ya plantea suficientes retos en relación con el sistema de responsabilidad general del Derecho penal como para que los obviemos en disquisiciones más abstractas[31]. Como advirtió Surden, es necesario que no olvidemos las discusiones dogmáticas y político criminales en torno a la IA de hoy, con sus capacidades y limitaciones, en vez de sólo teorizar sobre sistemas hipotéticos que aún no sabemos si surgirán o qué características tendrán[32].

---

[30] Russell, S. J., y Norvig, P. *Artificial intelligence...*, ob. Cit.

[31] En tal sentido Hallevy, G. (2013). "*When Robots kill, Artificial Intelligence under Criminal Law*", Northester University Press, New England.

[32] Surden, H. (2019). "Artificial Intelligence and Law: An Overview", G*eorgia State University Law Review,* Vol. 35.

b) Responsabilidad penal ante daños causados mediante una IA "autónoma"

Afirmar que los sistemas de IA en la actualidad no conllevan la aparición de un nuevo agente moral penal que obligue a revisar el sistema global de responsabilidad penal, no es incompatible con aseverar que las categorías, modelos teóricos e instituciones tradicionales de responsabilidad penal deben ser reevaluados y adaptados a los retos que plantea esta tecnología. En particular, el problema que plantea la introducción de sistemas de IA tiene que ver con la dificultad que puede suponer atribuir responsabilidad penal al ser humano por los daños causados cuando esta tecnología ha participado en el proceso causal. Ya hemos dicho que los sistemas de IA no son autónomos en términos morales, pero sí pueden tener algún nivel mínimo de autonomía funcional, en el sentido de algún grado de independencia en sus acciones del control humano. Cada vez se están asignando más tareas a los sistemas de IA, algunos de ellos opacos y/o complejos, de modo que su funcionamiento pueda resultar difícil de prever para quienes lo usan, para los que lo distribuyen y producen e, incluso, también para quienes los diseñan y programan. La cuestión que surge ante ello, pues, es si el sistema de atribución de responsabilidad penal responde bien ante estas situaciones o debe ser adaptado y de qué modo.

Para resolver esta cuestión resulta fundamental relacionar la cuestión de la autonomía, como cesión de la agencia sobre parte de la decisión, con un proceso mayor que es el que lleva a la creación y al uso de IA: la automatización de procesos decisorios y la cesión a las máquinas de la ejecución de partes de ellos. Si algo promete la IA es la automatización de cualquier proceso de toma de decisiones basado en datos debido a la alta capacidad de cálculo, a la alta fiabilidad de los mismos y a la cantidad y diversidad de variables que pueden ser analizadas. Los procesos clásicos de toma de decisiones, basados en la interacción de diferentes agentes humanos con distintos conocimientos y responsabilidades destinadas a tomar las decisiones más adecuadas en función de determinados fines, al ser apoyados o sustituidos por sistemas de IA, pueden verse afectados (teóricamente mejorados) tanto por el aumento de la rapidez en la que se decide, como por la mayor objetividad en las decisiones basadas en datos al eliminar el sesgo humano. Eso sí, cualquier automatización de procesos puede implicar un cambio en el "momento" en el que la agencia humana se vuelve crucial. Al automatizar procesos y decisiones, lo que hacemos es cambiar el momento de agencia humana del responsable: ya no situamos la misma cerca de la consecuencia o el resultado de la decisión, sino antes, cuando diseñamos el proceso que, por

medio de otros agentes, bien sean otros humanos o bien sean máquinas, llevará de forma (supuestamente) inevitable al resultado esperado. Cuando diseñamos un proceso decisorio y lo hacemos mal al no calcular bien sus consecuencias, el resultado está más lejos de nuestro actuar, pero sigue siendo nuestro, en cuanto seamos quienes tengamos el control (y la responsabilidad) sobre el mismo. Si a ello añadimos la introducción de un agente distinto al humano al que, se supone, no podemos transmitirle un control del que pueda hacerse responsable, lo que estamos haciendo es trasladar aún más claramente el momento clave de la responsabilidad a un lugar muy anterior a aquel que está cerca del daño.

La primera consideración relevante que debemos hacer de cara a la cuestión de la atribución de responsabilidad penal por daños causados mediante el uso de un sistema de IA, es que con el uso de sistemas de IA el momento clave en el que se desencadena la responsabilidad ya no se situará, por lo general, cerca de la exteriorización del daño o del riesgo. En su lugar, las primeras etapas del ciclo de vida de la IA, como el diseño del algoritmo o la selección de los datos que alimentarán el sistema, serán más relevantes para el Derecho penal en la mayoría de los escenarios. Esto puede explicarse por el hecho de que es en esas etapas en las que los daños o riesgos pueden preverse y prevenirse[33]. Con la IA, la selección de los propósitos de los algoritmos o de lo que formará el contexto (y el contenido) de su toma de decisiones, se vuelve decisiva en la forma en que la IA "actúa". Por esta razón, lo lógico es que los sistemas normativos que determinen la responsabilidad deban tener en cuenta esos momentos clave (y los competentes para cada uno de ellos) para atribuirla, si bien es cierto que estos son muy anteriores a aquellos que tradicionalmente suelen ser relevantes para el Derecho penal.

Hay una segunda consideración relevante relacionada con que la automatización de procesos que se lleva a cabo con el uso de sistemas de IA generalmente incluye (en aras de incrementar la eficiencia o reducir los costes) la cesión de una o varias de las partes del proceso a un ente capaz de "actuar autónomamente". Aquí es donde la idea de autonomía entra en juego: cuando se transfiere la decisión, o parte de ella, a la máquina, y elementos claves del actuar se dejen en

---

[33] Eso es claramente lo que está ocurriendo en relación con el debate sobre la regulación de los vehículos autónomos. Véase, con profundidad y ejemplos, Miró Llinares, F., "General Report on Penal law and criminalization of AI offences", Miró-LLinares, F, Santisteban-Galarza, M; Duvac, C; Tudorel, T (eds. (2024), *RIDP*, Vol. 94 issue 3, *Penal law and criminalization of AI offences,* International Colloquium Section II, Bucharest, 13-16 June.

manos de un ente no humano que, en tal sentido de no actuar bajo una supervisión humana, es autónomo. Si tenemos en cuenta, además, que un elemento esencial de esta tecnología sería la capacidad de aprender por sí misma y de actuar conforme a ese aprendizaje, esto podría suponer, según algunos autores, que nos encontráramos con daños causados por sistemas de IA en los que no pudieran atribuirse responsabilidad ni a los diseñadores, desarrolladores, fabricantes o comercializadores (por haber sido perpetrados en el marco de la autonomía de las máquinas y no ser capaces de prever el daño) ni tampoco a estas por tratarse de agentes "no morales" a los que no se puede atribuir responsabilidad[34]. Es esta supuesta idea de las "lagunas de responsabilidad" que pueden derivarse de la dificultad de atribución de responsabilidad por algunos daños causados por máquinas autónomas, lo que ha llevado a un sector de la doctrina a sostener la necesidad de revisar el sistema de responsabilidad penal[35]. Otros, en cambio, entienden que ello no es necesario, bien porque las obligaciones de control pueden subsanar las supuestas lagunas de responsabilidad[36], o bien porque tenemos que aceptar que allí donde no haya bases suficientes para la responsabilidad penal no puede haberla por mor del principio de legalidad[37].

Más allá de la interesante discusión terminológica y de fondo sobre las potenciales lagunas de responsabilidad a las que podría llevar el uso de sistemas de IA autónomos, creo que lo señalado hasta el momento pone de manifiesto dos cuestiones: La primera, que quizás en breve se tipifiquen delitos que sancionen actos preparatorios relacionados con la producción, comercialización y diseño de sistemas de IA autónomos que, por la falta de previsibilidad y control en sus

---

[34] Danaher, J. (2019). *Automation and Utopia: Human Flourishing in a World without Work,* Harvard University Press.

[35] Así, Danaher, J. (2016). "Robots, law and the retribution gap". *Ethics and Information Technology, 18*(4), 299-309, y especialmente Sparrow, R. (2007), "Killer robots". *Journal of Applied Philosophy, 24*(1), 62-77. Se ha opuesto a ello König, quien señala, añadiendo una reflexión que a mi parecer tiene mucho interés, que resulta poco plausible suponer que el alto grado de autonomía de un sistema autónomo permita exculpar comportamientos negligentes o malintencionados de sus diseñadores Königs, P. (2022), "Artificial intelligence and responsibility gaps: what is the problem?". *Ethics Inf Technol* 24, 36. https://doi.org/10.1007/s10676-022-09643-0

[36] Hindriks, F. y Veluwenkamp, H. (2023). "The risks of autonomous machines: from responsibility gaps to control gaps". *Synthese* 201, 21. https://doi.org/10.1007/s11229-022-04001-5

[37] Navarro Dometsch, R. (2023). "Brechas de responsabilidad penal y entes inteligentes artificiales", texto manuscrito presentado en el Congreso Internacional "Sistema penal, inteligencia artificial y su regulación", Universidad Católica de Maule (Talca, Chile), 29 y 30 de noviembre.

acciones, constituyan un riesgo grave para bienes jurídicos relevantes. Sobre esto volveré más adelante al tratar la cuestión de la criminalización. La segunda, que el sistema de responsabilidad penal puede ser adecuado para dar respuesta a los daños causados cuando se usan sistemas inteligentes autónomos, si bien la justificación y argumentación de esta responsabilidad puede resultar aún más compleja de lo habitual. Es el momento de dar, aunque sea a modo de pincelada, algunas claves sobre los retos que plantea la misma.

Pues bien, en primer lugar, parece evidente que el uso de sistemas de IA y la atribución de responsabilidad por los daños causados en relación con el mismo nos obliga a mirar la responsabilidad de todos los implicados en las distintas fases del ciclo de vida de la IA. Desde los múltiples diseñadores y programadores de cada uno de los algoritmos que pueden conformar un proceso de decisión compleja, pasando por los proveedores de los datos, los productores, vendedores y distribuidores de los productos, será esencial no sólo definir la contribución de cada uno de ellos sino su rol a la luz de las obligaciones sectoriales del sistema de IA de que se trate (coche autónomo, dron, etc.) para poder determinar si actúan dentro del riesgo permitido. También habrá que atender a lo realizado por el usuario final del sistema de IA, si bien la responsabilidad en su caso tampoco excluirá la de los demás si se puede decir que, por acción u omisión, han contribuido a la cadena causal por medio de un riesgo prohibido. La clave, en todo caso, para atribuir responsabilidad a cada uno de ellos, será poder comprobar quién (o quiénes) ha infringido la concreta posición personal de deber en relación con el conjunto de competencias asignadas en las distintas fases del ciclo de vida de los sistemas de IA.

En segundo lugar, parece también evidente que no será la causación de daños dolosa por medio de sistemas de IA lo que planteará problemas en cuanto a la atribución de responsabilidad penal, sino que en la mayoría de supuestos el título de imputación más usado a la vez que problemático será la imprudencia. Y aquí, como ha señalado la AIDP, lo primero que hay que decir es que la responsabilidad penal por conductas negligentes de personas que han actuado usando sistemas de IA deberá ajustarse a los principios generales del Derecho penal, en concreto al principio de culpabilidad personal[38]. Esto implica que no deberá bastar

[38] AIDP, Resolution on Traditional Criminal Law categories and AI, pp. 54 y ss. Véase, también, con más detalle, Picotti, L.: "General Report on Traditional Criminal Law Categories and AI", Picotti, L, Panattoni, B (eds.) (2024), *RIDP,* Vol. 94 issue i, *Traditional Criminal Law*

con la conexión objetiva entre la contribución causal del agente humano y la comisión del delito por el sistema de IA, sino que habrá que probar tanto que el agente podría haber previsto el resultado como que tenía capacidad para evitar el mismo. Esto puede ser muy relevante en el caso de que consiga demostrarse que, efectivamente, algún tipo de aprendizaje autónomo del sistema de IA impedía la previsibilidad o la evitabilidad del hecho ilícito. Además de ello, y conectando este punto con el anterior, la responsabilidad por negligencia tendrá que relacionarse con el modo en que se estructura y opera el agente artificial en relación con todos los intervinientes en el hecho. Si se adoptaron medidas de vigilancia; si se entrenaron los algoritmos con muestras adecuadas teniendo en cuenta el ámbito de aplicación del sistema de IA de que se trate; si se tenía conocimiento por alguno de los diseñadores de resultados imprevistos; si había transparencia en el algoritmo para que los que lo usaran pudieran adaptar su aplicación a contextos de riesgo, etc. Y todo ello teniendo en cuenta el riesgo permitido según lo establecido en las obligaciones específicas de seguridad y normas cautelares a aplicar a las actividades de diseño, desarrollo, producción, distribución y venta, así como de uso de los sistemas de IA[39].

En tercer lugar, no todos los sistemas autónomos plantearán los mismos problemas para la atribución de responsabilidad ni para todos los sistemas autónomos se establecerán las mismas obligaciones de control y supervisión. Es claro, por un lado, que habrá que tener en cuenta el nivel de autonomía decisoria, en el sentido de separación del actuar de la máquina respecto del actuar humano, de cada sistema de IA. Para determinar esto, habrá que atender a cómo queda la supervisión humana y qué modelo se adopta atendiendo a ella, si *man in the looop, man on the loop* o *man out of the loop*, pero también el distinto tipo de automatización en el aprendizaje, la capacidad de introducción de datos y de adaptación de los mismos al algoritmo por parte de la IA, y la capacidad de explicabilidad y la propia transparencia de los algoritmos usados. Lo razonable es que haya mayores obligaciones de control en diseñadores, programadores y productores allí donde, por las citadas características, el proceso decisorio quede más alejado de la conducta de riesgo y la IA tenga, en ese sentido, más autonomía más cerca del potencial daño. También

---

Catyegories and AI: Crisis or Palingenesis? International Colloquium Section I, Siracusa, 15-16, September 2022.

[39] Véase en este sentido, AIDP, Resolution on Traditional Criminal Law categories and AI, pp. 55 y ss.

habrá que tener en cuenta, en todo caso, la relevancia del bien jurídico que puede ser puesto en peligro o dañado por el sistema autónomo, en cuanto que las obligaciones de control y supervisión serán mayores cuando estén en juego bienes como la vida o los derechos fundamentales.

Todo esto, en cualquier caso, si pone algo de manifiesto es el evidente carácter secundario que el Derecho penal va a tener en estos ámbitos. Incluso para la atribución de responsabilidad penal por daños causados por estos sistemas será determinante lo que establezcan las regulaciones sectoriales a nivel nacional e internacional en el diseño y producción de cada uno de los sistemas. Es cierto, como ha señalado Beck, que estas normativas pueden tener su propia lógica que no se corresponda exclusivamente con la prevención de peligros sino con la no afectación del mercado, y que la jurisprudencia penal irá limando también tales exigencias normativas[40], pero en esta fase de desarrollo de la IA es especialmente necesario que aparezcan normativas como el Reglamento Europeo de Inteligencia Artificial que, desde una perspectiva de cuáles son los bienes que pueden estar en riesgo, establezca obligaciones concretas que sirvan para determinar, en caso de incumplimiento, quien debe responsabilizarse también penalmente de los daños causados.

Y queda una última consideración. Hasta el momento hemos planteado cómo impactará el uso de sistemas de IA a la atribución de responsabilidad penal a personas físicas pero, como es sabido, en Derecho penal también son responsables penalmente las personas jurídicas y si a ello sumamos que gran parte de los sistemas de IA son producidos o utilizados por personas jurídicas, parece evidente que estas también podrán ser hechas responsables de los delitos cometidos usando dichos sistemas. La tendencia a la hiper normativización de *soft law* y Derecho administrativo a la que va a someterse la creación y uso de herramientas de IA muy probablemente llevará a que las empresas que usen robots o sistemas predictivos algorítmicos tengan que actualizar sus programas de cumplimiento para evitar la responsabilidad en el caso de que una IA en su seno cause daños. El *compliance* seguirá siendo, pues, un modo de prevenir riesgos, pero deberá adaptarse a los nuevos peligros de estas herramientas. Por otro lado, y como señalé en otro lugar, los propios programas de cumplimiento pueden

---

[40] Beck, S. (2016). "Intelligent agents and criminal law-Negligence, diffusion of liability and electronic personhood." *Robotics and Autonomous Systems* 86, 138-143.

beneficiarse en su desarrollo de estas herramientas[41]. La datificación y automatización del proceso de valoración del riesgo de perpetración de delitos está, probablemente, mucho más cerca gracias a esta tecnología.

Por otra parte, y como ha puesto de manifiesto la AIDP, el que los sistemas de IA no pueden ser hechos responsables penalmente de los daños causados, puede hacer que sea recomendable la aplicación de medidas accesorias o preventivas que sirvan para evitar o reducir los efectos nocivos de algunos sistemas de IA. Como ha sido señalado, medidas como la incautación, el decomiso, la vigilancia judicial o las medidas interdictivas, pueden ser adecuadas dada la potencial gravedad de los daños que pueden ser causados por una IA, y, en particular, el decomiso, permitiría actuar directamente contra el sistema de IA con el que o por el que se cometió el delito, sin necesidad de reconocerle personalidad jurídica o capacidad penal[42].

2.2.2. La cuestión de la criminalización de nuevas conductas ante los riesgos de la IA

Es común que la aparición de nuevas esferas de riesgo emergentes de revoluciones tecnológicas, como ocurrió con la automoción, la biotecnología y ahora con la inteligencia artificial (IA), ejerzan presión sobre el marco de responsabilidad penal existente y el legislador responda a la misma creando nuevas tipificaciones delictivas. Es muy posible, pues, que conforme se consoliden los daños y riesgos asociados a la IA presenciemos reformas en el Código Penal que incluyan la instauración de nuevas figuras delictivas o la modificación de las actuales. El argumento subyacente para justificar tales reformas es la necesidad de protección de los bienes jurídicos que podrían verse perjudicados por el avance de esta tecnología, ya que tradicionalmente se busca sancionar conductas para prevenir daños o riesgos a bienes merecedores de protección legal. Partiendo de esta base, hay dos motivos principales que podrían impulsar una reforma en la legislación penal especial: por una parte, la necesidad de salvaguardar nuevos intereses sociales que no están completamente relacionados con los actualmente protegidos por

---

[41] Miró Llinares, F. (2022). "Inteligencia artificial, delito y control penal: nuevas reflexiones y algunas predicciones sobre su impacto en el derecho y la justicia penal", *El Cronista del Estado Social y Democrático de Derecho* 100, 174-183.

[42] AIDP, Resolution on Traditional Criminal Law categories and AI.

el derecho penal, y por otra, la utilización de la IA como instrumento para atentar contra bienes jurídicos ya resguardados, en cuyo caso los delitos tipificados hasta ahora podrían no ser aplicables a las nuevas modalidades de conducta, requiriendo así una actualización legislativa. De lo primero me ocuparé en la siguiente sección. Me centraré, a continuación, en la potencial reforma del catálogo de delitos debido a la aparición de nuevos riesgos o daños a los bienes jurídicos ya considerados dignos de tutela. Lo haré atendiendo, primero, a unas consideraciones generales sobre la criminalización de nuevos delitos relacionados con la IA y, después, atendiendo a la relación entre estas consideraciones y el futuro Reglamento de Inteligencia Artificial que puede resultar esencial para indicar los ámbitos de riesgo y los riesgos no permitidos que podrían definir el contenido de injusto de las futuras figuras delictivas tipificadas para responder a los retos de la IA.

a) Sobre criminalización y adelantamiento de barreras de protección en relación con el diseño y producción de sistemas de IA de riesgo

El Código Penal apenas necesitará reformas para dar respuesta al uso intencionado de sistemas de IA para causar daños a cualquier bien jurídico ya tutelado o considerado digno de tutela. El uso malicioso de sistemas de IA para perpetrar delitos puede ser sancionado penalmente y apenas requerirá modificaciones. Las potenciales adaptaciones y reformas de la parte especial del Código Penal en relación con bienes jurídicos ya existentes estarán relacionadas, más bien, con la aparición de nuevos riesgos a los mismos y con la consiguiente tipificación de conductas de infracción de deber peligrosas para tales intereses jurídicos. He mencionado antes, en particular, que, en el contexto de la IA, el instante crítico de la activación de la responsabilidad penal no coincide, como solía ser, con el momento en que se manifiesta el daño o el riesgo. Más bien, se ha desplazado hacia las fases iniciales del desarrollo de la IA, tales como la creación del algoritmo o la elección de datos que se utilizan para entrenar al sistema, las cuales adquieren mayor importancia en el ámbito penal en la mayoría de las situaciones. Esto se debe a que es durante estas fases preliminares donde se pueden identificar y mitigar potenciales daños o riesgos. La definición de las finalidades de los algoritmos y los datos que conforman el entorno de sus decisiones es determinante en el comportamiento de la IA. Por consiguiente, no es improbable que se considere la posibilidad de criminalizar acciones vinculadas a estas etapas tempranas, aunque estas se presenten mucho antes de los momentos tradicionalmente considerados adecuados en el Derecho penal. Y esto se ve aún más claro cuando volvemos a la cuestión del problema de

la "autonomía" de algunas acciones y tareas por parte de sistemas de IA. Ante sistemas de IA inteligentes, con capacidad para aprender de los datos del entorno y de modificar sus funciones y acciones[43], es posible que entremos en un escenario real en el que ya no podamos decir que los diseñadores y usuarios dispongan de una forma viable de predecir el comportamiento de estos sistemas, base esencial para determinar su responsabilidad negligente[44]. Ante ello, o se prohíben aquellos sistemas de IA que puedan proceder de ese modo como señala Sparrow[45], o se acepta que aquellas conductas quedan impunes y no se adopta una visión punitivista o, siguiendo la línea adoptada por Hindricks y Veluwenkamp, se entiende que las máquinas autónomas sólo pueden construirse de modo que presenten un nivel de riesgo moralmente aceptable, y si no alcanzan este nivel entonces se estarán infringiendo obligaciones de control[46]. Conforme a este último modelo, y como ocurre en otros ámbitos de especial riesgo, será probable que la intervención penal se anticipe a momentos alejados del daño, pero próximos a la acción humana responsable, creando nuevas figuras delictivas específicas por ejemplo relacionadas con las obligaciones de control.

Los Códigos Penales podrían, pues, sancionar actos de infracción de deberes administrativos, o conductas preparatorias que, en cualquiera de los casos, se considerase que entrañan riesgo suficiente para ser sancionadas de forma anticipada y autónoma, desvinculadas de la responsabilidad por los posibles hechos lesivos que pudieran producirse como consecuencia de los mismos. Conductas como la consistente en no mantener los niveles necesarios de normas de seguridad de actividades como las pruebas, la fabricación, la actualización, el control, etc., de

---

[43] Dice Asaro que ello, como tal, ya es posible con los sistemas de Machine learning en general, pero creo que habría que matizar mucho esa afirmación hasta el punto de dejarla casi sin sentido Asaro, P. M. (2016), "The Liability Problem for Autonomous Artificial Agents", Indurkhya, B. y Stojanov, G. (eds.), *AAAI Symposium on Ethical and Moral Considerations in Non-Human Agents,* Stanford, 21-23 March. USA: Association for the Advancement of Artificial Intelligence, pp. 190–194. Available from: https://www.aaai.org/ocs/index.php/SSS/SSS16/paper/view/12699 [Accessed 29 December 2018].

[44] Osmani, N. (2020). "The complexity of criminal liability of AI systems", *Masaryk University Journal of Law and Technology*, *14*(1), 53-82.

[45] Sparrow, R. (2007). "Killer robots", *Journal of Applied Philosophy, 24*(1), 62-77

[46] Hindriks, F., Veluwenkamp, H. (2023). "The risks of autonomous machines: from responsibility gaps to control gaps", *Synthese* 201, 21. https://doi.org/10.1007/s11229-022-04001-5

determinadas IA[47] que se sepan especialmente lesivas, u omisiones como la de no atender a determinadas precauciones por parte de los fabricantes de agentes autónomos o artificiales. Incluso la ocultación u obstaculización del acceso al tipo de programación utilizado por el sistema de IA[48], aunque no se haya producido ningún daño por tales incumplimientos, podría aspirar a convertirse no sólo en infracciones de deberes administrativos sino, allí donde se puede afirmar un riesgo grave, en nuevos delitos de peligro. En este caso estaríamos limitando la impunidad a aquellos casos en los que sí pueda decirse que, en aquellos momentos en los que se están diseñando y produciendo aquellas herramientas sobre las que es difícil prever el riesgo y que podrían ser incluso capaces de actuar con cierta autonomía, los agentes humanos han tratado de mantener todo el control posible y exigible para evitar resultados lesivos y no pueden ser hechos responsables de los mismos.

Más allá de la cuestión del posible adelantamiento de las barreras de protección relacionada con el uso de algunos sistemas de IA, hay otra cuestión general que debe ser planteada en relación con la posible reforma de la parte especial de los códigos penales debida a la irrupción de esta tecnología. Los sistemas de IA pueden amplificar la escala del daño relacionado con su funcionamiento o uso. Y, al igual que sucedió con la aparición del ciberespacio que trajo consigo un similar efecto de amplificar la escala del daño y de aumentar la posibilidad de afectación lesiva de la conducta a muchos más sujetos[49], habrá que plantearse no ya la posibilidad de crear nuevos delitos sino la adaptación de la penalidad de los existentes a la supuesta mayor gravedad de las conductas perpetradas con IA. Aquí la cuestión no es sólo de legitimidad (por proporcionalidad), sino de la técnica adecuada para lograrla: puede ser que el modo en que ya estén tipificados los delitos permita directamente la adaptación de la pena a aquellos supuestos

---

[47] Provaznick, J. "Czech Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds.) (2024), *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences,* International Colloquium Section II, Bucharest, 13-16 June.

[48] Miró Llinares, F. (2024). "General Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds.), *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences* International Colloquium Section II, Bucharest, 13-16 June.

[49] Flor, R., Gullo, A. (2024). "Italian Report on Penal law and criminalization of AI offences", Miró-LLinares, F., Santisteban-Galarza, M., Duvac, C. y Tudorel, T. (eds.) (2023), *RIDP,* Vol. 94 issue 3, *Penal law and criminalization of AI offences*, International Colloquium Section II, Bucharest, 13-16 June.

que sean realmente más graves, pero puede ser que la motivación/disuasión que busque la prevención de esas conductas obligue a una generalización de la agravación cuando se usen. En todo caso, realizar, per se, una asunción total de que el uso de esta tecnología conlleva mayor gravedad, por ejemplo, mediante la introducción de circunstancias agravantes que abarquen el uso de la IA, puede no ser una solución adecuada en cuanto que puede acabar equiparando en gravedad usos de IA que den lugar a una mayor lesividad de otros que no lo hagan.

Por supuesto, todo lo señalado no se dará del mismo modo en todos los ámbitos de riesgo. Es evidente que hay bienes jurídicos más relevantes que otros y, también, bienes que van a ser puestos más gravemente en peligro por la irrupción de esta tecnología que otros. Así, por ejemplo, el desarrollo de la tecnología de la conducción autónoma o la potencialidad lesiva de drones y otras armas letales autónomas sitúan a la vida y la salud como bienes jurídicos especialmente necesitados de protección y llevarán, muy probablemente, a la regulación específica de riesgos relacionados con la producción de estos sistemas que, probablemente, también acaben teniendo incidencia en la criminalización de algunas conductas de riesgo. El ciberespacio y la protección en el de bienes jurídicos como la privacidad y el patrimonio también constituye un ámbito en el que el desarrollo de la IA puede suponer retos del máximo interés. Y el uso de sistemas de IA ya se ha relacionado también con nuevos problemas como el de la desinformación que, en muchos países, está llevando a la criminalización de conductas de difusión de noticias falsas que pueden tener importantes repercusiones en la protección de las condiciones básicas de la democracia pero que, a su vez, puede conllevar también una excesiva criminalización que limite notablemente la libertad de expresión. Eso sí, y en todo caso, la tutela de intereses dignos de protección no puede ser, por sí misma, razón suficiente para la criminalización de conductas, sino que habrá que atender, además, a las posibilidades preventivas de otras ramas del ordenamiento jurídico y a la auténtica necesidad de protección penal para que la creación de nuevas figuras delictivas esté legitimada.

b) El Reglamento Europeo de Inteligencia Artificial y su posible impacto en la criminalización ante los retos de la IA

Lo señalado acerca de la posible tendencia a la criminalización de actos de diseño, producción y criminalización de sistemas de IA que conlleven riesgos para intereses dignos de tutela concuerda, a mi parecer, con el modelo que la UE ha adoptado para establecer prácticas prohibidas y de riesgo en el futuro Reglamento de Inteligencia Artificial. Aunque el Derecho penal sea autónomo

en el establecimiento de los riesgos que debe tratar de evitar por medio de la tipificación de delitos, es evidente que la regulación extrapenal de la IA será un indicador de qué usos de la IA pueden considerarse suficientemente peligrosos como para, incluso, plantearse su criminalización. Y el enfoque en el riesgo que ha adoptado el Reglamento de Inteligencia Artificial ya anticipa dos posibles vías de criminalización de conductas. Por un lado, tenemos la posibilidad de que los estados decidan sancionar penalmente conductas relacionadas con el desarrollo e implantación (por parte de aquellos a los que el Reglamento se refiere como proveedores) de sistemas de IA prohibidos. En particular el artículo 5 del futuro reglamento prohíbe el desarrollo en Europa de sistemas de IA que utilicen técnicas subliminales o manipulativas para alterar significativamente la capacidad de decisión de una persona, causando un daño considerable; de sistemas que se aprovechan de vulnerabilidades específicas de individuos o grupos para influir en su comportamiento causando perjuicios; de sistemas de clasificación de personas basándose en datos biométricos para inferir características personales sensibles, excepto en determinados supuestos relacionados con la aplicación de la ley[50]; sistemas para evaluar o clasificar socialmente a individuos o grupos en función de su comportamiento o características personales, que resulten en un trato desfavorable o injusto[51]; sistemas de identificación biométrica en tiempo real en espacios públicos para fines policiales, salvo para buscar víctimas de crímenes graves o prevenir amenazas significativas a la seguridad pública[52]; sistemas que evalúen

---

[50] Señala el artículo 5.1.b9, que esta prohibición "no cubre ningún etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente, como imágenes, basado en datos biométricos o categorización de datos biométricos en el ámbito de la aplicación de la ley".

[51] En particular cuando la puntuación social "conduzca a una de las siguientes situaciones o a ambas: a) trato perjudicial o desfavorable de determinadas personas físicas o grupos enteros de estas en contextos sociales que no guardan relación con los contextos en los que se generaron o recopilaron originalmente los datos; y b) el trato perjudicial o desfavorable, injustificado o desproporcionado con respecto a su comportamiento social o a la gravedad del mismo, de determinadas personas físicas o grupos de estas" Reglamento de IA art. 5.1.c).

[52] En concreto se establecen como excepciones: a) la búsqueda selectiva de víctimas concretas de secuestros, trata de seres humanos y explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas; b) la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas o una amenaza real y actual o real y previsible de atentado terrorista; y c) la localización o identificación de una persona sospechosa de haber cometido una infracción penal, con el fin de llevar a cabo una investigación penal, el enjuiciamiento o la ejecución de una sanción penal por las infracciones contempladas en el anexo II bis y castigadas en el Estado miembro de que se trate con una pena privativa de

el riesgo de que un individuo cometa un delito basado únicamente en su perfil personal; sistemas de IA que generen bases de datos de reconocimiento facial a través de la recolección indiscriminada de imágenes de internet o CCTV; o sistemas de IA para inferir emociones en el lugar de trabajo o en instituciones educativas, excepto cuando sean necesarios por razones médicas o de seguridad. Dada la potencial lesividad de estos sistemas, y siempre que el daño causado por medio de los mismos no pueda dar lugar a la aplicación de alguno de los preceptos existentes del Código Penal, no sería descartable la creación de delitos relacionados con la infracción de la citada prohibición en supuestos especialmente lesivos.

Pero el Reglamento de Inteligencia Artificial no sólo establece la prohibición de la comercialización de unos concretos sistemas, sino que define otros como de "alto riesgo", estableciendo unas exigencias normativas para quienes desarrollen los mismos. Sin pretender desgranar la compleja regulación que establece el reglamento para la determinación de qué sistemas de IA deberán ser considerados de alto riesgo y cuáles no, si considero que es importante hacer dos referencias a cómo esta relevante referencia para la normativa penal va a determinar qué es un sistema de IA de alto riesgo. Por un lado, en el Anexo 2 el Reglamento enumera sistemas de Alto riesgo por ámbitos. Así, 1) para la biometría, y en la medida en que su uso esté permitido por la legislación nacional, considera de alto riesgo los sistemas de identificación biométrica a distancia (excepto aquellos cuyo único propósito sea confirmar que una persona física específica es la persona que dice ser), los destinados a ser utilizados para la categorización biométrica, de acuerdo con atributos o características sensibles o protegidos, basados en la inferencia de dichos atributos o características, y los sistemas de IA destinados a ser utilizados para el reconocimiento de emociones. 2) En el caso de las infraestructuras críticas, identifica como de alto riesgo los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, tráfico rodado y suministro de agua, gas, calefacción y electricidad. 3) En la educación y formación profesional, señala a los sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión o para asignar personas físicas a instituciones educativas y de formación profesional a todos los niveles, los destinados a ser utilizados para evaluar los resultados del

libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años. El presente apartado se entiende sin perjuicio de lo dispuesto en el artículo 9 del RGPD para el tratamiento de datos biométricos con fines distintos de los policiales.

aprendizaje[53], los sistemas para la evaluación del nivel de educación que recibirá una persona y los sistemas usados para controlar comportamientos prohibidos de los estudiantes durante la evaluación de su educación. 4) En el ámbito del empleo, la gestión de trabajadores y el acceso al autoempleo, nombra los sistemas destinados a la contratación o selección de personas físicas, en particular para filtrar solicitudes y evaluar a los candidatos, y también los sistemas de IA destinados a ser usados para decidir sobre condiciones laborales, promocionar, asignar tareas o evaluar el rendimiento laboral. 5) En el campo del acceso y disfrute de servicios privados esenciales y de servicios y prestaciones públicos esenciales, incluye los sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar el derecho de las personas físicas a prestaciones y servicios esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios; también los sistemas de IA destinados a evaluar la solvencia de las personas físicas o a establecer su calificación crediticia, con excepción de los sistemas de IA utilizados para detectar fraudes financieros; los sistemas de IA destinados a evaluar y clasificar llamadas de emergencia de personas físicas o a utilizarse para enviar o establecer la prioridad en el envío de servicios de primera respuesta de emergencia, incluidos los de policía, bomberos y asistencia médica, así como de sistemas de triaje de pacientes de asistencia sanitaria de emergencia; y finalmente los destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con personas físicas en el caso de los seguros de vida y de enfermedad. 6) En el ámbito policial y de aplicación de la ley también se establecen una serie de usos de alto riesgo que detallaré más adelante cuando analice las potencialidades de la IA para la investigación y prevención del crimen[54]. 7) En lo relativo a la gestión de la migración, el asilo y el control de fronteras, se consideran sistemas de alto riesgo los destinados a ser utilizados para evaluar a las personas como polígrafos y herramientas similares, también los destinados a ser utilizados para evaluar un riesgo, incluido un riesgo para la seguridad, un riesgo de migración irregular o un riesgo para la salud, planteado por una persona física que pretenda entrar o haya entrado en el territorio de un Estado miembro; los destinados a ser

---

[53] Se añade que "incluso cuando dichos resultados se utilicen para dirigir el proceso de aprendizaje de personas físicas en centros de educación y formación profesional de todos los niveles". Anexo III, 3.b.

[54] *Vid.* Supra. III.

utilizados para asistir a las autoridades públicas competentes en el examen de las solicitudes de asilo, visado y permisos de residencia y las reclamaciones conexas en relación con la admisibilidad de las personas físicas que solicitan un estatuto, incluida la evaluación conexa de la fiabilidad de las pruebas; y, finalmente, los destinados a ser utilizados con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje; y todos ellos siempre que su uso esté permitido en virtud del Derecho de la Unión o nacional pertinente. 8) Finalmente, y en el campo de la administración de justicia y en relación con los procesos democráticos, se consideran sistemas de alto riesgo los destinados a ser utilizados por una autoridad judicial o en su nombre para asistir a una autoridad judicial en la investigación e interpretación de hechos y de la ley y en la aplicación de la ley a un conjunto concreto de hechos o utilizados de manera similar en la resolución alternativa de litigios; y los sistemas de IA destinados a ser utilizados para influir en el resultado de unas elecciones o referéndum o en el comportamiento electoral de personas físicas en el ejercicio de su voto en elecciones o referéndum[55].

Ninguno de estos sistemas, per se, van a dar lugar a una criminalización, pero sí constituyen una referencia ineludible para la determinación del riesgo permitido en el caso de que se decida que alguna de estas conductas merece ser considerada delictiva. No es difícil, de hecho, imaginar que la creación intencionada de alguno de estos sistemas ya pudiera ser considerada delictiva cuando se sea consciente del daño potencial producido. Tampoco que, si se entiende que los preceptos existentes, por no permitir la sanción del comportamiento imprudente o por otros motivos, no responden adecuadamente a los riesgos que conllevan algunos de estos sistemas, se adopten delitos para evitar sus efectos. En el caso de que así sea, sin embargo, debería relacionarse esta lista de sistemas de IA de riesgo del anexo III del Reglamento Europeo de Inteligencia Artificial con lo señalado por el artículo 7.2 del mismo reglamento, que establece de forma más clara cuáles son las bases de consideración de la existencia de un riesgo según este texto normativo.

---

[55] Se señala en el citado precepto que "no se incluyen los sistemas de IA a cuyos resultados no están expuestas directamente las personas físicas, como las herramientas utilizadas para organizar, optimizar y estructurar campañas políticas desde un punto de vista administrativo y logístico".

Establece el citado precepto del reglamento una serie de criterios para evaluar si un sistema de IA plantea un riesgo de daño para la salud y la seguridad o un riesgo de repercusión negativa en los derechos fundamentales "equivalente o superior al riesgo de daño que plantean los sistemas de alto riesgo mencionados en el anexo III". Con esto ya nos indica que tales sistemas son considerados de riesgo en relación con esos daños que, tradicionalmente, han sido considerados dignos de tutela penal. Pero, además, nos ofrece una serie de criterios muy interesantes para determinar tal riesgo a tales intereses, concretamente: (a) la finalidad prevista del sistema de IA; (b) la medida en que se ha utilizado o es probable que se utilice; (b bis) la naturaleza y la cantidad de los datos tratados y utilizados por el sistema de IA, en particular si se tratan categorías especiales de datos personales; (b ter) la medida en que el sistema de IA actúa de forma autónoma y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un daño potencial; (c) la medida en que el uso de un sistema de IA ya ha causado daños a la salud y la seguridad, ha tenido un impacto adverso en los derechos fundamentales o ha suscitado preocupaciones significativas en relación con la probabilidad de tales daños o impactos adversos, como demuestran, por ejemplo, informes o alegaciones documentadas presentadas a las autoridades nacionales competentes u otros informes, según proceda; (d) el alcance potencial de dicho perjuicio o de dicho impacto adverso, en particular en términos de su intensidad y de su capacidad de afectar a una pluralidad de personas o de afectar de manera desproporcionada a un grupo particular de personas; (e) la medida en que las personas potencialmente perjudicadas o afectadas negativamente dependen del resultado producido con un sistema de IA, en particular porque por razones prácticas o jurídicas no es razonablemente posible excluirse de dicho resultado; (f) la medida en que existe un desequilibrio de poder, o las personas potencialmente perjudicadas o con efectos adversos se encuentran en una posición vulnerable en relación con el usuario de un sistema de IA, en particular debido a su estatus, autoridad, conocimientos, circunstancias económicas o sociales, o edad; (g) la medida en que el resultado producido por un sistema de IA es fácilmente corregible o reversible, teniendo en cuenta las soluciones técnicas disponibles para corregirlo o revertirlo; los resultados que tengan un impacto adverso en la salud, la seguridad o los derechos fundamentales no se considerarán fácilmente corregibles o reversibles; (g ter) la magnitud y la probabilidad del beneficio del despliegue del sistema de IA para los individuos, los grupos o la sociedad en general, incluidas las posibles mejoras en la seguridad de los productos; y (h) la medida en que la legislación vigente de la Unión prevé

medidas eficaces de reparación en relación con los riesgos que plantea un sistema de IA, con exclusión de las reclamaciones por daños y perjuicios, o bien medidas eficaces para prevenir o minimizar sustancialmente dichos riesgos.

Estos elementos serán referencia para determinar cuáles son los riesgos que el Derecho penal puede considerar inaceptables y, por tanto, pueden determinar el adelantamiento de las barreras de protección siguiendo las consideraciones adelantadas en el punto anterior. También deberá tenerse en cuenta, en este caso, las obligaciones que los artículos 8 y ss. del reglamento establecen para los sistemas de IA de alto riesgo. Sin ser posible aquí realizar un detallado análisis de tales obligaciones, en ellas se establece una serie de obligaciones que deben cumplir los proveedores de esos servicios de IA para garantizar la conformidad de sus productos con la legislación europea y que incluyen la evaluación de los riesgos del sistema, abarcando toda la vida útil del sistema e incluyendo identificación, análisis, estimación y evaluación de riesgos; la gestión y mitigación de los mismos, implementando medidas de control y mitigación y formación a los implementadores; pruebas de sistema; pruebas en condiciones reales; medidas para la atención de potenciales impactos negativos en colectivos vulnerables; registro automático de actividades para garantizar un nivel de trazabilidad adecuado para identificar situaciones de riesgo, facilitar la monitorización del mercado y la operación del sistema; o medidas de supervisión humana que permitan la supervisión efectiva por parte de personas naturales, apuntando a prevenir o minimizar riesgos, y habilitar a los responsables para monitorizar su operación, interpretar salidas y, si es necesario, intervenir o interrumpir el sistema. Se señala en el reglamento que estos requisitos son vitales para asegurar que los sistemas de IA de alto riesgo sean seguros, fiables y respeten los derechos fundamentales a lo largo de toda su operatividad. A mi parecer estas obligaciones podrían constituir tanto una base interpretativa fundamental para determinar la posible responsabilidad imprudente en el caso de sistemas de alto riesgo que no cumplan las mismas, como para constituir potenciales bases de futuras criminalizaciones.

En todo caso debe quedar claro que, para pasar de la mera infracción de las obligaciones establecidas para los sistemas de alto riesgo conforme al Reglamento Europeo de IA a la criminalización, será necesario un análisis de legitimidad que parta de una primera exigencia relacionada con la puesta en peligro o la lesión de intereses dignos de tutela. En el caso de pretender criminalizar la distribución de algunos sistemas de IA especialmente lesivos o dañosos, estaríamos obligados a reflexionar si hay un interés digno de protección que se puede

ver dañado en el caso de que se realice la conducta. Para criminalizar la ausencia de control en el diseño y producción de ciertas IAs, deberíamos poder afirmar que la conducta que puede ser tipificada pone en peligro los bienes jurídicos dignos de tutela; y lo mismo se puede decir de la segunda técnica consistente en la ampliación del catálogo de conductas imprudentes, en cuanto constituya una forma similar de recurrir a una anticipación de la protección penal. Pero hará falta, además, que podamos decir que el Derecho administrativo no es suficiente para lograr la prevención necesaria y que se requiere de la intervención penal para la tutela adecuada de los intereses dignos de protección. El Derecho penal debería quedar esencialmente para evitar la creación y diseño de sistemas de IA que planteen riesgos elevados para determinados bienes jurídicos significativos y sólo en caso de que estemos ante un peligro real y presente.

2.2.3. La protección penal de los sistemas de IA

El desarrollo de la IA y de otras tecnologías afines puede plantear la necesidad de proteger nuevos intereses o valores jurídicos. Los datos de los que se nutren los algoritmos, los propios sistemas de IA, determinadas condiciones de su aplicación o, incluso, intereses asociados a los robots, pueden constituir en un futuro próximo intereses jurídicos individuales o colectivos dignos de protección por el Derecho penal. Más allá de la protección de la propia IA como posible bien jurídico diferenciado, aún estamos lejos de poder adivinar cuáles serán esos intereses y cómo debe configurarse su protección. Sí que se puede anticipar algo: que la concepción que tenemos de la privacidad como interés digno de protección puede ser que se acabe modificando. No se trataría, por tanto, de la aparición de un nuevo bien jurídico sino de la modificación del alcance y significación de uno ya existente. El uso de los datos para la IA puede suponer un cambio de paradigma en la comprensión de este interés, e incluso una revisión del significado tradicional del derecho a la intimidad como un derecho puramente individual o personal. El valor colectivo de los datos más allá del significado que tienen para el propio individuo y las implicaciones que su control y uso por parte de instituciones o individuos puede tener para el conjunto de la sociedad, hace que algunos autores comiencen a preguntarse si la IA no debería conducirnos a una nueva comprensión social del derecho a la intimidad[56] .

---

[56] Véliz, C. (2020). *Privacy is power*, Corgi Books.

En cuanto a la necesidad de proteger la IA, es evidente que los propios sistemas de IA pueden ser objeto de actividades delictivas, perturbándolos o dañándolos, y que si estos son usados para llevar a cabo determinadas actividades, como parte de una infraestructura crítica, su mal funcionamiento podría causar daños considerables. De ahí, sin embargo, no se puede derivar que sea necesario reformar los sistemas penales para proteger autónomamente la IA como un nuevo interés jurídico digno de protección penal, puesto que sería la tutela de la función de que se tratase la que daría lugar a la respuesta penal en el caso de que lo mereciera. Además, y teniendo en cuenta que la mayoría de esos sistemas podrán entrar dentro del entendimiento amplio que hace el Convenio de Budapest de "sistema informático" como cualquier dispositivo o grupo de dispositivos interconectados o relacionados, uno o más de los cuales, de conformidad con un programa, realiza el procesamiento automático de datos[57], lo normal es entender que cualquier daño a estos sistemas pueda ser sancionado por medio de los distintos tipos penales que castigan en los diferentes códigos penales el daño informático. Y en cuanto a la copia de estos sistemas lo que se verá afectado será el interés económico patrimonial de los creadores que podrá ser tutelado bien por los delitos relacionados con la tutela de los derechos, bien por los que protegen los derechos de propiedad industrial cuando pueda ser patentado o, muy probablemente, por medio de los delitos contra la libre competencia.

Sí es posible que en un futuro cercano se requiera de una protección específica en el caso de los robots, que tenga en cuenta los distintos bienes y valores vinculados a estas tecnologías de IA, especialmente en caso de que alcancen un cierto grado de autonomía. Aunque es evidente que el nivel actual de desarrollo de la robótica en la que se usa IA permite una protección suficiente con los delitos que protegen los intereses económicos relacionados con estas máquinas como con cualesquiera otras, no es descartable que cuando su autonomía les de singularidad frente a otras máquinas puedan requerir de una tutela especial. Tampoco lo es, como ya ha sido señalado acertadamente por algún autor, que

---

[57] Del mismo modo, la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información entiende por sistema informático "un dispositivo o grupo de dispositivos interconectados o relacionados entre sí, uno o más de los cuales, en virtud de un programa, realiza un tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho dispositivo o grupo de dispositivos a efectos de su funcionamiento, utilización, protección y mantenimiento".

incluso antes de que se puedan considerar agentes morales autónomos decida prohibirse determinados actos (en mi opinión, ofensivos) ejecutados en público y realizados sobre los mismos[58].

BIBLIOGRAFÍA

AIDP. *Recomendación 4 de la Resolution on Traditional Criminal Law categories and AI*, ob. cit., p. 55.

AIDP. *Resolution on Traditional Criminal Law categories and AI*, 54 y ss.

AIDP. *Resolution on Traditional Criminal Law categories and AI*, 55 y ss.

Asaro, P. M. (2016). "The Liability Problem for Autonomous Artificial Agents." In *AAAI Symposium on Ethical and Moral Considerations in Non-Human Agents*, edited by B. Indurkhya y G. Stojanov, 190-194, Stanford: Association for the Advancement of Artificial Intelligence. https://www.aaai.org/ocs/index.php/SSS/SSS16/paper/view/12699.

Beck, S. (2016). "Intelligent agents and criminal law - Negligence, diffusion of liability and electronic personhood", *Robotics and Autonomous Systems* 86:138-143.

Danaher, J. (2019). *Automation and Utopia: Human Flourishing in a World without Work*, Cambridge, MA: Harvard University Press.

Danaher, J. (2016). "Robots, law and the retribution gap", *Ethics and Information Technology 18*, núm. 4, 299-309.

---

[58] Así lo señala Mamak, K. (2022). Should violence against robots be banned? *International Journal of Social Robotics*, *14*(4), 1057-1066, con respecto a la violencia pública señalando que la ilicitud de tales actos no derivaría de la voluntad de la protección de algunas características intrínsecas de los robots, sino de la general tendencia a la prohibición de actos en lugares públicos como decir palabrotas, ir desnudo y beber alcohol. En mi opinión se trataría de un evidente ejemplo de criminalización de ofensas que, sin embargo, no creo que se pueda desvincular completamente, tal y como hace el autor, de la consideración moral que poco a poco vayamos teniendo de los robots, aunque sí de la autonomía moral real que ellos tengan. De hecho, es interesante en este sentido el análisis de Darling, K. (2016). "Extending legal protection...", ob. cit; quien incluso relaciona la potencial protección de los robots frente a abusos de diverso tipo con la evolución en la protección de los animales y la criminalización de conductas abusivas contra los mismos. Dice Darling que, si bien ahora mismo aún podríamos estar lejos, conforme "la tecnología ensanche la brecha entre los robots sociales y las tostadoras" y la gente desarrolle cada vez más un fuerte apego a algunas tipologías de robots, nos iremos acercando a un escenario en el que, independientemente de su autonomía moral, se llegue a un consenso social respecto a la necesidad de esta tutela.

Darling, K. (2016). "Extending legal protection to social robots: The effects of anthropomorphism, empathy and violent behavior towards robotic objects", en *Robot law*, Edward Elgar Publishing, 213-232, Cheltenham: Edward Elgar Publishing.

De la Cuesta Aguado, P. (2016). "La ambigüedad no es programable: racionalización normativa y control interno en inteligencia artificial", *Revista de Derecho y Proceso Penal 44*, 165-194.

Del Rosal Blasco, B. (2023). "¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial?", *REDEPEC: Revista Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance* 2.2.

European Parliament (2024). "Amendment 18 of the parliament to the recital 6 of the commission".

Flor, R. y A. Gullo (2024). "Italian Report on Penal law and criminalization of AI offences." In RIDP, Vol. 94 issue 3, *Penal law and criminalization of AI offences*, F. Miró-Llinares, M. Santisteban-Galarza, C. Duvac y T. Tudorel, International Colloquium Section II, Bucharest, 13-16 June.

Hallevy, G. (2010). "The criminal liability of artificial intelligence entities – from science fiction to legal social control", *Akron Intellectual Property Journal 4*, 171-201.

Hallevy, G. (2013). *When Robots kill, Artificial Intelligence under Criminal Law*, New England: Northeastern University Press.

Harbers, M., M. M. Peeters y M. A. Neerincx (2017). "Perceived autonomy of robots: Effects of appearance and context", *A World with Robots*, M. I. Aldinhas Ferreira, J. Silva Sequeira, M. O. Tokhi, E. Kadar y G. S. Virk, 19-33, Cham: Springer.

Hindriks, F. y H. Veluwenkamp (2023). "The risks of autonomous machines: from responsibility gaps to control gaps", *Synthese 201*, 21. https://doi.org/10.1007/s11229-022-04001-5.

Holland, O. (2004). "The future of embodied artificial intelligence: Machine consciousness?", *Embodied artificial intelligence*, F. Lida, R. Pfeifer, L. Steels y Y. Kuniyoshi, 37-53. Berlin: Springer.

Karchevskyi, M. y Radutniy, A. (2024). "Ukranian Report on Penal law and criminalization of AI offences", *RIDP*, Vol. 94 issue 3, *Penal law and criminalization of AI offences*, F. Miró-Llinares, M. Santisteban-Galarza, C. Duvac y T. Tudorel, International Colloquium Section II, Bucharest, 13-16 June.

Königs, P. (2022). "Artificial intelligence and responsibility gaps: what is the problem?", *Ethics Inf Technol 24*, 36. https://doi.org/10.1007/s10676-022-09643-0.

Lida, F., Pfeifer, R., Steels, L. y Kuniyoshi, Y. (eds.) (2004). *Embodied artificial intelligence*. Berlin, Springer.

Mamak, K. (2022). "Should criminal law protect love relation with robots?", *AI & SOCIETY*, 1-10.

Mamak, K. (2022). "Should violence against robots be banned?", *International Journal of Social Robotics 14*, núm. 4, 057-1066.

Martínez Garay, L. (2018). "Peligrosidad, algoritmos y due process: el caso State vs. Loomis", *Revista de Derecho Penal y Criminología 20*, 485-502.

Micromachismos (2018). "Rosalía y las fotos manipuladas que la mostraban desnuda: su cuerpo no es mercancía ni estrategia de marketing", *eldiario.es*. Accessed December 29. https://www.eldiario.es/blog/micromachismos/rosalia-fotos-manipuladas-mostraban-desnuda-cuerpo-mujer-no-mercancia-estrategia-marketing_132_10235525.html

Miró Llinares, F. "AI and criminal law reform: notes on the inadequacy of a criminalization model based on a substantive principle", en prensa.

Miró Llinares, F. (2024). "General Report on Penal law and criminalization of AI offences", *RIDP*, Vol. 94 issue 3, *Penal law and criminalization of AI offences*, F. Miró-Llinares, M. Santisteban-Galarza, C. Duvac y T. Tudorel, International Colloquium Section II, Bucharest, 13-16 June.

Miró Llinares, F. (2022). "Inteligencia artificial, delito y control penal: nuevas reflexiones y algunas predicciones sobre su impacto en el derecho y la justicia penal", *El Cronista del Estado Social y Democrático de Derecho 100*, 174-183.

Miró-Llinares, F. y Aguerri, J. C. (2023). "Misinformation about fake news: A systematic critical review of empirical studies on the phenomenon and its status as a 'threat'", *European Journal of Criminology 20*, núm. 1, 356-374.

Navarro Dometsch, R. "Brechas de responsabilidad penal y entes inteligentes artificiales", Manuscript presented at the Congreso Internacional "Sistema penal, inteligencia artificial y su regulación", Universidad Católica de Maule, Talca, Chile, November 29-30.

Organisation for Economic Co-operation and Development (2019). *Recomendación del Consejo sobre Inteligencia Artificial*, adoptada el 22 de mayo.

Osmani, N. (2020). "The complexity of criminal liability of AI systems." *Masaryk University Journal of Law and Technology 14*, núm. 1, 53-82.

Parlamento Europeo (2024). *Exposición de motivos del Reglamento de Inteligencia Artificial*. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión, COM(2021)0206 - C9-0146/2021 - 2021/0106(COD).

Picotti, L. (2023). "General Report on Traditional Criminal Law Categories and AI", *RIDP*, Vol. 94 issue i, *Traditional Criminal Law Categories and AI: Crisis or Palingenesis?*, L. Picotti y B. Panattoni, International Colloquium Section I, Siracusa, 15-16 September.

Provaznick, J. (2023). "Czech Report on Penal law and criminalization of AI offences", RIDP, Vol. 94 issue 3, *Penal law and criminalization of AI offences*, F. Miró-Llinares, M. Santisteban-Galarza, C. Duvac y T. Tudorel, International Colloquium Section II, Bucharest, 13-16 June.

Quintero Olivares, G. (2017). "La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas", *Revista Electrónica de Estudios Penales y de la Seguridad: REEPS* 1, 1.

Russell, S. J. y Norvig, P. *Artificial intelligence*, ob. cit.

Santisteban Galarza, M. (2024). "La criminalización de las ultrafalsificaciones (con especial atención a las implicaciones de la normativa europea de servicios digitales e inteligencia artificial)", *Revista de Derecho Penal y Criminología*, 3ª época, núm. 31, enero, 211-249.

Simó Soler, E. (2023). "Retos jurídicos derivados de la inteligencia artificial generativa", *InDret*.

Sparrow, R. (2007). "Killer robots", *Journal of Applied Philosophy 24*, núm. 1, 62-77.

Surden, H. (2019). "Artificial Intelligence and Law: An Overview", *Georgia State University Law Review 35*.

Véliz, C. (2020). *Privacy is power*. London, Corgi Books.

Wang, X. y Bai, L. (2023). "Chinese Report on Penal law and criminalization of AI offences", *RIDP*, Vol. 94 issue 3, *Penal law and criminalization of AI offences*, F. Miró-Llinares, M. Santisteban-Galarza, C. Duvac y T. Tudorel, International Colloquium Section II, Bucharest, 13-16 June.

Zanol, J., Buchelt, A., Tjoa, S. y Kieseberg, P. (2022). "What is "AI"? Exploring the scope of the "artificial intelligence act". https://jusletter-it.weblaw.ch/dam/publicationsystem_leges/iris2022/zanoal_et_al_what_is_ai.pdf

Capítulo 5
LA GENERACIÓN DE CONTENIDOS A TRAVÉS DE INTELIGENCIA ARTIFICIAL Y SU INCIDENCIA EN LA PROPIEDAD INTELECTUAL

Sebastián López Maza
Profesor Titular de Derecho Civil
Universidad Autónoma de Madrid
https://orcid.org/0000-0003-3641-3416

1. INTRODUCCIÓN

La inteligencia artificial (en adelante, IA) ha venido para quedarse. No se trata de una moda pasajera, al estilo de la comercialización de obras mediante NFTs, sino de un avance tecnológico sin precedentes que tenderá a evolucionar hasta límites insospechados. Es más, podría ocurrir que, en un par de años, todo lo que se indica en este capítulo quede totalmente desfasado por el desarrollo de estos sistemas. A través de la inteligencia artificial se trata de imitar la inteligencia humana –se llega a hablar hasta de "redes neuronales"–, entrenando a los sistemas, mediante el denominado proceso de *machine learning*, para que produzcan un determinado resultado. Se podría decir que lo realizado a través de esta tecnología es prácticamente idéntico a lo que podría hacer una persona física. De hecho, se ha definido la IA como aquel sistema que trata de imitar los procesos de aprendizaje y razonamiento de los seres humanos[1]. Su desarrollo y su capacidad está creciendo a pasos agigantados con el transcurso del tiempo. Esta tecnología se ha aplicado en muy diversos campos: la medicina, el Derecho, el cine, la música o el arte, entre otros muchos. Hoy en día, la IA es capaz de

[1] Tessier, C. (2017). "Robots Autonomy: Some Technical Challenges", *Autonomy and artificial intelligence: A Threat or Savior?* W.F. Lawless, R. Mittu, D. Sofge y S. Russell (eds.), Springer, Reino Unido, p. 179.

pintar un cuadro, escribir una novela, componer una canción, diseñar un edificio o crear escenas para una película.

En lo que a la propiedad intelectual respecta, la aplicación de IA en la producción de obras y prestaciones ha generado no pocos debates y discusiones. Y es que las nuevas tecnologías van marcando el camino por el que discurre la propiedad intelectual, en la medida en que permiten nuevas formas de crear contenidos. En el ámbito concreto de los derechos de autor, son muchas las cuestiones que se plantean: ¿qué se protege en todo el proceso de generación de productos a través de IA?, ¿cómo deberían tutelarse los resultados?, ¿a quién debería atribuirse derechos sobre tales resultados?, ¿pueden considerarse originales?, ¿es posible entrenar los sistemas de IA mediante obras y prestaciones preexistentes sin necesidad de autorización de los titulares de derechos sobre esos contenidos utilizados? Algunas de estas preguntas tienen ya respuesta en la legislación vigente. Sin embargo, otras aún no han sido reguladas en Europa ni en España, por lo que todo queda al juicio crítico de la doctrina y al tratamiento que la jurisprudencia empieza a darle a esta problemática. No obstante, las instancias europeas son conscientes del juego que la IA puede dar en el ámbito de la propiedad intelectual. De hecho, en la Comunicación de la Comisión de 25 de abril de 2018, sobre IA para Europa[2], y en la Resolución del Parlamento Europeo de 20 de octubre de 2020, sobre derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la IA[3], se pone de manifiesto la necesidad de reflexionar sobre la interacción entre la IA y los derechos de propiedad intelectual, con el fin de conseguir el equilibrio adecuado entre la innovación y la seguridad jurídica. Europa ve necesario promover y proteger la creación y la innovación, así como los intereses de los creadores.

El último hito en este camino se ha producido con ocasión de la aprobación del Reglamento (UE) 2024/689, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, Reglamento IA)[4]. Su objetivo es la adopción de una IA fiable y centrada en el ser humano y, al

---

[2] COM(2018) 237 final, disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237 (u. v. 05/08/2024).

[3] (2020/2015 (INI)), disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020IP0277 (u. v. 05/08/2024).

[4] Disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689 (u. v. 05/08/2024).

mismo tiempo, impulsar la innovación (art. 1.1). Se declara que, entre los derechos que pueden verse lesionados por la IA, se encuentran los de propiedad intelectual (cdos. 48, 88 y 167). La necesidad de protegerlos se apunta en numerosos artículos a lo largo del Reglamento [arts. 25.5, 52.6, 53.1.b), 78.1.a)]. De ahí que, en enero de 2024, la Comisión Europea aprobara la creación de la Oficina Europea de IA, que empezó a funcionar en febrero en Bruselas. Este organismo se encarga de controlar el cumplimiento del Reglamento IA.

En España, en diciembre de 2023, se creó la Agencia Española de Supervisión de la Inteligencia Artificial, ubicada en La Coruña, para proteger los derechos fundamentales de los españoles que puedan verse vulnerados por el uso de sistemas de IA. En febrero de 2024, el Ministerio de Cultura publicó una nota informativa que incluye una Guía de Buenas Prácticas de Uso de la IA, en la que se señala que los sistemas de IA deben cumplir con la normativa sobre propiedad intelectual[5]. Otros países de nuestro entorno también han empezado a elaborar informes con orientaciones y recomendaciones sobre el uso de esta tecnología[6].

2. CUESTIONES NO CONTROVERTIDAS EN EL USO DE IA

El artículo 3.1 Reglamento IA define un "sistema de IA" como todo sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación y que infiere de la información de entrada que recibe la manera de generar contenidos. La protección de estos por parte del derecho de autor resulta controvertida. No obstante, hay varias cuestiones relacionadas con la IA sobre las que no cabe discusión, pues resulta plenamente aplicable la normativa vigente sobre propiedad intelectual.

En primer lugar, se puede decir que el sistema de IA como tal estará protegido por derechos de autor, como programa de ordenador que es, siempre que conforme una obra que reúna los requisitos necesarios para recibir esa protección, recogidos en el artículo 10 LPI: a) creación humana; b) original; y c) exteriorizada. Siendo así, estaría amparado en el régimen especial de los

---

[5] Disponible en: https://www.cultura.gob.es/dam/jcr:469163cc-0fdf-4fe2-964f-d4815cde40b1/240219-nota-informativa-ia.pdf (u. v. 05/08/2024).

[6] En Francia, la Comisión de Inteligencia Artificial publicó, en marzo de 2024, el informe *IA: Notre ambition pour la France*, disponible en Internet: https://www.gouvernement.fr/upload/media/content/0001/09/4d3cc456dd2f5b9d79ee75feea63b47f10d75158.pdf. (u. v. 05/08/2024).

artículos 95 y ss. LPI[7]. En este caso, se atribuirán los derechos a la persona física o al grupo de personas físicas que han creado el programa, o a la persona jurídica que haya editado y publicado bajo su nombre tal obra, conforme al régimen de la obra colectiva (art. 97.1 LPI). Además, cabe señalar que se protegerá, según el artículo 96.1 LPI, la secuencia de instrucciones o indicaciones cuyo fin, directo o indirecto, sea realizar una función o una tarea o para obtener un resultado determinado, con independencia de cuál sea su forma de expresión y fijación, abarcando también la documentación preparatoria y los manuales de uso. Los programas de ordenador, además, están protegidos a nivel internacional [arts. 4 Tratado OMPI Derecho de Autor (en adelante, TODA) y 10 Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (en adelante, ADPIC)] y a nivel europeo (Directiva 2009/24, sobre programas de ordenador). Tales programas son equiparados a las obras literarias.

Téngase en cuenta que el derecho de autor no protege las ideas, los procedimientos o los métodos, sino la concreta forma de expresión. Así se expresan los artículos 2 TODA, 9.2 ADPIC, 1.2 Directiva 2009/24 y 96.4 LPI. En consecuencia, no quedaría amparado por esta protección el algoritmo, es decir, el principio en el que se basa el software de IA para cumplir determinadas funciones –la secuencia de pasos o instrucciones que permiten obtener un resultado–[8].

---

[7] Minero Alejandre, M. (2023). "Inteligencia artificial y propiedad intelectual", *Derecho, nuevas tecnologías e inteligencia artificial*, C. Alonso Salgado, A. Valiño Ces y A. Rodríguez Álvarez (dir.), Dykinson, Madrid, p. 87.

[8] Saiz García, C. (2019). "Las obras creadas por sistemas de inteligencia artificial y su protección", *InDret*, núm. 1, pp. 9-10. También niega la protección el Consejo Superior de la Propiedad Literaria y Artística, del Ministerio de Cultura francés, en su informe de 27 de enero de 2020, sobre inteligencia artificial y cultura (p. 28), disponible en Internet: https://www.culture.gouv.fr/es/Conocernos/Organisation-du-ministere/Consejo-Superior-de-Propiedad-Literaria-y-Artistica-CSPLA/Trabajos-y-publicaciones-del-CSPLA/Misiones-del-CSPLA/Mission-du-CSPLA-sur-les-enjeux-juridiques-et-economiques-de-l-intelligence-artificielle-dans-les-secteurs-de-la-creation-culturelle (u. v. 05/08/2024). Igualmente lo plantea el Max Planck Institute for Innovation and Competition (Múnich), en su Informe, de 9 de abril de 2021, relativo a la relación entre la IA y la propiedad intelectual (pp. 17-18). Disponible en Internet: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Position-Paper__SSRN_21-10.pdf (u. v. 05/08/2024). Según el Max Planck, los algoritmos no necesitan la protección de la propiedad intelectual porque ya están debidamente protegidos por otras figuras jurídicas, como la competencia desleal o el Derecho de los contratos. En contra, Aparicio Vaquero, J. P. (2022). "Derecho de autor y más allá: algoritmos, código de los programas de ordenador y apps", *Revista Pe.i.*, núm. 71, pp. 25 y ss. Considera este autor que el algoritmo es posible protegerlo como si de un programa de ordenador se tratara.

De hecho, el considerando 11 Directiva 2009/24 los excluye expresamente. El TJUE ha negado la protección del derecho de autor a las funcionalidades de los programas de ordenador expresadas a través de algoritmos, pues lo contrario podría llevar a la monopolización de las ideas, obstaculizando la innovación. Entiende que cualquier forma de expresión de un programa de ordenador debe estar protegida desde el momento en que su reproducción dé lugar a la reproducción del programa de ordenador en sí, permitiendo de este modo que el ordenador cumpla su función. Cabe destacar, en este sentido, las SSTJUE de 22 de diciembre de 2010[9] y de 2 de mayo de 2012[10].

En segundo lugar, la base de datos de la que se nutra el sistema de IA para poder producir resultados también estará protegida, tanto por el derecho de autor como por el derecho *sui generis*, siempre que se cumplan los requisitos específicos[11]. Para el caso de la protección como obra, será necesario que tenga originalidad, en el sentido de que, por la selección o disposición de sus contenidos, constituyan creaciones intelectuales (arts. 3.1 Directiva 96/9 y 12 LPI), y que no esté formada, por ejemplo, por toda la obra de un determinado autor. Para la protección por el derecho *sui generis*, el fabricante de la base de datos debe haber hecho una inversión sustancial (arts. 7.1 Directiva 96/7 y 133.1 LPI). Además, el propio sistema de IA puede crear bases de datos o colecciones, en el sentido de los preceptos señalados (ej.: las listas de reproducción de una determinada plataforma de *streaming*). Cuando es el sistema el que genera tales listas de reproducción, basándose, por ejemplo, en las canciones que el usuario viene escuchando, estaremos ante un proceso meramente técnico o mecánico, carente de creatividad. Ahora bien, si la lista de reproducción la elabora el usuario y dicha selección responde a parámetros originales, podríamos atribuirle originalidad conforme a los artículos 3.1 Directiva 96/9 y 12 LPI[12].

Y, en tercer lugar, tampoco hay discusión en otorgar derechos de autor a la persona que crea una obra utilizando como herramienta un sistema de IA.

---

[9] Caso *Bezpečnostní softwarová asociace*, asunto C-393-09, párs. 38 y 42-44, ECLI:EU:C:2010:816.

[10] Caso *SAS Institute Inc.*, asunto C-406/10, párs. 32 y 40, ECLI:EU:C:2012:259.

[11] Así también lo considera el Consejo Superior de la Propiedad Literaria y Artística, del Ministerio de Cultura francés, en su informe sobre inteligencia artificial y cultura (p. 30) y el Max Planck, en su informe sobre IA (pp. 6-7), ambos documentos reseñados en la nota 7.

[12] Saiz García, C. "Las obras creadas...", *op. cit.*, pp. 22-23.

Se trata de IA asistida. Así lo entiende el Parlamento Europeo en su Resolución de 20 de octubre de 2020 (punto 14)[13]. En estos casos, la persona física se ayuda de la IA para crear la obra. De la misma manera que el fotógrafo que realiza una fotografía sirviéndose de la máquina y desarrollando un proceso creativo será considerado autor de una obra fotográfica, quien utiliza un sistema de IA para crear una obra, controlando ese proceso, será considerado autor del resultado generado. Se aplican aquí las reglas generales sobre atribución de autoría. Ahora bien, es necesario que el usuario haya tomado decisiones libres y creativas para generar ese resultado a través de IA. La mayoría de las obras realizadas a través de IA son obras asistidas. Se trata de sistemas que deben ser entrenados y programados adecuadamente, y manipulados por personas físicas para poder producir los correspondientes resultados. Así ocurrió, por ejemplo, en los casos de *Next Rembrandt,* en el cual un sistema de IA logró pintar un cuadro totalmente nuevo imitando la técnica del pintor holandés*, Flow Machines,* creadora de la canción *Daddy's Car, o WASP,* compositor de poemas. Normalmente, estos resultados responden al esquema de las obras colectivas (art. 8 LPI): constituyen proyectos donde participa un gran número de personas, pero existe alguien que tiene la idea, coordina las aportaciones de los participantes, realiza la inversión económica necesaria para su desarrollo y edita el resultado final bajo su nombre[14]. En todo caso, la intervención de la persona física debe ser significativa, pues habría que negarle protección a aquel autor que pretende atribuirse un derecho de autor sobre un resultado obtenido con IA en el que su participación es testimonial. Así ocurrió, por ejemplo, en el caso *Death of an author*, una novela de Aidan Marchine, donde el 95% fue generado por IA y el 5% restante elaborado por el autor que se escondía tras ese seudónimo.

---

[13] Igualmente se pronuncia el Max Planck Institute en su informe sobre IA (pp. 21-22), referido en la nota 7.

[14] Así lo entienden también Ginsburg, J. C. y Budiardjo, A. L. (2019). "Authors and Machines", *Berkeley Technology Law Journal*, Vol. 34, núm. 2, p. 6; Saiz García, C., "Las obras creadas...", *op. cit.*, p. 22; Morán, M., "Creadores en riesgo de extinción", *V Certamen de artículos jurídicos sobre Derecho del Entretenimiento*, Premios DENAE, 2018, p. 4; Duque Lizarralde, M. (2020). "Las obras creadas por inteligencia artificial, un nuevo reto para la propiedad intelectual", en *Revista Pe.i.*, núm. 64, enero-abril, p. 23.

3. CUESTIONES CONTROVERTIDAS EN EL USO DE IA GENERATIVA

La IA generativa es aquel sistema que es capaz de producir contenidos de manera autónoma, sin ningún tipo de ayuda[15]. Con el desarrollo tecnológico, los procesos de aprendizaje de los sistemas de IA tienden al *deep learning*, esto es, a que las máquinas aprendan de sí mismas, tal y como hace un ser humano, sin necesidad de que nadie esté detrás introduciendo contenidos o programándola continuamente. Se utilizan, para ello, técnicas cognitivas a la hora de elaborar el programa que permite al sistema de IA funcionar, emulando las redes neuronales de las personas. Existen varios casos que han sido tratados como IA generativa. Entre ellos, los proyectos *Edmond de Belamy*, *DeepDream* o *Magenta*, a través de los cuales se crearon pinturas a partir del entrenamiento del sistema. En el sector literario, cabe destacar el caso de la novela corta *El día en que un ordenador escriba una novela*, o del libro de recetas de cocina *Cognitive Cooking with Chef Watson*. En el ámbito musical, el sistema *Deep Artificial Composer* o el caso de *La Sinfonía Inacabada*.

Los sistemas de IA generativa suscitan importantes e interesantes debates en el sector de la propiedad intelectual: 1) la titularidad de derechos sobre los resultados derivados de su aplicación; 2) la atribución de originalidad a dichos resultados; y 3) su entrenamiento a través de obras y prestaciones protegidas por la propiedad intelectual. Se podría decir que, en este ámbito, las controversias se plantean en dos momentos concretos: a) la fase de entrenamiento y aprendizaje del sistema de IA; b) la generación del resultado.

---

[15] En su Informe de 27 de enero de 2017, el Parlamento Europeo destacó las características que debían tener los robots autónomos inteligentes: 1) la interconectividad, esto es, la capacidad para adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno y el análisis de tales datos; 2) el autoaprendizaje o la capacidad de aprendizaje a través de la experiencia y la interacción; 3) la capacidad de adaptación de su comportamiento y acciones al entorno. *Vid*. Informe del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, 2015/2103(INL), p. 7, disponible en Internet: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html (u. v. 05/08/2024).

3.1. La titularidad de derechos sobre los resultados producidos por IA generativa

En los supuestos de IA generativa, la atribución de derechos es más complicada que en los casos de IA asistida, puesto que el acto "creativo" no lo realiza una persona física, sino una máquina. Conforme más avanza esta tecnología hacia la generación más absoluta y autónoma de contenidos, en el sentido de tener más libertad en la toma de decisiones, más problemática resulta la atribución de derechos. Podríamos manejar distintas posibilidades, concediendo los derechos a: 1) la máquina; 2) una persona física o jurídica que intervenga en el proceso de obtención del resultado; 3) los titulares de derechos sobre los contenidos que permiten generar los resultados por IA; y 4) nadie[16].

La primera posibilidad es atribuir derechos a la máquina, al sistema de IA. Cuando es generativo, lleva a cabo tareas similares a las que realiza una persona física al crear una obra, como el procesamiento de la información o la producción de un resultado. Sin embargo, hay otras tantas tareas que las máquinas son incapaces de hacer, por muy autónomas que sean, y que, por ahora, son exclusivas de los seres humanos, como la realización de un esfuerzo creativo o el empleo de la imaginación. No es posible atribuir un derecho de autor a la máquina por varios motivos. En primer lugar, porque una máquina carece de personalidad jurídica, lo que le impide ser titular de derechos[17]. El CC únicamente atribuye capacidad jurídica a las personas físicas (art. 30) y a las personas jurídicas (art. 35). Un sistema de IA no es una cosa ni la otra, por lo que la atribución de derechos a una máquina requeriría primeramente modificar el CC[18].

---

[16] Plantean también estas opciones Ginsburg, J. C. y Budiardjo, A. L. (2001). "Authors and Machines...", *op. cit.*; Glesser, D., "Copyright in Computer-Generated Works: Whom, If Anyone, Do We Reward?", *Duke Law and Technological Review*, Vol. 1.

[17] Así lo destacan Minero Alejandre, M., "Inteligencia artificial...", *op. cit.*, p. 90; Aparicio Vaquero, J. P., "Derecho de autor...", *op. cit.*, pp. 49-50.

[18] Apuestan por atribuir personalidad jurídica a las máquinas y otorgarles la condición de autor, creando una ficción similar a la que en su momento se estableció para las personas jurídicas, Yanisky-Ravidm, S. y Velez Herández, L. (2018). "Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model", en *Minnesota Journal of Law, Science and Technology*, Vol. 19, p. 51; Ortego Ruiz, M. (2018), "El concepto de autor en la era de los robots", en *Anuario de Propiedad Intelectual 2017*, Reus, Madrid, pp. 431-432. Se basan, para ello, en las propuestas de las instituciones europeas de atribuir a la IA una personalidad jurídica propia. Así se incluyó en la Resolución del Parlamento Europeo, de 27 de enero de 2017, sobre recomendaciones a la Comisión sobre normas de Derecho civil sobre robótica

En segundo lugar, y esto es fundamental, por el carácter eminentemente personalista del derecho de autor. Con carácter originario, se atribuyen los derechos de autor a aquella persona que haya creado una obra. Por tanto, es necesario un acto de creación para tener la condición de autor y, en consecuencia, ser titular de todos los derechos reconocidos en la LPI. La facultad de creación la tienen, por ahora, las personas físicas. Sólo ellas pueden llevar a cabo el esfuerzo creativo, tener conciencia de la creación, controlar ese proceso. Las obras protegidas únicamente pueden ser fruto de la inteligencia humana. En la LPI hay varias evidencias que llevan a esta conclusión. Una de ellas es el propio artículo 5 LPI, que habla de "persona natural". Tan sólo en el régimen de la obra colectiva encontramos una excepción a esta regla: la posibilidad de que una persona jurídica reciba la protección que la LPI concede a los autores personas físicas (arts. 5.2 y 8 LPI). En aquellas obras elaboradas por varios participantes en las que exista una persona que toma la iniciativa, coordina a la gente, y edita y divulga la obra bajo su nombre, es posible que se atribuyan derechos de autor a una persona jurídica cuando ha desarrollado todas estas tareas. Ahora bien, lo que la LPI configura aquí es una atribución originaria de derechos, pero dicha persona jurídica no es autora en sentido estricto, pues no ha realizado, como tal, un acto de creación –se atribuyen derechos de autor a entes que no han creado nada, pero han contribuido económicamente en la producción de la obra–. En sede de los programas de ordenador, el artículo 97.1 LPI considera autora a la persona física que lo haya creado o a la persona jurídica que sea contemplada como titular de los derechos de autor. No es que la persona jurídica sea autora, sino que será considerada autora, será tratada como tal, en la faceta que tiene que ver con la titularidad de los derechos. En cualquier caso, estamos ante una ficción que crea el legislador. Una segunda evidencia del carácter personalista de la LPI es el hecho de otorgar derechos morales, que, por contraposición a los derechos patrimoniales, tienen que ver con la parte más personal del individuo, lo que lleva también a entender únicamente a la persona como autora[19]. Por tanto, el ordenamiento español no protege los resultados que no constituyan un producto del intelecto humano.

(2015/2103(INL)) y la Comunicación de la Comisión, de 25 de abril de 2018, sobre inteligencia artificial para Europa [COM(2018) 237 final].

[19] Sanjuán Rodríguez, N. (2019). "Inteligencia artificial y propiedad intelectual", *Actualidad Jurídica Uría Menéndez*, núm. 52, p. 87.

En el plano internacional, la Declaración Universal de Derechos Humanos protege los intereses morales y materiales de toda persona sobre sus producciones científicas, literarias o artísticas de que sea obra (art. 27.2). El Convenio de Berna (en adelante, CB), no contiene un concepto de "autor" ni requiere expresamente la condición de persona física. Sin embargo, es difícil asumir que, en 1886, se estuviera pensando en obras creadas por IA, siquiera por ordenadores, por lo que resultaba innecesario preverlo[20]. No obstante, a lo largo del CB sí existen normas que nos pueden llevar a la conclusión de que el autor debe ser una persona física. Entre ellos, el artículo 3 CB, al utilizar la nacionalidad del autor o su lugar de residencia como criterios para conceder la protección. También el artículo 7.1 CB, al establecer el momento de la muerte del autor como parámetro para calcular el plazo de protección. En el ámbito de la UE, el artículo 2 Directiva 2009/24, sobre programas de ordenador, y el artículo 4.1 Directiva 96/9, sobre bases de datos, se refieren expresamente a las personas físicas como autoras de ambos tipos de obras –haciendo mención igualmente a la posibilidad de que las personas jurídicas sean consideradas como tales–. En definitiva, en el plano internacional, europeo y nacional, estamos antes sistemas eminentemente personalistas en cuanto a la atribución de derechos de autor.

La tercera razón para negar un derecho de autor al sistema de IA es la necesidad de que haya una persona detrás para realizar ciertas tareas relacionadas con la creación y con el ejercicio del eventual derecho de autor atribuido a la máquina (ej.: la persecución de las infracciones o la transmisión a terceros). Y la cuarta razón tiene que ver con los fines para los cuales se prevé el derecho de autor, que aquí no se cumplen. Uno de ellos es fomentar y estimular la creación de obras originales, algo imposible en una máquina. Otro es recompensar al autor por la realización de su esfuerzo a la hora de crear la obra, esfuerzo que una máquina no ha realizado porque la producción de resultados es prácticamente automática. Por tanto, la consideración como autor de entes distintos de una persona requeriría un cambio en la normativa sobre propiedad intelectual. El Parlamento Europeo desaconseja dotar a las tecnologías de IA de personalidad jurídica, por el impacto negativo que tendría en los incentivos para los creadores humanos, e insta a no proteger los resultados a través del derecho de autor,

---

[20] Ginsburg, J. C. (2018). "People Not Machines: Authorship and What It Means in the Berne Convention", *International Review of Intellectual Property and Competition Law*, Vol. 49, p. 133.

por no cumplirse los principios de originalidad y de personalidad del autor (*vid*. puntos 13 y 15 de su Resolución de 20 de octubre de 2020).

Hasta tal punto le resulta importante y seria al legislador europeo la labor de los creadores, y la necesidad de impedir que lo creado por una máquina sea atribuido a una persona física, que el artículo 50.2 Reglamento IA obliga a los proveedores de sistemas de IA que generen contenido de cualquier tipo (texto, audio, imagen, vídeo) a que lo etiqueten de tal manera que sea posible detectar que ha sido generado o manipulado de manera artificial. Se trata de evitar con ello que las personas puedan pensar erróneamente que los contenidos son auténticos (cdo. 134 Reglamento IA). No obstante, no surgirá esta obligación cuando el sistema de IA desempeñe una función de apoyo a la edición estándar o no alteren sustancialmente los datos de entrada. Además, la Oficina de IA fomentará y facilitará la elaboración de códigos de buenas prácticas a escala de la UE para promover la aplicación efectiva de las obligaciones relativas a la detección y el etiquetado de contenidos generados o manipulados de manera artificial (art. 50.7 Reglamento IA). El Reglamento se cuida de avisar que el cumplimiento de esta obligación de transparencia no debe interpretarse como un obstáculo a la libertad de expresión o a la libertad de las artes y de las ciencias, sobre todo cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción (cdo. 134). En estos casos, esta obligación no puede obstaculizar la presentación, el disfrute, la explotación y el uso normal de la obra.

En los ordenamientos del *Common Law*, tampoco se apuesta por otorgar derechos a la máquina. Así, la sección 178 de la *Copyright, Designs and Patents Act*, de 1988, de Reino Unido (en adelante, CDPA) permite la protección, a través del derecho de autor, de las obras generadas por un ordenador en circunstancias en la que no hay un autor persona física detrás. Ahora bien, como no es posible atribuir derechos de autor a una máquina, la sección 9(3) CDPA considera autor, en estos casos, a quien lleva a cabo los arreglos necesarios para la creación de la obra. Habrá que entender por tal a quien programa el sistema de IA y lo entrena para que produzca un resultado determinado. Aquí el plazo de protección se reduce a 50 años [secc. 12(7) CDPA] y no se reconocen derechos morales [secc. 81(2) CDPA]. Lo que esta norma no termina de aclarar es si resulta aplicable a todo tipo de resultados creados por IA o únicamente a aquellos que son suficientemente originales por haber expresado su autor elecciones libres y creativas. Desde luego, la CDPA se expresa en unos términos bastante amplios

("obras generadas por ordenador"). Obsérvese que se otorgan derechos de autor, no derechos conexos, con carácter originario a esas personas que realizan los arreglos necesarios para obtener el resultado final, a pesar de no intervenir de manera directa en la creación de este. Se rompe aquí el vínculo directo que debe haber entre el autor y la obra, además de atribuir originalidad a una creación que no tiene por qué serlo.

La *Digital Millenium Copyright Act* estadounidense (en adelante, DMCA) no recoge expresamente el requisito de la creación humana para que algo esté protegido por derechos de autor. Sin embargo, la *United States Copyright Office* (en adelante, USCO) así lo viene exigiendo para que una creación pueda ser registrada como obra protegida. Según la USCO, el *copyright* únicamente puede proteger los frutos de la labor intelectual que estén fundamentados en el poder creativo de la mente, dejando fuera las creaciones no humanas, como, por ejemplo, las realizadas por una máquina. Así lo ha señalado en la sección 306 del *Compendium of US Copyright Office Practices* –la última edición es de enero de 2021–[21]. Además, la sección 313.2 del Compendio termina de aclarar aún más este asunto, al señalar, sin ambages, que para que algo sea calificado como obra debe haber sido creado por un ser humano. En caso contrario, no podrá ser protegido por el derecho de autor. Y añade que no se registrarán obras producidas por una máquina o a través de un mero proceso mecánico que opera de manera aleatoria o automáticamente sin ningún tipo de intervención humana.

A este respecto, cabe destacar el caso *A recent entrance to paradise*. Steven Thaler, creador del sistema que permitió la elaboración de dicho resultado creativo, pretendió en 2018 registrarlo en Estados Unidos, atribuyendo la autoría a la IA, por haberlo creado de manera autónoma. Sin embargo, la USCO denegó el registro en 2019, al afirmar que no se había producido un acto creativo por parte de un ser humano, necesario para conseguir la tutela del derecho de autor. Posteriormente se fue recurriendo por el señor Thaler, hasta que en 2022 la *Copyright Review Board* confirmó la decisión de impedir su registro[22]. Se apuntó que el derecho de autor únicamente protege aquello que esté basado

---

[21] Disponible en: https://www.copyright.gov/comp3/docs/compendium.pdf (u. v. 05/08/2024).

[22] La resolución está disponible en Internet: https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf (u. v. 05/08/2024).

en las capacidades creativas de la mente humana, y no aquello que responda a un proceso meramente mecánico, en concordancia con la jurisprudencia estadounidense[23]. Posteriormente, la *Copyright Review Board* ha tenido ocasión de pronunciarse de nuevo en relación con creaciones generadas por IA, para volver a denegar su registro. Así, por ejemplo, en el caso *Zarya of the Dawn*, de 21 de febrero de 2023[24], el caso *Théatre D'opéra Spatial*, de 5 de septiembre de 2023[25], y el caso *SURYAST*, de 11 de diciembre de 2023[26].

En segundo lugar, cabe contemplar la opción de otorgar un derecho de autor a la persona física o jurídica que intervenga en el proceso de producción del resultado elaborado por el sistema de IA. A este respecto, podemos considerar: 1) el usuario del sistema; 2) el programador; 3) la persona física o jurídica que ha realizado una inversión considerable a la hora de desarrollar el sistema de IA. Al usuario cabe tenerlo en cuenta por varias razones: a) ha invertido en la compra del sistema de IA y sostiene su mantenimiento –no obstante, adviértase que la condición de usuario y de propietario del sistema de IA no tienen por qué coincidir siempre en la misma persona–; y b) implementa instrucciones concretas a la máquina para que produzca el resultado. En el caso del programador, es la persona que ha diseñado y creado el *software* necesario para que el sistema de IA funcione y genere unos determinados resultados, por lo que tendría sentido

---

[23] Entre otros, *vid*. los casos *Burrow-Giles Lithographic Co. v. Sarony* [111 U.S. 53, 56 (1884)], *Mazer v. Stein* [347 U.S. 201, 214 (1954)], *Goldstein v. California* [412 U.S. 546, 561 (1973)], *Feist Publications v. Rural Telephone Service Company, Inc.* [499 U.S. 340 (1991)], *Urantia Found v. Kristen Maaherra* [114 F.3d 955, 957-59 (9th Cir. 1997)] o *Naruto v. Slater* [17 U.S.C. 101 (2016)].

[24] Disponible en: https://www.copyright.gov/docs/zarya-of-the-dawn.pdf (u. v. 05/08/2024). En este caso, la *Copyright Review Board* se enfrentaba a una obra compleja, formada por texto e imágenes. Únicamente autorizó el registro de aquel material que había sido elaborado por una persona física.

[25] Disponible en: https://www.copyright.gov/rulings-filings/review-board/docs/Theatre-Dopera-Spatial.pdf (u. v. 05/08/2024). Aquí, la *Copyright Review Board* concluyó que en la imagen había más aportación de IA que humana, por lo que no cabía su registro. Se apunta que, para poder reconocer una autoría humana, es preciso que la persona tenga un control creativo sobre la obra.

[26] Disponible en: https://www.copyright.gov/rulings-filings/review-board/docs/SURYAST.pdf (u. v. 05/08/2024). Señaló la *Copyright Review Board* que la elección de la imagen a modificar y el filtro que se le aplicaría para cambiarla, entre los múltiples ofrecidos por la herramienta de IA, no dotan de originalidad a la obra ni la hacen merecedora de un derecho de autor. En definitiva, a su juicio, no se produjeron decisiones creativas.

que se le atribuyeran, como compensación, los derechos sobre ellos. Y, respecto del inversor, se podría apuntar la importante inversión económica que requiere el desarrollo de esta tecnología y la coordinación de grandes grupos de personas, al estilo de lo que ocurre con las obras colectivas.

Sin embargo, hay que descartar la atribución de un derecho de autor a estas personas por los siguientes motivos: a) el resultado, como se verá posteriormente, carece de originalidad, incumpliéndose así uno de los requisitos básicos para recibir la protección del derecho de autor; b) ninguna de ellas interviene de una manera directa, activa y creativa en los resultados propiamente dichos que se generan con el uso del sistema de IA –se produce una desconexión entre el acto creativo y la condición de autor, que correspondería a una persona que no ha participado en la producción del resultado–; y c) los resultados ni siquiera son obras derivadas del programa de ordenador sobre el que ostentan derechos el programador o la persona física o jurídica considerada autora conforme al artículo 97.1 LPI, pues en ellos no es posible identificar o reconocer el *software* –en algunas ocasiones, el resultado podría entenderse no obra, sino un resultado derivado de las obras preexistentes que ha minado el sistema de IA–. En el caso del programador, además, cabe añadir dos razones más para negarle la atribución de derechos: 1) con carácter general, los programadores han sido contratados por una empresa para el desarrollo del programa de ordenador, recibiendo instrucciones sobre cómo debe ser este y qué funciones debe desempeñar; y 2) a la hora de ceder sus derechos sobre el *software*, ya ha sido debida y suficientemente retribuido, por lo que no merecería una compensación adicional en forma de derechos sobre los resultados generados[27]. Por tanto, no es posible la atribución de derechos de autor respecto de los productos derivados de la IA generativa[28].

No obstante, que no resulte aplicable el derecho de autor no significa que no podamos buscar otras fórmulas de protección dentro o fuera de la propiedad

---

[27] Así lo entienden Carrasco Perera y Del Estal Sastre, que niegan tajantemente que el programador merezca tal protección suplementaria. *Vid*. Carrasco Perera, A. y Del Estal Sastre, R. (2017). "Artículo 5", en *Comentarios a la Ley de Propiedad Intelectual*, R. Bercovitz Rodríguez-Cano (coord.), Tecnos, Madrid, pp. 113-114.

[28] Glesser, D., "Copyright in Computer-Generated Works... *op. cit.*, pp. 2-3; Morán, M., "Creadores en riesgo...", *op. cit.*, p. 9; Lambert, P. (2017). "Computer Generated Works and Copyright: Selfies, Traps, Robots, AI and Machine Learning", en *European Intellectual Property Review*, núm. 31, Vol. 1, p. 11; Duque Lizarralde, M. "Las obras creadas por inteligencia artificial...", *op. cit.*, p. 47.

intelectual. Dentro de ella, podríamos manejar dos opciones: a) un derecho conexo; b) un derecho *sui generis*. En ambos casos, ya no se trata de proteger el esfuerzo creativo, como ocurre con el derecho de autor, sino la inversión económica realizada. Piénsese que el desarrollo de estos sistemas requiere de grandes inversiones de dinero, de ahí que las empresas que participan en su creación reclamen su recuperación mediante la atribución de derechos de exclusiva sobre los resultados obtenidos con el uso de IA[29]. No obstante, sea cual sea la opción a considerar, en ninguna de ellas sería posible atribuir derecho alguno a la máquina, pues toda titularidad de derechos comporta tener la condición de persona, como ya se ha indicado.

En el caso del derecho conexo, se abriría la posibilidad de tratar de aplicar alguno de los ya existentes o de crear uno nuevo. Por lo que respecta a la primera opción, se ha planteado la posible aplicación de aquel que se concede a los editores de obras inéditas que están en el dominio público, contemplado en el artículo 4 Directiva 2006/116/CE y en nuestro artículo 129.2 LPI, siempre que se dieran los requisitos establecidos en ellos[30]. Sin embargo, la exigencia en nuestro ordenamiento de que la edición pueda ser individualizada por su composición tipográfica, presentación y demás características editoriales supone una intervención humana que no se da en el caso de las producciones realizadas íntegramente por IA[31]. Además, este derecho conexo parece estar pensando en obras literarias, cuando la IA puede producir todo tipo de contenidos (literarios, musicales o audiovisuales). El resto de derechos conexos no parece que casen demasiado bien con estos supuestos, tanto por la condición de sus titulares como por el objeto sobre el que recaen.

La segunda opción sería crear un derecho conexo específico para las empresas inversoras en este tipo de tecnología, aprovechando la tendencia del legislador europeo en este sentido. Se trataría de un derecho más cercano al concedido a las

---

[29] El Parlamento Europeo, en su Resolución de 20 de octubre de 2020, apuesta por proteger estos resultados a través de un derecho conexo que garantice las inversiones en los sistemas de IA (punto 15).

[30] En este sentido, *vid*. Ramalho, A. (2018). "Machines that create and how EU copyright law views them", en *Kluwer Copyright Blog*, en Internet: https://copyrightblog.kluweriplaw.com/2018/11/12/ex-machina-ex-auctore-machines-that-create-and-how-eu-copyright-law-views-them/ (u. v. 05/08/2024).

[31] Saiz García, C. "Las obras creadas...", *op. cit.*, p. 32.

personas jurídicas (productores, organismos de radiodifusión o editoriales de publicaciones de prensa), que busca recuperar la inversión, que el otorgado a los artistas intérpretes o ejecutantes, que trata de proteger la prestación personal que llevan a cabo. El problema reside en definir el objeto sobre el que recae el derecho, su titular y su contenido. En cuanto a lo primero, este derecho conexo recaería sobre un producto carente de originalidad, como es el resultado derivado del uso de un sistema de IA generativo. Respecto a su titular, el derecho habría que reconocerlo a aquella persona que haya realizado la inversión sustancial, que no necesariamente coincidirá con la persona física que ha creado el programa para el funcionamiento del sistema de IA. Finalmente, el contenido de este derecho conexo se reduciría a derechos de exclusiva (reproducción, distribución y comunicación pública), sin reconocer derechos morales, si bien de una manera menos extensa que respecto a otros titulares de derechos conexos –cabría pensar en un esquema similar al atribuido a las editoriales de publicaciones de prensa y a las agencias de noticias en los artículos 15 Directiva 2019/790 y 129bis LPI–.

Con todo, existen derechos conexos reconocidos con independencia de la inversión que requiera la obtención de un resultado y que no implican una prestación personal, como son los atribuidos a los realizadores de meras fotografías. En estos casos, estas quedan protegidas a través del artículo 128 LPI, cuando el fotógrafo se limite a apretar el botón de la cámara, sin más. Su intervención queda reducida a la elección del tema que se va a fotografiar, pero no hay una labor creativa y original. No se concede el derecho conexo a quien invierte en la creación de cámaras de fotos –y no por eso se desincentiva la inversión, pues cada vez son más sofisticadas–, sino a quien utiliza la máquina y realiza la fotografía. Aplicando un esquema similar a los resultados producidos por IA generativa, podría concederse un derecho de exclusiva a la persona que se limita a apretar el botón de la máquina para que aquel tenga lugar o a introducir las instrucciones para que se genere. De esta manera, no se podría impedir que otro sistema de IA pudiera realizar un resultado similar o prácticamente idéntico, sino que se utilizara dicho resultado concreto sin el consentimiento de su titular. No obstante, es cuestionable que la aportación que hace el usuario al resultado tenga la suficiente relevancia como para merecer un derecho de exclusiva como el que otorga el artículo 128 LPI sobre las meras fotografías, protegidas, en muchas ocasiones, por su valor comercial, dada su importancia documental.

Por lo que se refiere al derecho *sui generis*, los artículos 7 y siguientes Directiva 96/9, y 133 y siguientes de la LPI lo otorgan a los fabricantes de bases de

datos, que quedarán protegidas incluso aunque estas carezcan de originalidad (arts. 7.4 Directiva 96/9 y 133.4 LPI). Sin embargo, varios son los argumentos que llevarían a excluir la aplicación del derecho *sui generis*[32]. En primer lugar, porque la elaboración de la propia base de datos requiere una actividad humana, algo que no ocurre en la producción de un resultado a través de los sistemas de IA generativos –la intervención humana está en la creación del *software* necesario para el funcionamiento del sistema, pero no en la producción misma del resultado–. Y, en segundo lugar, los productos generados no encajan en la definición de base de datos de los artículos 1.2 Directiva 96/9 y 12 LPI, pues no todos ellos constituirán elementos dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma.

En definitiva, no parece adecuado plantear la creación de un derecho conexo o de un derecho *sui generis*, aplicable a los resultados de los sistemas de IA generativa[33]. El objetivo pretendido (recuperación de la inversión), muy loable, no necesariamente tiene que conseguirse aplicando la protección de la propiedad intelectual sobre los resultados generados por la máquina –de la misma manera que los desarrolladores de cámaras de fotos no pueden pretender tener derechos de exclusiva sobre las fotografías que hagan los usuarios con ellas ni los titulares de programas de ordenador sobre las creaciones que realicen los usuarios del *software*–. Además, resulta muy complejo determinar las características que debe cumplir la inversión que tiene que producirse. Respecto de las bases de datos, la normativa exige que sea sustancial (art. 7.1 Directiva 96/9 y 133.1 LPI), pero no se concreta qué debe entenderse por tal[34]. Esta imprecisión podría acarrear el riesgo de proteger cualquier resultado generado por un sistema de IA, con independencia del

---

[32] Apunta estos argumentos Sanjuán Rodríguez, N., "Inteligencia artificial...", *op. cit.*, p. 92. A favor de la protección a través del derecho *sui generis*, *vid*. Minero Alejandre, M., "Inteligencia artificial...", *op. cit.*, p. 88; Aparicio Vaquero, J. P., "Derecho de autor...", *op. cit.*, p. 52. A favor de la protección a través del derecho *sui generis* se ha manifestado el Consejo Superior de la Propiedad Literaria y Artística, del Ministerio de Cultura francés, en su informe sobre inteligencia artificial y cultura (pp. 44-45), reseñado en la nota 7.

[33] Tampoco termina de acoger esta opción el Max Planck Institute en su informe sobre IA (p. 22), referido en la nota 7.

[34] *Vid*. sobre esta cuestión Minero Alejandre, G. (2023). "Estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de protección de las bases de datos: de los errores no reconocidos a las modificaciones indirectas de la Directiva. Identificación de las imprecisiones de la futura Data Act a la luz de la doctrina jurisprudencial", en *Revista Pe.i.*, núm. 72, pp. 18 y ss.

calado de la inversión, lo que podría afectar a la libre competencia. De la misma manera, la atribución de un plazo de duración de estos derechos constituye una tarea difícil, pues no tiene sentido una protección demasiado larga en un medio (la innovación) que se caracteriza por la rapidez en los cambios.

La penúltima posibilidad sería otorgar derechos de autor sobre los resultados a los titulares de derechos de las obras que han servido de "alimento" al sistema de IA generativa. En este sentido se pronuncia el artículo 2 de la Proposición francesa de Ley núm. 1630, encaminada a regular la IA a través del derecho de autor[35]. Dicho precepto viene a modificar el artículo L. 321-2 del Código francés de la Propiedad Intelectual, para atribuir a los autores derechos sobre los resultados de los procesos de IA, siempre que se pueda establecer la trazabilidad con tales obras. Sin embargo, como se ha indicado anteriormente, cuesta pensar en un derecho de autor sobre una producción en la que no han intervenido activamente. Además, los resultados normalmente toman como base multitud de obras, por lo que será muy complejo determinar qué proporción de autoría tiene cada uno.

Una última posibilidad sería no otorgar derechos a nadie sobre los resultados generados por el uso de IA. No todo lo que produzca una máquina puede ser protegido por la propiedad intelectual, por mucha similitud que tenga con una obra literaria o artística. Así, esos resultados pasarían, desde el momento de su producción, al dominio público, de tal manera que cualquiera podría utilizarlas, atendiendo al derecho de acceso a la cultura, recogido en el artículo 44 de la Constitución Española. Dado que no pueden atribuirse a ninguna persona física, se incumple el principio de autoría y deberían pasar al dominio público[36]. Piénsese que una buena parte de las obras de las que se nutren los sistemas de IA están en el dominio público, por lo que no sería descabellado afirmar que los resultados generados entren también en el dominio público. Esta opción plantea dos problemas. El primero es que los sistemas de IA también se entrenan mediante obras aún protegidas y que no han pasado aún al dominio público. De hecho, la excepción sobre minería de textos y datos, recogida en

---

[35] Disponible en Internet: https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi (u. v. 05/08/2024).

[36] A favor de esta opción, *vid.*, Ginsburg, J. C. y Budiardjo, A. L., "Authors and Machines... *op. cit.*, pp. 446-447; Ramalho, A. (2017). "Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems", *Forthcoming in the Journal of Internet Law*, p. 19.

los artículos 3 y 4 Directiva 2019/790 y 67 RD-ley 24/2021, permite el uso de obras y prestaciones a estos efectos. Y el segundo problema tiene que ver con la pérdida de interés que podría producir en los desarrolladores de este tipo de sistemas, que no tendrían ningún incentivo en invertir en estas tecnologías si luego los resultados no van a ser objeto de ninguna protección. No obstante, conviene reiterar que el interés y la inversión no deberían estar condicionados a una atribución de derechos de propiedad intelectual sobre los resultados[37].

Finalmente, podríamos plantear la posibilidad de proteger los resultados derivados del uso de sistemas de IA generativa a través de un derecho de propiedad ordinaria a favor del propietario de la máquina o del usuario, fuera ya de la propiedad intelectual[38]. En el caso del propietario, de nuevo, por la inversión realizada en la adquisición del sistema. Y, en el caso del usuario, por el hecho de haberlo utilizado dándole un mínimo de instrucciones para generar el resultado –como ocurre, por ejemplo, con las fotografías obtenidas a través de un fotomatón–. Se trataría de un régimen similar al aplicable a la creación realizada por un animal. Somos propietarios del soporte en el que queda plasmada, pero carecemos de derechos de propiedad intelectual sobre ella.

En conclusión, no parece que los resultados producidos por IA generativa merezcan la protección de la propiedad intelectual. Además de la dificultad a la hora de determinar el alcance exacto de los mismos y su plazo de duración, podría tener un impacto negativo en los creadores personas físicas, que quedarían debilitados en el mercado frente a esas creaciones artificiales. La protección de estos contenidos, de rápida realización y fácil acceso, a través de la propiedad intelectual podría llevar a una infravaloración del esfuerzo creativo realizado por autores personas físicas. Podríamos llegar a una masificación de contenidos y a una saturación del mercado de la cultura, en perjuicio del autor tradicional. El valor está en dos elementos: 1) el sistema de IA; y 2) los contenidos que sirven para entrenar al sistema de IA. El primero está ya debidamente protegido. Los segundos, si bien están protegidos, no lo están a un nivel suficiente frente a la potencia de estas tecnologías. Para evitar la sustitución de las obras generadas

---

[37] Así lo entienden Glesser, D., "Copyright in Computer-Generated Works...", *op. cit.*, p. 7; Morán, M., "Creadores en riesgo...", *op. cit.*, p. 20.

[38] Apuntan esta opción Sanjuán Rodríguez, N., "Inteligencia artificial...", *op. cit.*, p. 87; Saiz García, C., "Las obras creadas...", *op. cit.*, p. 35.

por personas físicas por los contenidos producidos por IA, podría contemplarse un sistema de compensación, imponiendo una obligación de pago a los proveedores de herramientas de IA generativa y refugiándolo en la gestión colectiva obligatoria[39]. Quedando ambos elementos bien protegidos, los resultados pueden perfectamente tutelarse a través de un derecho de propiedad ordinario.

3.2. La originalidad de los resultados producidos por IA generativa

Además de que la creación sea fruto de un esfuerzo humano, otro requisito que se exige para obtener la protección dispensada por la LPI es que se trate de un resultado original (*vid*. art. 10). El CB no habla de "originalidad", sino de "creación intelectual" en su artículo 2, de donde parece desprenderse tal exigencia[40]. La doctrina ha venido manejando un doble concepto de originalidad: objetivo y subjetivo. El primero tiene que ver con la novedad. Conforme al concepto objetivo, algo es original si es nuevo. Ahora bien, para recibir protección es necesario que exista un mínimo de altura creativa. Sólo entonces se entiende que el esfuerzo realizado por el autor es merecedor de protección. En cambio, conforme al concepto subjetivo algo es original cuando es el reflejo de la personalidad del autor en la obra. En todo caso, el concepto de "originalidad" no puede estar sujeto a consideraciones subjetivas, no puede depender de la valoración personal que haga el sujeto que está contemplando la obra, sino que debe construirse sobre la base de criterios objetivos, de tal manera que se pueda atribuir la condición de original a la obra con independencia de que guste o no al público. El considerando 16 Directiva 2006/116 establece que la creación intelectual, para estar protegida, debe reflejar la personalidad del autor, sin que se tome en cuenta ningún otro criterio como el mérito o la finalidad, lo que parece decantarse por un concepto subjetivo de originalidad. Ciertas directivas europeas hablan, a la hora de determinar el objeto protegido, de creaciones intelectuales propias de su autor. Así ocurre con los programas de ordenador (art. 1.3 Directiva 2009/24), con las bases de datos (art. 3.1 Directiva 96/9) y con las fotografías (art. 6 Directiva 2006/116).

---

[39] Propone esta solución Senfleben, M. (2023). "Generative AI and Author Remuneration", en *International Review of Intellectual Property and Competition*, Vol. 54, p. 22.

[40] Bercovitz Rodríguez-Cano, R. (2013). "Artículo 2", en *Comentarios al Convenio de Berna*, R. Bercovitz Rodríguez-Cano (coord.), Tecnos, Madrid, p. 104.

El TJUE ha desarrollado un concepto autónomo del Derecho de la Unión con un claro carácter subjetivista[41]. Según el TJUE, la obra debe ser original, en el sentido de constituir una creación intelectual propia de su autor, produciéndose esto último cuando refleje su personalidad, lo que sucede cuando aquél haya podido expresar su capacidad creativa tomando decisiones libres y creativas e imprimiendo su toque personal. Si la realización de un objeto ha venido determinada por consideraciones técnicas, reglas u otras exigencias que no han dejado espacio al ejercicio de dicha libertad, no podrá considerarse que exista la originalidad necesaria como para estar ante una obra. Así lo ha manifestado en sus sentencias de 16 de julio de 2009[42], de 1 de diciembre de 2011[43], de 1 de marzo de 2012[44], de 29 de julio de 2019[45] o de 12 de septiembre de 2019[46], entre otras. Por tanto, la personalidad del autor debe estar plasmada en la obra, lo que implica que el autor sea consciente en todo momento en su producción[47]. Este concepto subjetivo está conectado íntimamente a la consideración del autor como persona física, puesto que sólo así puede haber impronta de la personalidad del autor, algo que no es posible en un sistema de IA. Asimismo, en la sentencia de 13 de noviembre de 2018, el TJUE establece el concepto autónomo de "obra", apuntando que debe poder identificarse con suficiente precisión y objetividad[48]. Nuestra jurisprudencia, por el contrario, ha venido aplicando un criterio eminentemente objetivo, ligado a la novedad y a la exigencia de altura creativa (entre otras, SSTS 24 de junio de 2004, de 9 de diciembre de 2010, de 5 de abril de 2011, de 27 de septiembre de 2012, de 25 de junio de 2013 o de 26 de abril de 2017[49]).

---

[41] Sobre el concepto autónomo de "originalidad" elaborado por el TJUE, *vid*. Cámara Águila, P. (2019). "Los conceptos autónomos sobre el objeto de protección del derecho de autor: el concepto de obra y el concepto de originalidad", en *La unificación del Derecho de propiedad intelectual en la Unión Europea*, P. Cámara Águila e I. Garrote Fernández-Díez (coords.), Tirant lo Blanch, Valencia, pp. 47 y ss.

[42] Caso *Infopaq International*, asunto C-5/08, pár. 35 ECLI:EU:C:2009:465.

[43] Caso *Painer*, asunto C-145/10, párs. 88-89 y 92, ECLI:EU:C:2011:798.

[44] Caso *Football Dataco*, asunto C-604/10, pár. 38, ECLI:EU:C:2012:115.

[45] Caso *Funke Medien*, asunto C-469/17, pár. 19, ECLI:EU:C:2019:623.

[46] Caso *Cofemel*, asunto C-683/17, párs. 30-31, ECLI:EU:C:2019:721.

[47] DUQUE LIZARRALDE, M. "Las obras creadas... *op. cit.*, p. 33.

[48] Caso *Levola*, asunto C-310/17, pár. 33, ECLI:EU:C:2019:899.

[49] RJ 2004/4318, RJ 2011/1407, RJ 2011/3146, RJ 2012/9707, RJ 2013/4981 y RJ 2017/1736, respectivamente. No obstante, nuestro TS también ha utilizado el concepto subjetivo de originalidad en algunas sentencias. Entre otras, *vid*. SSTS de 26 de noviembre de 2003 (RJ 2003/8098) y de 16 de febrero de 2021 (RJ 2021/456).

Lo anterior nos lleva a concluir que, en el caso de IA generativa, no cabe hablar de originalidad, por lo que no resultaría posible atribuir un derecho de autor. El usuario no realiza un esfuerzo creativo ni es posible calificar de original la obra. El proceso de creación de una obra original conlleva un esfuerzo, unas emociones y unas vivencias de las que se sirve el autor –incluso su personalidad le influye a la hora de crear–, y nada de esto ocurre en el caso de la IA generativa. Precisamente, el resultado generado por el uso de estos sistemas viene dado por consideraciones técnicas e instrucciones introducidas en la máquina. Si está configurada de tal manera que la expresión del resultado sólo es posible a través de una única vía, entonces no habrá originalidad. En cambio, en los supuestos de IA asistida, es posible que el usuario sea considerado autor y el resultado sea original cuando ha sido capaz de plasmar, siquiera a través de la máquina, su impronta personal, de la misma manera que puede ocurrir con el uso de una cámara de fotos o de un *software* para retocar una obra audiovisual[50]. En estos casos, el sistema de IA constituye una herramienta o instrumento del que se ayuda la persona física para conseguir un resultado creativo. Para ello, es necesario que el realizador de la obra pueda tomar decisiones creativas y que el resultado no venga dado por las instrucciones previamente incorporadas por el programador. Cuanto más concreto sea el usuario a la hora de dar indicaciones a la máquina y señalar qué es lo que quiere y cómo lo quiere, más originalidad habrá en el resultado. Y viceversa: cuando el usuario se limita a dar instrucciones generales y es la máquina la que decide sobre el resultado final con base en los parámetros previamente introducidos por el programador, la originalidad será, más bien, escasa.

La pregunta es: ¿hasta qué punto el sistema de IA debe actuar solo, sin la participación de un ser humano, para que el resultado sea excluido de la protección del derecho de autor? ¿Qué tipo de actuaciones de la persona física son las que hacen imprimir originalidad a un resultado producido a través de un sistema de IA? Las actuaciones meramente técnicas o mecánicas no dotan de originalidad al resultado obtenido. No son actividades lo suficientemente cualificadas como para imprimir originalidad al resultado todas aquellas que sirven para permitir que el sistema de IA opere de manera autónoma, como, por ejemplo, el

---

[50] Yu, R., "The Machine Author: What Level of Copyright Protection is appropriate for Fully Independent Computer Generated Works?", en *University of Pensylvania Law Review*, núm. 165, 2017, p. 1245; Denicola, R. (2016). "Ex Machina: Copyright Protection for Computer-Generated Works", en *Rutgers University Law Review*, núm. 69.

entrenamiento del sistema de IA con meros datos o a través de un rastreo masivo de Internet, o la digitalización de objetos (ej.: una pintura o una escultura), o el dar una orden sencilla[51]. En cambio, sí podría dotar de originalidad al resultado tareas como la elección de los colores, de la forma, de los materiales y del resto de los elementos que aparecen en la pintura final, la determinación del nombre de los personajes y de las tramas, o la incorporación de la letra de una canción para la cual el sistema de IA realizará la música. En definitiva, se trata de acciones imprescindibles para que la máquina pueda alcanzar el resultado final que nosotros queremos, introduciéndole una serie de patrones. En este caso, el margen de maniobra que tiene el sistema de IA es menor porque las decisiones creativas las tomamos nosotros. Asimismo, téngase en cuenta que la selección de los contenidos a partir de los cuales operará dicho sistema en la fase de entrenamiento puede ser original, pues no puede perderse de vista que, con ello, se crea una base de datos que tendrá originalidad cuando la selección o disposición de sus contenidos constituya una creación intelectual. Ahora bien, esto imprimirá originalidad, llegado el caso, a la base de datos con la que nutrimos al sistema, no al resultado mismo que se produzca.

El desarrollo de esta tecnología aún no es lo suficientemente sofisticado como para poder producir algo por sí sola, sino que necesita basarse en obras y datos preexistentes. La "libertad creativa" de la IA generativa está, en cierta medida, restringida, pues produce a partir de los contenidos rastreados previamente accesibles o introducidos en la máquina. A la hora de valorar la originalidad de un objeto generado por IA, resulta irrelevante la pericia, el esfuerzo realizado o la inversión económica[52]. Tampoco es importante la imprevisibilidad del resultado, pues algo no es original por el mero hecho de haber resultado imprevisible.

En los casos de IA generativa y en los de IA asistida en los que no haya originalidad, no resulta apropiado hablar de "obra" para referirse a lo que genera la máquina, sino, más bien, de "resultado" o "producto"[53]. Esto tendrá un efecto indirecto evidente: la desprotección de aquellos artistas intérpretes o ejecutantes que canten, reciten, interpreten o ejecuten contenidos producidos por IA

---

[51] Minero Alejandre, M. "Inteligencia artificial...", *op. cit.*, p. 90.

[52] Saiz García, C. "Las obras creadas...", *op. cit.*, p. 19.

[53] Así lo entienden Aparicio Vaquero, J. P., "Derecho de autor...", *op. cit.*, p. 52; Navas Navarro, S. (2018). "Obras generadas por algoritmos, en torno a su posible protección jurídica", *Revista de Derecho Civil*, núm. 2, p. 287.

generativa. Y ello porque los artículos 2.a) Tratado OMPI sobre Interpretación o Ejecución y Fonogramas, 2.a) Tratado OMPI sobre Interpretaciones y Ejecuciones Audiovisuales y 105 LPI, otorgan la condición de artista intérprete o ejecutante a la persona que represente, cante, lea, recite, interprete o ejecute en cualquier forma una obra. Sería necesario modificar estas normas para que también queden protegidos cuando hagan estas mismas acciones respecto de contenidos generados por IA, que no constituyen obra. Piénsese que no es nada raro que un sistema de IA cree una partitura, la letra de una canción, el guion de una película o un poema.

3.3. El entrenamiento de los sistemas de IA a partir de obras y prestaciones protegidas

Para que un sistema de IA pueda funcionar correctamente y genere contenidos, es preciso entrenarlo. Ese trabajo de entrenamiento consiste en suministrar a la máquina grandes cantidades de contenidos preexistentes en los que pueda basarse para crear otros nuevos o en configurarla de tal manera que pueda rastrear la red en su búsqueda –no debe perderse de vista que los resultados generados por IA también pueden servir de "alimento" de otros sistemas para producir–. La riqueza de éstos dependerá del material que se le haya introducido previamente. En ese proceso de alimentación o de rastreo, podemos encontrarnos con varios tipos de materiales: a) obras que están en el dominio público, carentes de todo tipo de protección, pero respecto de las cuales hay que respetar el derecho de paternidad y de integridad; b) contenidos totalmente desprotegidos por la propiedad intelectual por carecer de originalidad; c) contenidos carentes de originalidad, pero protegidos por algún derecho conexo (ej.: meras fotografías, grabaciones audiovisuales) o por un derecho *sui generis* (ej.: los datos contenidos en una base de datos no original); d) obras que están protegidas porque aún no ha transcurrido el plazo de protección; y e) obras que están protegidas por la propiedad intelectual, pero cuyo autor ha autorizado un uso libre a través de una licencia *Creative Commons* –dentro de esta categoría, es posible que el autor haya autorizado o no los usos comerciales y haya consentido o no los usos transformativos–.

Los dos primeros supuestos no plantean problema, en tanto que, al estar los contenidos desprotegidos o en dominio público, pueden servir de "alimento" al sistema de IA –respetando, eso sí, el derecho de integridad en al supuesto a)–. Más problemáticos resulta el resto de los supuestos. La solución hay que buscarla en la excepción relativa a la minería de textos y datos, recogida en los artículos 3

y 4 Directiva 2019/790, de derechos de autor y derechos conexos en el mercado único digital, transpuestos en nuestro ordenamiento a través del artículo 67 Real Decreto-ley 24/2021. Se trata de una excepción de transposición obligatoria para los Estados miembros, pues la labor de minería es imprescindible para el desarrollo de sistemas de IA[54]. Cabe señalar, antes de analizar tales excepciones, que no sería posible aplicar el límite sobre reproducciones provisionales, incluido en los artículos 5.1 Directiva 2001/29 y 31.1 LPI, pues las copias introducidas en sistemas de IA no tienen un carácter temporal, sino que deben ser almacenadas durante todo el tiempo necesario para la producción de resultados, y tienen un significado económico independiente.

La minería de textos y datos incluye toda técnica analítica automatizada destinada a analizar textos y datos en formato digital con el fin de generar información que incluye pautas, tendencias, correlaciones o elementos similares (arts. 2.2 Directiva 2019/790 y 66.1 RD-ley 24/2021). El Reglamento IA denomina a los datos usados para entrenar un sistema de IA a través del ajuste de sus parámetros entrañables "datos de entrenamiento" (art. 3.29). Y constituyen "datos de entrada" aquellos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce la información de salida (art. 3.33). La Directiva 2019/790 recoge dos excepciones para la minería: una para fines de investigación científica, realizada por organismos de investigación y por instituciones responsables del patrimonio cultural (art. 3) y otra de alcance más general (art. 4). En cambio, el legislador español no distingue claramente entre ambas finalidades en el artículo 67 RD-ley 24/2021, resultando un precepto caótico y complejo en cuanto a su interpretación[55]. El concepto de «minería» es tan amplio, que abarcaría las técnicas de *machine learning* para entrenar los sistemas de IA[56].

---

[54] El Max Planck Institute for Innovation and Competition alerta sobre la incertidumbre que plantean los requisitos necesarios para la aplicación de las excepciones sobre minería. Señala que no son lo suficientemente flexibles, lo que provocará una reducción de su utilidad práctica. *Vid*. Informe sobre la relación entre la IA y la propiedad intelectual (pp. 7-8), referido en la nota 7.

[55] Sobre las excepciones de minería y la problemática de su transposición al ordenamiento español, *vid*. Gemma Minero, A., "Los dos límites (el obligatorio y el optativo) de minería de textos y datos", en *La transposición en España de la Directiva sobre derechos de autor y mercado único digital*, dirs. P. Cámara Águila e I. Garrote Fernández-Díez, Tirant, Valencia, 2024 (en prensa).

[56] Margoni, T. y Kretschmer, M., «A deeper look into the EU Text and Data Mining exceptions: Harmonisation, data ownership, and the future of technology», en *CREATe*, núm.

Conforme al artículo 3.1 Directiva 2019/790, los organismos de investigación y las instituciones responsables del patrimonio cultural pueden realizar reproducciones y extracciones de obras y prestaciones a las que hayan tenido acceso lícito, para llevar a cabo minería de textos y datos con fines de investigación científica. Se trata de un límite a los derechos previstos en el artículo 5.a) y 7.1 Directiva 96/9 (derecho de reproducción de los autores de bases de datos y derechos de extracción y reutilización de los fabricantes de bases de datos), en el artículo 2 Directiva 2001/29 (derecho de reproducción concedido a los autores, a los artistas intérpretes o ejecutantes, a los productores y a los organismos de radiodifusión) y en el artículo 15.1 Directiva 2001/790 (derecho de reproducción y de puesta a disposición reconocido a las editoriales de publicaciones de prensa). El legislador ha entendido que la minería afecta, básicamente, al derecho de reproducción. La excepción no cubre, en cambio, la distribución ni la comunicación pública de obras y prestaciones, por lo que la minería que implique tales actos estará sujeta, en todo caso, a la autorización de los titulares de derechos. Tampoco la transformación, a pesar de que, en ocasiones, el minado y el proceso de elaboración de un producto a través de sistemas de IA puede conllevar la transformación de obras preexistentes, yendo más allá de una mera digitalización[57]. Se deja de lado el derecho de transformación por dos motivos: 1) porque no está armonizado en la UE para las obras en general; y 2) por la dificultad que supone el determinar si se ha producido o no una transformación en estos casos. Asimismo, también es evidente el riesgo que puede suponer para el derecho moral de integridad, recogido en nuestro ordenamiento en el artículo 14.4º LPI –piénsese, por ejemplo, en un sistema de IA que acaba una obra inconclusa tras haber fallecido su autor–. Sin embargo, tampoco los derechos morales han sido objeto de armonización.

A pesar de que esta primera excepción de minería beneficia exclusivamente a los organismos de investigación y a las instituciones responsables del patrimonio cultural que persigan una finalidad investigadora, cabe la posibilidad de que recurran a socios privados para realizar la minería, en caso de que no dispongan

7, 2021, 24-28. Sobre las diferencias entre el *machine learning* y la minería de textos y datos, *vid*. Nadal Cebrián, M., «¿Pueden los sistemas de inteligencia artificial "aprender" utilizando obras protegidas por derechos de propiedad intelectual sin la autorización de sus titulares? Los retos del *machine learning* en perspectiva comparada: UE, EE. UU. y Japón», en *Revista Pe.i.*, núm. 68, 2021, pp. 41 y ss.

[57] Lee, K., Cooper, A. F., y Grimmelmann, J. (2024). "Talkin'Bout AI Generation: Copyright and the Generative-AI Supply Chain", *Journal of the Copyright Society*, p. 63.

de los medios tecnológicos adecuados (cdo. 11 Directiva 2019/790). En todo caso, debe haber un acceso lícito a la obra o prestación sobre la que se realizará la minería. Esta exigencia se cumplirá en los casos de acceso a contenidos basado en una política de acceso abierto o por medio de disposiciones contractuales entre los titulares de derechos y los beneficiarios de este límite, como suscripciones, o por otros medios lícitos, así como el acceso a contenidos disponibles de forma gratuita en línea (cdo. 14 Directiva 2019/790). Además, el legislador europeo cierra la puerta a someter la aplicación de la excepción a algún tipo de compensación para los titulares de derechos, pues entiende que el posible perjuicio que se les pueda causar será mínimo (cdo. 17 Directiva 2019/790). En todo caso, los titulares de derechos podrán aplicar medidas para garantizar la seguridad e integridad de las redes y bases de datos en que estén almacenadas las obras y prestaciones, si bien tales medidas no podrán ir más allá de lo necesario para conseguir dichos objetivos (arts. 3.3 Directiva 2019/790 y 67.4.II RD-ley 24/2021).

La excepción relativa a la minería de textos y datos del artículo 4.1 Directiva 2019/790 se refiere a todos los derechos anteriores y, además, al derecho de reproducción y al derecho de transformación reconocido a los autores de programas de ordenador en las letras a) y b) del artículo 4.1 Directiva 2009/24, respectivamente –el artículo 67 RD-ley 24/2021 sí parece cubrir estos derechos a través de la minería, con independencia de la finalidad–. En este caso de minería con alcance más general, se permite el uso de obras y prestaciones a cualquier tercero, siempre y cuando se haya accedido a ellas de forma legítima. Así, cubriría: a) la minería llevada a cabo por cualquiera, incluyendo los organismos de investigación y las entidades responsables del patrimonio cultural, para fines diferentes de la investigación científica, entre los que cabría incluir los lucrativos; b) la minería realizada por sujetos distintos a los organismos de investigación y a las entidades responsables del patrimonio cultural, para fines de investigación científica. Y es que la minería es fundamental para el desarrollo de nuevas aplicaciones y tecnologías, como pone de manifiesto el considerando 18 Directiva 2019/790. Aquí el legislador europeo tampoco entiende que se ocasione un perjuicio excesivo a los titulares de derechos con el uso de obras y prestaciones a efectos de minería para fines distintos de la investigación científica, por lo que, a su juicio, ni siquiera en estos casos debería preverse una compensación a cambio de disfrutar del límite –obsérvese que el considerando 17 Directiva 2019/790 se refiere a las excepciones relativas a minería, en plural, lo que abarcaría tanto el artículo 3 como el artículo 4 de dicha directiva–.

Por otro lado, según el artículo 7.1 Directiva 2019/790, toda disposición contractual contraria al uso de obras y prestaciones para la minería a que se refiere el artículo 3 de dicha norma será inaplicable. El legislador europeo no quiere que se pueda impedir esta excepción por parte de los titulares de derechos, pues es consciente de que las actividades de investigación pueden afectar a la posición competitiva de la UE como espacio de investigación (cdo. 10 Directiva 2019/790). En cambio, no hay una previsión similar para la minería a que se refiere el artículo 4 Directiva 2019/790, esto es, la realizada con fines diferentes a la investigación científica o por entidades distintas a las mencionadas en el artículo 3 Directiva 2019/790, por lo que sería perfectamente posible pactar contractualmente la prohibición de minería (por ejemplo, la realizada con fines lucrativos). El legislador español no ha transpuesto la posibilidad contemplada en el artículo 7 Directiva 2019/790, por lo que se plantea la duda de si ha cercenado a los titulares de derechos la posibilidad de impedir la minería en estos casos.

Igualmente, el artículo 4.3 Directiva 2019/790 somete la aplicación de esta excepción a la condición de que el uso de obras y prestaciones para fines de minería contemplado en ese precepto no esté reservado expresamente por los titulares de derechos de manera adecuada –el artículo 67.3 RD-ley 24/2021, al no distinguir la finalidad concreta que debe perseguirse con la minería, genera la cuestión de si la reserva de derechos resulta aplicable también a aquella que persiga fines de investigación–. Es decir, los titulares de derechos de propiedad intelectual pueden oponerse a que sus obras y prestaciones sean utilizadas a efectos de minería para fines distintos de la investigación científica por cualquier entidad o para fines de investigación por entidades distintas a las mencionadas en el artículo 3 Directiva 2019/790 –esto hace que no quepa calificar este tipo de minería de verdadera excepción–[58]. Cuando el titular de los derechos se haya reservado adecuadamente

[58] Se ha defendido que la minería de obras y prestaciones debería ser un uso que siempre estuviera permitido, sin que pudiera estar en manos de los titulares de derechos, llegándose a hablar, incluso, de un derecho a la lectura por las máquinas, al igual que ocurre con las personas físicas. *Vid*. Hilty, R. y richter, H., «Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules Part B Exceptions and Limitations (Art. 3 – Text and Data Mining)», en *Max Planck Institute for Innovation and Competition*, núm. 17(2), 2019, p.5; Geiger, G., Frosio, G., y Bulayenko, O., «The exception for Text and Data Mining (TDM) in the proposed Directive on copyright in the digital single market – legal aspects», en *Center for International Intellectual Property Studies*, núm. 2, 2018, p. 32; Ducato, R., y Strowel, A., «Limitations To Text and Data Mining and Consumer Empowerment. Making the Case for a Right to «Machine Legibility», en *CRIDES*, 2018, pp. 20-21.

el derecho de exclusión, los proveedores de sistemas de IA deberán obtener su autorización para llevar a cabo la minería (cdos. 105 y 106 Reglamento IA). A la hora de hacer esa reserva, el considerando 18 Directiva 2019/790 distingue dos posibles supuestos: 1) en el caso de contenidos puestos a disposición del público online, la reserva de derechos debería hacerse a través de medios de lectura mecánica, incluyendo los metadatos y las condiciones de un sitio web o un servicio; y 2) en otros supuestos, la reserva se puede hacer mediante otros medios, como los acuerdos contractuales o una declaración unilateral. Por otro lado, la posibilidad de reserva de derechos requiere un sistema adecuado de licencias que permitan al titular de los derechos, llegado el caso, consentir el uso a efectos de minería a cambio de una remuneración. Por tanto, si los titulares de derechos no se oponen a la minería a que se refiere el artículo 4 Directiva 2019/790, se presume que la consienten. La falta de oposición es expresión de su consentimiento implícito. Ahora bien, para que el titular de derechos pueda decidir adecuadamente si autoriza o no la minería, es necesario que esté debidamente informado, especialmente sobre los usos que se van a hacer de su obra o prestación. Sin esta información previa, el titular de derechos no estará en disposición de posicionarse al respecto. En este sentido se pronunció el TJUE en su sentencia de 16 de noviembre de 2016, exigiendo, en estos supuestos en que se concede una facultad de oposición o exclusión, la existencia de un mecanismo que garantice la información efectiva e individualizada a los titulares de derechos (aps. 37-43)[59].

El problema surge en el propio funcionamiento de aquellos sistemas de IA donde se produce un rastreo masivo e indiscriminado de contenidos para entrenar a la máquina. Cuando es una persona la que "alimenta" al sistema de IA con obras y prestaciones concretas, esta debe tener especial cuidado para no introducir contenidos respecto de los cuales los titulares de derechos hayan querido impedir su uso con fines de minería –obviamente, en aquellos casos en que cabe impedirlo–. Sin embargo, cuando el sistema está programado para que haga un rastreo en Internet para poder entrenarse, resulta muy complicado evitar tales contenidos. La única manera de conseguirlo es utilizando medidas tecnológicas que impidan el acceso, lo que coloca a las espaldas de los titulares de derechos la obligación de hacer uso de ellas si quisieran impedir la aplicación de la excepción de minería recogida en el artículo 4 Directiva 2019/790 –de hecho, su apartado

[59] Caso *Soulier*, asunto C-301/15, ECLI:EU:C:2016:878.

tercero establece que la reserva debe hacerse "de manera adecuada"–. A estos efectos, según el TJUE, la única manera de garantizar la seguridad jurídica y el buen funcionamiento de Internet es utilizando medidas tecnológicas efectivas a la hora de limitar el consentimiento por parte de los titulares de derechos (SSTJUE de 9 de marzo de 2021[60] y de 23 de enero de 2014[61]). A su juicio, a falta de tales medidas, podría resultar difícil comprobar si un titular pretendía oponerse al uso de una obra o prestación, sobre todo cuando este ha sido objeto de sublicencias.

Esto nos lleva a verificar la relación que tienen las excepciones con el uso de medidas tecnológicas. El artículo 7.2 Directiva 2019/790 apunta que los párrafos primero, tercero y quinto del artículo 6.4 Directiva 2001/29 serán aplicables a, entre otros, los artículos 3 y 4 de aquélla –el legislador español también omite esta cuestión en el artículo 67 RD-ley 24/2021–. Esta previsión del legislador europeo resulta muy complicada de interpretar y plantea no pocos problemas. El artículo 6.4.I Directiva 2001/29 establece que los titulares de derechos, a pesar de utilizar medidas tecnológicas, deben garantizar el disfrute de determinados límites, y enumera los contenidos en las letras a), c), d) y e) del artículo 5.2 y las letras a), b) y e) del artículo 5.3 Directiva 2001/29 –la aplicación de tales límites se condiciona, no obstante, a que el beneficiario de los mismos haya tenido un acceso legal a la obra o prestación–. Como se puede comprobar, no todos los límites recogidos en el artículo 5 Directiva 2001/29 deben quedar asegurados cuando los titulares de derechos utilizan medidas tecnológicas. El propio considerando 7 Directiva 2019/790 señala la importancia de que el uso de medidas tecnológicas no impida el disfrute de las excepciones establecidas en esa directiva. En definitiva, el artículo 7.2 Directiva 2019/790 está incluyendo en este listado de límites privilegiados la minería, tanto la del artículo 3 como la del artículo 4. Ahora bien, en caso de que el titular de derechos impida su disfrute mediante medidas tecnológicas, los beneficiarios del límite de minería no pueden eludirlas por sí mismos, pues el propio acto de elusión constituye una infracción, conforme al artículo 6.1 Directiva 2001/29 –en el caso de España, tendrán que acudir a la jurisdicción civil para que sea un juez quien obligue a la retirada de la medida tecnológica (art. 197.2 LPI)–. En consecuencia, la elusión por cuenta de usuario de las medidas tecnológicas que impidan la minería conllevará

---

[60] Caso *VG Bild-Kunst*, asunto C-392/19, pár. 46, ECLI:EU:C:2021:181.
[61] Caso *Nintendo*, asunto C-355/12, págs. 24-27, ECLI:EU:C:2014/25.

un acceso ilícito a la obra o prestación, excluyendo, por tanto, la posibilidad de aplicar la excepción[62]. Además, dado que el artículo 7.2 Directiva 2019/790 no incluye la aplicación del párrafo cuarto del artículo 6.4 Directiva 2001/29, no se podría distinguir, a efectos de la minería, entre las obras y prestaciones puestas a disposición del público con arreglo a un contrato, por un lado, y las obras y prestaciones puestas a disposición del público sin un contrato. Todas entrarían dentro del ámbito de aplicación del límite de minería, puesto que esta distinción entre ambas categorías únicamente se produce cuando se pone en relación el párrafo primero con el párrafo cuarto del artículo 6.4 Directiva 2001/29, algo que aquí no se produce –así parece derivarse de la última frase del considerando 7 Directiva 2019/790–[63]. No obstante, como ya se ha indicado, el artículo 4.3 Directiva 2019/790 permite a los titulares de derechos impedir el uso de obras y prestaciones a efectos de minería, con independencia de que la puesta a disposición se haya producido con arreglo a lo convenido en un contrato o no. Con todo, conviene tener presente que las medidas tecnológicas restringen el acceso o el copiado de los contenidos sin excepción, pues no pueden distinguir cuándo concurre una finalidad de investigación y cuándo no.

Por lo demás, el párrafo tercero del artículo 6.4 Directiva 2001/29 concede protección tanto a las medidas tecnológicas adoptadas voluntariamente por los titulares de derechos, incluyendo las derivadas de acuerdos voluntarios, como las adoptadas en aplicación de medidas consignadas por los Estados miembros. Finalmente, el párrafo quinto de ese artículo 6.4 establece la aplicación de este precepto en el ámbito de las bases de datos.

En todo caso, el Reglamento IA presta especial atención a la protección de los derechos de propiedad intelectual cuando se desarrolla la minería, estableciendo obligaciones para los proveedores de IA, sobre todo la realizada al amparo del artículo 4 Directiva 2019/790. Es una manera de evitar que personas físicas o jurídicas puedan atribuirse derechos de autor sobre productos que han sido enteramente realizados a través de sistemas de IA generativa. Por un

---

[62] Stamatoudi, I. y Torremans, P. (2021). "The Digital Single Market Directive", *EU Copyright Law. A commentary,* Edward Elgar, Cheltenham, p. 690.

[63] Rosati entiende aplicable el artículo 6.4 Directiva 2001/29, a los efectos de la excepción de minería, a las obras y prestaciones puestas a disposición del público a través de servicios a la carta. *Vid*. Rosati, E., *Copyright in the Digital Single Market. Article-by-Article. Commentary to the Provisions of Directive 2019/790*, Oxford University Press, Reino Unido, 2021, p. 91.

lado, están obligados a elaborar y poner a disposición del público un resumen suficientemente detallado de los contenidos utilizados para el entrenamiento del sistema, con el fin de que los titulares de derechos puedan, llegado el caso, ejercitar y hacer cumplir sus derechos [cdo. 107 y art. 53.1.d) Reglamento IA][64]. Y no solamente los titulares de derechos se pueden ver beneficiados con esta previsión, sino también los potenciales compradores o usuarios de productos generados por IA, que les permitirá estar informados sobre el proceso de producción. Señala ese considerando 107 que ese resumen se puede hacer, por ejemplo, a través de una enumeración de los principales conjuntos o recopilaciones que hayan servido para entrenar al sistema y proporcionando una explicación descriptiva sobre las fuentes utilizadas. A estos efectos, la Oficina de IA podría proporcionar un modelo para el resumen. De hecho, dicha Oficina será la encargada de supervisar si se ha cumplido esa obligación, si bien no se exige que proceda a una evaluación obra por obra de los datos de entrenamiento para ver si se han respetado los derechos de propiedad intelectual (cdo. 108 Reglamento IA). Además, se obliga a los proveedores de modelos de IA de uso general a establecer directrices para detectar y cumplir, a través de tecnología, la reserva de derechos expresada conforme al artículo 4.3 Directiva 2019/790 [art. 53.1.c) Reglamento IA][65]. Aunque debe ser bienvenido este principio de transparencia impuesto por el Reglamento IA, debería haberse previsto con carácter previo al uso de la obra o prestación y no únicamente *ex post*. Previo al entrenamiento del sistema, debería haberse establecido una obligación de información a los titulares de derechos de que sus obras se van a utilizar para estos fines, con el objetivo de que pudieran

---

[64] Conforme al artículo 3.3 Reglamento IA, un proveedor es la persona física o jurídica o autoridad, órgano u organismo público que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente.

[65] El artículo 3.63 Reglamento IA define el "modelo de IA de uso general" como aquel *entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado*. El "sistema de IA de uso general" es aquel *basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA* (art. 3.66 Reglamento IA).

decidir, llegado el caso, consentirlo o no, como se ha indicado anteriormente, en consonancia con la jurisprudencia del TJUE ya citada[66].

Por otro lado, el entrenamiento de sistemas de IA mediante contenidos protegidos por la propiedad intelectual podría dar lugar a varias creencias erróneas y llevar a la incorrecta conclusión de que no son necesarias siquiera las excepciones de minería. En primer lugar, uno podría pensar que el objetivo de esos sistemas es acceder a los elementos de una obra que carecen de protección, como la información, las ideas, los hechos, la técnica, el método, los acordes, los ritmos, los tonos o el estilo, entre otros[67]. Sin embargo, el entrenamiento del sistema requiere de la copia de obras y prestaciones, lo que afecta al derecho de reproducción de los titulares, y, en la gran mayoría de casos, no sólo se utilizan esos elementos no protegidos, sino también los elementos característicos de una obra. Y, en segundo lugar, cabría plantearse que, de la misma manera que una persona física se inspira en contenidos preexistentes para realizar sus propias creaciones, los sistemas de IA deberían poder también basarse en ellos. A ello cabe objetar que la inspiración humana nada tiene que ver con la inspiración artificial, pues la primera supone un proceso mucho más profundo e intelectual que la segunda, que es más mecánico y automático. Además, que puedan tener cierta semejanza no significa que deba asegurarse un uso gratuito de las obras en todo caso.

En definitiva, las labores de rastreo de obras y prestaciones y de entrenamiento de sistemas de IA quedan cubiertas por las excepciones de minería de textos y datos[68]. Sin embargo, cuando la minería se lleve a cabo conforme al artículo 4

---

[66] Propone esta obligación de información previa la Asociación Literaria y Artística Internacional (ALAI) en su Resolución de 17 de febrero de 2024, sobre el impacto de la inteligencia artificial en el derecho de autor. Disponible en Internet: https://www.alai.org/en/assets/files/resolutions/240217-impact-ia-copyright_en.pdf (u. v. 05/08/2024).

[67] Considera Nadal Cebrián que no debería haber obstáculo para que los sistemas de IA fueran entrenados con obras protegidas por la propiedad intelectual, siempre que el fin sea extraer ideas, hechos, información o conceptos de tales contenidos, pues lo contrario supondría un freno a la innovación. *Vid*. Nadal Cebrián, M., «¿Pueden los sistemas de inteligencia artificial "aprender"... *op. cit*., p. 64.

[68] Ponen de manifiesto la insuficiencia de las excepciones de minería de la Directiva 2019/790 para cubrir adecuadamente los usos de obras y prestaciones protegidas por parte de sistemas de IA, además del Max Planck en su informe sobre IA (pp. 8-9), Geiger, C., «The Missing Goal-Scorers in the Artificial Intelligence Team: of Big Data, the Fundamental Right to Research and the Failed Text and Data Mining Limitations in the CSDM Directive», en *PIJIP/TLS*, núm. 66, 2021, p. 4.

Directiva 2019/790, los titulares de derechos podrán impedir que se aplique a sus contenidos. Parece, por tanto, que esta posibilidad de reserva es suficiente para proteger a los titulares de derechos. Aunque esto podría ser considerado como un freno al desarrollo de proyectos relacionados con la IA[69], son varias las razones que llevan a aplaudir esta norma: 1) la minería de textos y datos con fines lucrativos y distintos de la investigación científica puede suponer un considerable perjuicio para los titulares de derechos; 2) la ausencia de una compensación a favor de los titulares de derechos que permita rebajar el nivel de perjuicio debe llevar a restringir lo máximo posible su ámbito de aplicación; y 3) los sistemas de IA pueden producir resultados que alcancen un valor muy considerable en el mercado y del que no se van a beneficiar los titulares de derechos sobre las obras y prestaciones que sirvieron para producir dicho resultado, beneficiándose así del esfuerzo ajeno. Debería haberse previsto una compensación a favor de esos titulares, con independencia de la finalidad perseguida con la minería, especialmente cuando se tengan unos objetivos lucrativos[70]. En otros límites sí se ha previsto la compensación, incluso aunque el uso de la obra o prestación sea para fines de investigación. Véase, por ejemplo, la copia privada (art. 31.2 LPI), el *press-clipping* (art. 32.1.II LPI), la ilustración de la enseñanza en determinados casos (art. 32.4 LPI), el uso de trabajos sobre temas de actualidad (art. 33.1 LPI), el préstamo público (art. 37.2 LPI), o la puesta a disposición de obras a través de terminales especializados en bibliotecas y en otras instituciones (art. 37.3 LPI). Sólo así se garantizaría el cumplimiento de la regla de los tres pasos, recogida, entre otras normas, en los artículos 5.5 Directiva 2001/29, 7.2 Directiva

---

[69] Alertan de este peligro Geiger, C., Frosio, G. y Bulayenko, O., "Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/E", *Propiedad intelectual y mercado único digital europeo,* C. Saiz García y R. Evangelio Llorca (dirs.) (2019), Tirant lo Blanch, Valencia, p. 60; Levendowski, A. (2018), "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem", en *Washington Law Review*, núm. 93, p. 589; González Otero, B. (2019), "Las excepciones de minería de textos y datos más allá de los derechos", *Propiedad intelectual y mercado único digital europeo*, C. Saiz García y R. Evangelio Llorca (dirs.), Tirant lo Blanch, Valencia, p. 83; Rosati, E., «Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and its Role in the Development of AI Creativity», en *Asia Pacific Law Review*, núm. 27(2), 2020, p. 23; Nadal Cebrián, M., «¿Pueden los sistemas de inteligencia artificial "aprender"... *op. cit*., p. 48.

[70] La ALAI, en la resolución referida en la nota 63, propone esta compensación, con independencia de que exista o no ánimo de lucro. En el mismo sentido, *vid*. Geiger, C., «The Missing Goal-Scorers in the Artificial Intelligence Team... *op. cit*., p. 9.

2019/790 y 40bis LPI. Cabría también plantearse aplicar un sistema de licencias para la minería con fines comerciales[71].

4. CONCLUSIONES

La IA suscita grandes y complejas cuestiones jurídicas desde el punto de vista de la propiedad intelectual. Sin embargo, la normativa actual puede dar solución a buena parte de ellas. Sea cual sea la opción que se adopte, resulta necesario llegar a conclusiones que permitan la adaptación al paso del tiempo y al desarrollo de las nuevas tecnologías. La atribución de un derecho de autor a la propia máquina sobre los resultados generados por la IA generativa resulta muy problemática. Ello pasaría, desde luego, por modificar el concepto de "autor", conceder personalidad jurídica a seres distintos de los seres humanos, y apostar por el concepto objetivo de "originalidad", despojándolo de toda referencia a la impronta o reflejo de la personalidad del autor. Otra posibilidad sería otorgar el derecho de autor a otros intervinientes en el uso del sistema de IA, como son los programadores o los usuarios. Sin embargo, reconocer este derecho a quienes no han hecho ningún tipo de esfuerzo creativo en ese resultado concreto –recuérdese que nos referimos a IA generativa– casa mal con la necesidad de realizar ese esfuerzo. Por tanto, conviene descartar la concesión de un derecho de autor sobre estos resultados, con independencia de quién sea el adjudicatario del mismo. Piénsese que el objetivo de otorgar este haz de facultades al autor de una obra es recompensarle por su trabajo y esfuerzo, para que se sienta lo suficientemente satisfecho como para continuar creando. En el caso de las máquinas, no tiene sentido atribuirles este derecho porque no hay esfuerzo que compensar.

Otras opciones a contemplar serían la concesión de un derecho conexo o de un derecho *sui generis* a favor de los creadores del *software* necesario para

---

[71] Considera Nadal Cebrián que, de exigirse el pago de una licencia, la innovación quedaría resentida y únicamente las grandes empresas podrían permitirse el desarrollo de estas tecnologías, en detrimento de las pequeñas empresas, lo que podría afectar a la competencia. *Vid*. Nadal Cebrián, M., «¿Pueden los sistemas de inteligencia artificial "aprender"... *op. cit*., p. 71. Sin embargo, este mismo argumento podría servir para cualquier establecimiento abierto al público que quisiera utilizar obras y prestaciones protegidas para, por ejemplo, amenizar a sus clientes. Un establecimiento pequeño no dejará de operar por el hecho de tener que pagar la oportuna licencia a la entidad de gestión correspondiente -no será éste el mayor de sus gastos-. De nuevo, la innovación tecnológica no tiene por qué llevarse a cabo menoscabando los derechos de propiedad intelectual.

su funcionamiento o a favor de los inversores en este tipo de sistemas. Todas ellas presentan ventajas, pero también inconvenientes nada desdeñables. El más importante es que la protección de estos resultados producidos por IA generativa a través de la propiedad intelectual, entrando en competencia directa con las obras creadas por personas físicas, podría desincentivar la creación de obras originales. Además, pondría en peligro la remuneración equitativa y justa a favor de los autores, por la que el legislador europeo viene luchando en los últimos tiempos (*vid*. art. 18 Directiva 2019/790). La promoción de la creación artística y del surgimiento de nuevas vanguardias en cambios artísticos conlleva manejar otro tipo de soluciones. Quizá lo menos problemático sea atribuir un derecho de propiedad ordinario sobre los resultados generados por IA a favor del usuario o de la empresa que ha invertido en el desarrollo del sistema, otorgando, al mismo tiempo, una compensación a los autores cuyas obras son utilizadas para el entrenamiento de sistemas de IA.

En todo caso, es la IA la que debería estar al servicio de la propiedad intelectual y no viceversa. En los últimos años, el legislador ha decantado la balanza a favor de las nuevas tecnologías, sacrificando el derecho de autor y los derechos conexos –no hay nada más que detenerse en la ingente cantidad de excepciones a estos derechos–. La IA es un gran avance en el sector cultural, pero no debe servir de justificación para menoscabar a los autores y a otros contribuyentes en la creación de contenidos protegidos por la propiedad intelectual. Una incorrecta aplicación de excepciones, como la relativa a la minería de textos y datos, puede llevar a una retracción en la innovación y en los incentivos para producir nuevas obras y prestaciones. La locura por las nuevas tecnologías no debe hacernos perder de vista los objetivos y la razón de ser de la propiedad intelectual.

BIBLIOGRAFÍA

Aparicio Vaquero, J. P. (2022). "Derecho de autor y más allá: algoritmos, código de los programas de ordenador y apps", *Revista Pe.i.*, núm. 71.

Bercovitz Rodríguez-Cano, R. (2013). "Artículo 2", *Comentarios al Convenio de Berna*, R. Bercovitz Rodríguez-Cano (coord.), Tecnos, Madrid.

Cámara Águila, P. (2019). "Los conceptos autónomos sobre el objeto de protección del derecho de autor: el concepto de obra y el concepto de originalidad", *La unificación del Derecho de propiedad intelectual en la Unión Europea*, P. Cámara Águila e I. Garrote Fernández-Díez (coords.), Tirant lo Blanch, Valencia.

Carrasco Perera, A. y Del Estal Sastre, R. (2017). "Artículo 5", *Comentarios a la Ley de Propiedad Intelectual*, R. Bercovitz Rodriguez-Cano (coord.), Tecnos, Madrid.

Denicola, R. (2016). "Ex Machina: Copyright Protection for Computer-Generated Works", *Rutgers University Law Review*, núm. 69.

Ducato, R. y Strowel, A., "Limitations To Text and Data Mining and Consumer Empowerment. Making the Case for a Right to «Machine Legibility»", en *CRIDES*, 2018.

Duque Lizarralde, M. (2020). "Las obras creadas por inteligencia artificial, un nuevo reto para la propiedad intelectual", *Revista Pe.i.*, núm. 64, enero-abril.

Geiger, C. (2021). "The Missing Goal-Scorers in the Artificial Intelligence Team: of Big Data, the Fundamental Right to Research and the Failed Text and Data Mining Limitations in the CSDM Directive", en *PIJIP/TLS*, núm. 66.

— (2018) "The exception for Text and Data Mining (TDM) in the proposed Directive on copyright in the digital single market – legal aspects", en *Center for International Intellectual Property Studies*, núm. 2.

Geiger, C., Frosio, G. y Bulayenko, O. (2019). "Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/E", *Propiedad intelectual y mercado único digital europeo*, C. Saiz García y R. Evangelio Llorca (dirs.), Tirant lo Blanch, Valencia.

Ginsburg, J. C. y Budiardjo, A. L. (2019). "Authors and Machines", *Berkeley Technology Law Journal*, Vol. 34, núm. 2.

Ginsburg, J. C. (2018). "People Not Machines: Authorship and What It Means in the Berne Convention", *International Review of Intellectual Property and Competition Law*, Vol. 49.

Glesser, D. (2001). "Copyright in Computer-Generated Works: Whom, If Anyone, Do We Reward?", *Duke Law and Technological Review*, Vol. 1.

González Otero, B. (2019). "Las excepciones de minería de textos y datos más allá de los derechos", *Propiedad intelectual y mercado único digital europeo*, C. Saiz García y R. Evangelio Llorca (dirs.), Tirant lo Blanch, Valencia.

Hilty, R. y Richter, H. (2019). "Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European

Copyright Rules Part B Exceptions and Limitations (Art. 3 – Text and Data Mining)", en *Max Planck Institute for Innovation and Competition*, núm. 17(2).

Lambert, P. (2017). "Computer Generated Works and Copyright: Selfies, Traps, Robots, AI and Machine Learning", *European Intellectual Property Review*, Vol. 1, núm. 31.

Lee, K., Cooper, A. F. y Grimmelmann, J. (2024). "Talkin'Bout AI Generation: Copyright and the Generative-AI Supply Chain", *Journal of the Copyright Society*.

Levendowski, A. (2018). "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem", *Washington Law Review*, núm. 93.

Margoni, T. y Kretschmer, M. (2021). "A deeper look into the EU Text and Data Mining exceptions: Harmonisations, data ownership, and the future of technology", en *CREATe*, núm. 7.

Minero Alejandre, G. (2023). "Estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de protección de las bases de datos: de los errores no reconocidos a las modificaciones indirectas de la Directiva. Identificación de las imprecisiones de la futura Data Act a la luz de la doctrina jurisprudencial", *Revista Pe.i.*, núm. 72.

— (2023). "Inteligencia artificial y propiedad intelectual", en Derecho, nuevas tecnologías e inteligencia artificial, C. Alonso Salgado, A. Valiño Ces y A. Rodríguez Álvarez (dirs.), Dykinson, Madrid.

— (2024). "Los dos límites (el obligatorio y el optativo) de minería de textos y datos", en *La transposición en España de la Directiva sobre derechos de autor y mercado único digital*, dirs. P. Cámara Águila e I. Garrote Fernández-Díez, Tirant, Valencia.

Morán, M. (2018). "Creadores en riesgo de extinción", *V Certamen de artículos jurídicos sobre Derecho del Entretenimiento*, Premios DENAE.

Nadal Cebrián, M. (2021). "¿Pueden los sistemas de inteligencia artificial "aprender" utilizando obras protegidas por derechos de propiedad intelectual sin la autorización de sus titulares? Los retos del *machine learning* en perspectiva comparada: UE, EE. UU. y Japón", en *Revista Pe.i.*, núm. 68.

Navas Navarro, S. (2018). "Obras generadas por algoritmos, en torno a su posible protección jurídica", *Revista de Derecho Civil*, núm. 2.

Ramalho, A. (2018). "Machines that create and how EU copyright law views them", *Kluwer Copyright Blog*.

— (2017). "Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems", *Forthcoming in the Journal of Internet Law*.

Rosati, E. (2020). "Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and its Role in the Development of AI Creativity", en *Asia Pacific Law Review*, núm. 27(2).

— (2021). *Copyright in the Digital Single Market. Article-by-Article. Commentary to the Provisions of Directive 2019/790*, Oxford University Press, Reino Unido.

Saiz García, C. (2019). "Las obras creadas por sistemas de inteligencia artificial y su protección", *InDret*, núm. 1.

Sanjuán Rodríguez, N. (2019). "Inteligencia artificial y propiedad intelectual", *Actualidad Jurídica Uría Menéndez*, núm. 52.

Senfleben, M. (2023). "Generative AI and Author Remuneration", *International Review of Intellectual Property and Competition*, Vol. 54.

Stamatoudi, I. y Torremans, P. (2021). "The Digital Single Market Directive", *EU Copyright Law. A commentary,* Edward Elgar, Cheltenham.

Tessier, C. (2017). "Robots Autonomy: Some Technical Challenges", *Autonomy and artificial intelligence: A Threat or Savior?*, W.F. Lawless, R. Mittu, D. Sofge y S. Russell (eds.), Springer, Reino Unido.

Yanisky-Ravidm, S. y Velez Herández, L. (2018). "Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model", *Minnesota Journal of Law, Science and Technology*, Vol. 19.

Yu, R. (2017). "The Machine Author: What Level of Copyright Protection is appropriate for Fully Independent Computer Generated Works?", *University of Pensylvania Law Review*, núm. 165.

Capítulo 6
DERECHO DE DAÑOS, ROBÓTICA E INTELIGENCIA ARTIFICIAL[1]

María José Santos Morón
Catedrática de Derecho Civil
Universidad Carlos III de Madrid
https://orcid.org/0000-0001-6486-4869

1. INTRODUCCIÓN

El presente trabajo pretende esbozar un panorama sobre la regulación que se pretende implementar en la Unión Europea en lo que concierne a la reparación de los daños provocados por robots y sistemas de inteligencia artificial[2].

En el momento actual cuando hablamos de robots nos referimos habitualmente a objetos tangibles (máquinas) que pueden interactuar con el entorno y desarrollar tareas similares a las realizadas por ser humano. Los robots suelen llevan incorporados sistemas de inteligencia artificial que les dotan de distintos grados de autonomía[3]. Mientras que, por ejemplo, los robots quirúrgicos

---

[1] Este trabajo se ha realizado en el marco del Proyecto de Investigación PID2020-115352GB-I00, financiado por AEI/10.13039/501100011033.

[2] Definir qué se entiende por sistema de inteligencia artificial no es fácil. El Reglamento de Inteligencia Artificial [COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)] cuyo texto definitivo, en el momento de escribir estas líneas, está pendiente de publicación, pretende ofrecer una noción amplia y flexible. En la última versión disponible (texto aprobado el 13-3-2024, TA-9-2024-0138, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html) el art. 3,1 lo define del siguiente modo : "sistema de IA: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su implementación y que, para objetivos explícitos o implícitos infiere, a partir de los datos de entrada que recibe, cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que puedan influir en entornos físicos o entornos físicos o virtuales".

[3] Adviértase que también es posible que se califique como "robot" a una máquina que realiza ciertas tareas de forma repetitiva (v. gr. mover cajas), aunque no esté provista de un sistema de

precisan en su mayoría de la intervención de algún ser humano (v. gr. el conocido Da Vinci), los robots móviles autónomos, como los de limpieza o los usados para almacenamiento, pueden decidir por sí mismos la acción a realizar en función de la información que han percibido. Ahora bien, la inteligencia artificial puede presentarse igualmente de manera independiente como sucede con los sistemas tipo software (v. gr. software para la selección y contratación de personal, o para manipular imágenes y vídeos que pueden parecer auténticos). Así cuando hablamos de "inteligencia artificial" hemos de considerar incluidos tanto los productos que llevan integrados sistemas de inteligencia artificial, como son los robots, drones y/o vehículos autónomos y en general los denominados "smart products" (v. gr. reloj inteligente), como los sistemas de inteligencia artificial que podríamos calificar como "digitales" o "incorpóreos" *(standalone software*). Partiendo de esta premisa a partir de ahora utilizaré el término "sistema de inteligencia artificial" o "sistema inteligente" para englobar ambos supuestos.

El desarrollo de estas tecnologías ha suscitado muchas inquietudes en lo que respecta a la reparación de los daños que puedan producirse, pues, si bien no está claro que el uso de robots y sistemas inteligentes suponga necesariamente un incremento del riesgo de daños[4], lo que sí parece evidente es que los sistemas tradicionales de responsabilidad civil, basados en la culpa del agente, no se adaptan a las particularidades de estas tecnologías. Ello puede dificultar la prueba de algunos de los elementos de la responsabilidad como la culpa o la relación causal, haciendo inviable la reparación de los daños sufridos por el perjudicado.

¿Cuáles son estas particularidades? Suele decirse que las tecnologías emergentes de carácter digital se caracterizan por su *complejidad y opacidad.* La c*omplejidad* se manifiesta tanto en el diseño como en el funcionamiento de los sistemas de inteligencia artificial. En su creación y diseño intervienen muchos participantes: desarrollador de software, diseñadores de algoritmos, suministradores de datos, fabricantes de sensores, etc. Además, estos sistemas suelen estar compuestos por multiplicidad de elementos que en muchos casos interactúan entre ellos. Esta

---

inteligencia artificial. Aquí nos vamos a referir a los robots "inteligentes". Sobre el concepto de robot, vid. Ataz López, J., "Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial", Working Paper 4/2020, pp. 19 y ss.; Atienza Navarro, M. L. (2022), *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier, pp. 47 y ss.

[4] Cabría pensar, incluso, que reduce los riesgos respecto a la realización de la misma actividad por un ser humano. Atienza Navarro, M.L, *ob. cit*., p. 25.

complejidad genera su vez un elevado grado de *opacidad* a la hora de entender cómo estos sistemas funcionan y se comportan en la práctica, Si el sistema funciona incorrectamente y provoca un daño, es complicado saber a qué obedece su mal funcionamiento, es decir, es difícil determinar cuál ha sido la causa concreta del daño. Ello trae consigo que sea difícil determinar a qué sujeto, del conjunto de los que han intervenido en su diseño y producción, debe atribuirse el daño y, por consiguiente, el deber de indemnizarlo. Esto se manifiesta, particularmente, en los casos en que el sistema inteligente aprende por sí mismo, en cuyo caso es muy difícil explicar cómo ha tomado sus decisiones. Otra característica problemática es *el carácter abierto de estas tecnologías*. Los ecosistemas tecnológicos no están completos cuando se ponen en circulación, necesitan interactuar con otros sistemas o fuentes de datos para funcionar, y además están sujetos a continuas actualizaciones y mejoras. Ello afecta a la determinación de la relación causal y un problema adicional viene dado por su *vulnerabilidad*, determinada, por un lado, por la dependencia de los datos que le son suministrados, que si son insuficientes o inadecuados pueden comprometer su funcionamiento, y por otro por la posibilidad de ciberataques. Por último, hay sistemas de inteligencia artificial que tienen capacidad de aprendizaje y pueden desarrollar un cierto grado de *autonomía en la toma de decisiones* lo que incrementa su imprevisibilidad y hace surgir nuevamente la interrogante de quién debe responder cuando el daño ha sido causado por una decisión autónoma de un sistema de inteligencia artificial[5].

Todo esto ha propiciado que en el seno de la UE se hayan elaborado numerosos textos y documentos sobre esta cuestión[6]. Sin embargo, las instituciones europeas han abandonado la postura inicialmente mantenida en la Propuesta de Reglamento relativo a la responsabilidad civil por el funcionamiento de sistemas de inteligencia artificial (2020/2014 (INL) –Resolución de 20 de octubre de 2020– que pretendía articular un régimen específico de responsabilidad para los

---

[5] *Vid.* European Law Institute (2022), "Response of the European Law Institute to the European Commission's Public Consultation on civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence", pp. 24 y ss.; Expert Group on Liability and New Technologies (2019), "Liability for Artificial Intelligence and Other Emerging Digital Technologies", pp. 32-33.

[6] *Vid.* Platero Alcón, A. (2021). "Breves notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix", *Ius et Scientia,* Vol, 7, núm. 1, pp. 138-140; Atienza Navarro, M.L., *Daños causados por inteligencia artificial,* cit., pp. 26 y ss.

daños producidos por sistemas de inteligencia artificial. Conforme a esta Propuesta podían ser declarados responsables de los daños causados por tales sistemas tanto el denominado "operador inicial" como el denominado "operador final". El primero era equiparable al fabricante (aunque también podía considerarse como tal al diseñador o al prestador de servicios en línea), y el segundo al usuario del sistema de inteligencia artificial[7]. Uno y otro respondían objetivamente en caso de sistemas de IA de alto riesgo, previéndose un sistema de responsabilidad por culpa en caso contrario. En la actualidad se ha llegado a la conclusión de que los daños causados por sistemas de inteligencia artificial deben repararse conforme a la normativa europea de responsabilidad por productos defectuosos –que ha de ser adaptada a las peculiaridades de las tecnologías de carácter digital– y, cuando no proceda su aplicación, acudiendo a los sistemas internos de responsabilidad de cada Estado miembro, que por lo general están basados en la culpa del agente. En consonancia con ello se han publicado dos Propuestas de Directivas, una dirigida a sustituir a la actual Directiva de daños causados por productos defectuosos (Directiva 85/374/CEE) por otra más adecuada a las nuevas tecnologías (en adelante, Propuesta de Directiva sobre Productos Defectuosos[8]) y otra que pretende flexibilizar la prueba de los elementos de la responsabilidad por culpa, cuando resulte aplicable este régimen de responsabilidad (en adelante, Propuesta de Directiva sobre Responsabilidad IA[9]).

---

[7] El "operador inicial" era conceptuado como el sujeto que define las características de la tecnología, proporciona datos y presta el servicio de apoyo esencial para su funcionamiento. El "operador final se definía como "toda persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento" (art. 3, letras d, e y f). Sobre ello, Navas Navarro, S. (2022). *Daños ocasionados por sistemas de inteligencia artificial. Especial atención futura regulación,* Comares, Granada, pp. 50 y ss.; Atienza Navarro, M. L., *Daños causados por inteligencia artificial,* cit., pp. 292 y ss.

[8] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos, COM (2022) 495 FINAL. Las instituciones europeas (Consejo, Parlamento y Comisión) alcanzaron un acuerdo sobre esta Propuesta en diciembre de 2023. Como resultado, el 24 de enero 2024 el "Permanent Representatives Committee" envió al Parlamento un texto de compromiso que es la última versión disponible de la Propuesta de Directiva en el momento de redacción de este trabajo y que va a ser tenida en cuenta junto a la Propuesta inicial.

[9] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), COM (2022) 496 FINAL.

Esto implica que la responsabilidad por los daños causados por sistemas de inteligencia artificial tiende a concentrarse en el fabricante del producto, que es el sujeto fundamentalmente responsable conforme a la normativa de productos defectuosos, y que responde, además, *objetivamente* de los daños causados. El usuario de un robot o sistema de IA, por el contrario, no parece que vaya a responder por el mero hecho de hacer uso del mismo y beneficiarse de su funcionamiento. Salvo que la normativa interna que resulte aplicable disponga otra cosa, solo responderá si ha actuado *negligentemente*.

Las dos propuestas de Directiva mencionadas forman parte de un "paquete" mediante el cual las instituciones europeas pretenden adaptar las normas de responsabilidad actuales a la era digital. Junto a ellas hay que tener en cuenta el Reglamento sobre Inteligencia Artificial (*Artificial Inteligence Act*)[10] –cuyo texto definitivo está pendiente de publicación[11]– ya que algunos de los conceptos empleados en la Propuesta de Directiva sobre Responsabilidad IA se corresponden con definiciones incorporadas en dicho Reglamento (cfr. Cdo. 15 Propuesta de Directiva sobre Responsabilidad IA).

2. ¿RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS O RESPONSABILIDAD POR CULPA?

De acuerdo con lo indicado, para obtener la reparación de los daños causados por sistemas de inteligencia artificial parece que ha de acudirse, en primer término, a la normativa de productos defectuosos. Cuando esta no sea aplicable o no permita resarcir el daño de que se trate habrá que recurrir a las reglas generales de responsabilidad de los ordenamientos internos. En tal caso, y siempre que resulte de aplicación un régimen de responsabilidad *extracontractual* basado en la culpa, puede entrar en juego la Propuesta de Directiva sobre Responsabilidad

---

[10] Este texto pretende garantizar que los sistemas de IA que se desarrollen y utilicen en la UE cumplan ciertos requisitos de seguridad y se ajusten a los valores vigentes en la sociedad europea, pero no regula la responsabilidad derivada de los daños que puedan causar. Puede verse una explicación del contenido y fines de la Propuesta de Reglamento IA, en Martín Casals, M., "Las propuestas de la UE para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *Indret* 2-2023, pp. 60 y ss.

[11] La última versión disponible en el momento de redacción de este trabajo es el texto aprobado el 13-3-2024, TA-9-2024-0138, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html.

IA, con el fin de facilitar al perjudicado la prueba de la culpa y, fundamentalmente, la de la relación causal.

Conviene, por tanto, determinar en qué casos los daños causados por sistemas de inteligencia artificial podrán ser reparados conforme a la Propuesta de Directiva de Productos defectuosos. No obstante, dado que el régimen que incorpora es muy similar al contemplado en la actualmente vigente, es aconsejable exponerlo brevemente.

La actual Directiva 85/374 CEE –cuyo contenido está incorporado en el Derecho español en los arts. 128 y ss. del TRLC– establece un régimen de responsabilidad objetiva en el que el sujeto fundamentalmente responsable es el fabricante del producto causante del daño, al cual se equipara el importador cuando el producto ha sido fabricado fuera de la UE. El sujeto protegido es cualquiera que sufra un daño como consecuencia de un producto defectuoso (sea consumidor, empresario, trabajador, etc.), si bien los daños resarcibles varían según la condición del perjudicado. El elemento fundamental para desencadenar la responsabilidad es el carácter "defectuoso" del producto de que se trate, que viene determinado por su falta de seguridad. Es decir, un producto es defectuoso si no ofrece la seguridad que cabe legítimamente esperar (por ejemplo, un supuesto paradigmático de producto defectuoso es el de las botellas –de cerveza, gaseosa, etc.– que estallan sin ser manipuladas, cfr. STS 2-11-2023, RJ 2023/5731; 21-10-2003, RJ 2003/2133; 23-6-1993, RJ 1993/5380), debiendo tenerse en cuenta que los defectos de "calidad" (v. gr. ausencia de cualidades o ineptitud para el fin presupuesto al contratar) se rigen por las reglas de la responsabilidad contractual. Si el perjudicado prueba el daño, el defecto y la relación de causalidad entre ambos, el fabricante (o en su caso el importador) será responsable del mismo a menos que concurra alguna de las causas de exoneración previstas en la Directiva 85/374 CEE.

Para que este régimen de responsabilidad pueda ser aplicado satisfactoriamente a los daños causados por sistemas de inteligencia artificial es necesario realizar algunas modificaciones que se expondrán con posterioridad (v. gr. ampliación de la noción de producto, que ahora está limitada a los bienes tangibles; modificación de las causas de exoneración, etc.).

Sin embargo, pese a las modificaciones proyectadas, no todos los daños causados por robots y sistemas inteligentes podrán ser reparados conforme a la normativa de productos defectuosos. Para que sea así deben darse una serie de requisitos:

a) Que el sistema de inteligencia artificial que ha causado el daño pueda ser considerado como un "producto"

Esta circunstancia no es particularmente problemática porque la Propuesta de Directiva sobre productos defectuosos, como se verá con más detenimiento con posterioridad, amplía el concepto de producto para que queden incluidos los sistemas de inteligencia artificial, tanto si están incorporados a un objeto tangible (robots y demás productos inteligentes) –en cuyo caso son considerados como "componentes"– como, en particular, si se presentan de manera independiente. En concreto, dispone que son también productos "los archivos de fabricación digital" y los "programas informáticos" (art. 4.1), que, según el Cdo. 12, abarcan, por ejemplo, los sistemas operativos, los programas de ordenador, las aplicaciones o los sistemas de inteligencia artificial. Este mismo considerando aclara que el desarrollador o productor de un programa informático deberá ser tratado como un fabricante.

En la versión inicial de la Propuesta, dicho Considerando indicaba que los programas de ordenador tienen la consideración de producto "independientemente de su modo de suministro o uso" esto es, con independencia de que estén almacenados en un dispositivo o se acceda a ellos a través de la nube. Aunque de ahí cabía deducir que el denominado "software como servicio", (SaaS), que se distribuye por medio de licencias basadas generalmente en su suscripción, podía tener la consideración de producto[12], en la última versión disponible de la Propuesta, de 24-1-2024, el repetido Cdo. 12 confirma esta interpretación.

De acuerdo con ello parece que las distintas modalidades de IA quedarían cubiertas por el régimen de responsabilidad previsto en la Propuesta de Directiva.

b) Que, una vez catalogado como "producto" el sistema de inteligencia artificial en cuestión, pueda ser calificado a su vez como "defectuoso"

El carácter defectuoso, como ya se ha indicado, supone que el producto no cumple la *seguridad* que del mismo cabe esperar. Las deficiencias que afectan a la calidad del producto deberán resolverse por lo general conforme a las

---

[12] Así lo entendía Martín Casals, M., ob. cit., p. 79, si bien otros autores consideraban dudosa la cuestión (Spindler, G. (2023). "Different approaches for liability of Artificial Inteligence-Pros and Cons", en *Liability for AI,* Lohsse, Schulze y Staudenmayer (eds.), Nomos, p. 44).

reglas de la responsabilidad contractual. Esto, en el ámbito de los sistemas IA, puede provocar algunos problemas de delimitación. Por ejemplo, si un sistema IA para evaluar la calificación crediticia o la solvencia funciona incorrectamente e impide acceder indebidamente al crédito a ciertos sujetos ¿nos encontramos ante un defecto de "seguridad" o ante un mero mal funcionamiento ligado a la deficiente calidad del producto? La respuesta en este caso es indiferente porque el daño derivado de la imposibilidad de acceder al crédito (daño económico puro), como luego se verá, no está cubierto por la normativa de productos defectuosos. Sin embargo, puede ser relevante en otros casos, ya que la imposibilidad para calificar el producto como "defectuoso" determinará que la víctima solo pueda exigir indemnización con base en las reglas generales de responsabilidad extracontractual o, en su caso, contractual.

Con independencia de cómo se redacte finalmente el art. 6,1 de la futura Directiva[13], para determinar el estándar de seguridad exigible a un producto se suele atender a las expectativas del ciudadano medio[14] y a la relación riesgo-beneficio del producto, de especial importancia, por ejemplo en el caso de medicamentos y productos sanitarios[15]. Habrá casos en que será relativamente sencillo concluir que el producto no alcanza la seguridad esperada. Por ejemplo, si un robot corta-césped no es capaz de detectar la presencia de un humano y lo atropella, o si un vehículo autónomo hace caso omiso de un semáforo en rojo y provoca una colisión, parece claro que uno y otro deberán considerarse "defectuosos". En otros casos, sin embargo, puede ser más difícil determinar el estándar de seguridad exigible, y la cuestión se complica cuando se trata de sistemas inteligentes que tienen capacidad de aprendizaje y pueden decidir autónomamente. ¿Qué pasaría, por ejemplo, si un vehículo autónomo, para evitar atropellar

---

[13] El art. 6.1 de la Propuesta de Directiva dispone, en su redacción inicial, que "un producto se considerará defectuoso cuando no ofrece la seguridad *que el público en general tiene derecho a esperar*". El Parlamento introdujo una enmienda dirigida a sustituir esta frase por otra relativa a la seguridad que *un ciudadano medio* pueda esperar (Enmienda núm. 70; puede consultarse en https://www.europarl.europa.eu/doceo/document/A-9-2023-0291_EN.html#_section6). En la versión de compromiso de 24-1-2024 (ver nota 7) se alude simplemente a la seguridad que "*una persona* pueda esperar".

[14] Como observa Martín Casals, M., ob. cit., p. 83, generalmente se entiende que el test de las legítimas expectativas de seguridad es objetivo, y no subjetivo.

[15] Santos Morón, M. J. (2022). "La responsabilidad por daños causados por productos defectuosos", *Derecho de consumo. Visión normativa y jurisprudencial actual,* Tecnos, pp. 138-140.

a un peatón que aparece repentinamente en la calzada, provoca una colisión en cadena? ¿Debería ser considerado defectuoso? Cuando existen estándares técnicos que presuponen un determinado nivel de seguridad (v. gr. condiciones para la activación del airbag de un coche), es claro que, si el producto se aparta del mismo, puede considerarse defectuoso. No obstante, es posible que no siempre sea así. La doctrina sugiere que el estándar de seguridad exigible al funcionamiento de un robot o sistema inteligente debe ser al menos igual al de un ser humano en el desempeño de la misma actividad, de modo que si el sistema de IA genera riesgos superiores debería ser considerado defectuoso[16]. Por otra parte, también cabría comparar el funcionamiento del producto dañoso en cuestión con otros objetos o sistemas inteligentes similares, de modo que, si estos hubiesen evitado el daño, aquél deberá ser considerado defectuoso.

Las circunstancias establecidas en el art. 6 de la Directiva proyectada, así como las presunciones de defecto que establece su art. 9, pueden ser de utilidad para valorar el carácter defectuoso del producto, como se verá más adelante (infra ep.3). Pero si el perjudicado no puede probar la defectuosidad del producto causante del daño, no habrá lugar a imponer responsabilidad objetiva a su fabricante y, si bien en teoría podría acudir a las reglas generales de responsabilidad, se encontrará con dificultades, posiblemente mayores, para demostrar su culpa o negligencia (o la de otros sujetos que hayan podido intervenir en la causación del daño).

c) Que los daños sufridos por el perjudicado –que debe ser persona física– sean daños personales o daños materiales causados en bienes no utilizados exclusivamente con fines profesionales

El texto original de la Propuesta de Directiva, de modo similar a la Directiva actual, excluye el resarcimiento de los daños morales, permite la reparación de los daños personales a cualquier perjudicado, y, por lo que respecta a los daños materiales, contempla su indemnización solo si afectan a cosas distintas del propio producto defectuoso y siempre que el bien en cuestión no sea usado

---

[16] Martín Casals, M., ob. cit., p. 84; Atienza Navarro, M. L. (2023). "¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)", *InDret,* núm. 2, p. 17.

exclusivamente con fines profesionales (art. 4.6)[17]. La Propuesta ha incorporado también dentro del concepto de daño resarcible "la pérdida o corrupción de datos" pero, nuevamente, siempre que no se utilicen exclusivamente con fines profesionales. Quedan fuera, por tanto, los daños provocados a bienes de uso profesional o industrial, la pérdida o corrupción de datos empleados en actividades profesionales[18], así como los daños patrimoniales de otro tipo (v. gr. imposibilidad de acceder a un crédito a consecuencia del incorrecto funcionamiento de un programa automático de *credit scoring*). Por lo que respecta a los daños morales, hay que advertir que el Texto de compromiso de 24 enero 2024 ha modificado la versión original de la Propuesta, incorporando un nuevo art. 5a relativo al daño resarcible, que permite reparar el daño moral, pero solo si es consecuencia de daños corporales y materiales cubiertos por la futura Directiva, y en la medida que sea indemnizable conforme al Derecho nacional. Por otra parte, dado que el sujeto protegido por la futura Directiva ha de ser persona física (art. 1), los daños sufridos por personas jurídicas no pueden ser reparados en ningún caso con base en la normativa de productos defectuosos.

Lo dicho supone que, si el daño ocasionado por el perjudicado es un *daño moral* derivado, por ejemplo, de la lesión de un derecho fundamental (v. gr. igualdad y no discriminación), cosa que puede suceder, por ejemplo, si se utiliza un software para la contratación de empleados que funciona indebidamente o contiene determinado sesgo, o si se utiliza un sistema de inteligencia artificial para determinar quién es merecedor de asilo político que genera un resultado erróneo, no podrá acudirse al régimen previsto en la Directiva de productos defectuosos. La reparación de tales daños solo será posible al amparo de las reglas generales de responsabilidad contractual o, en su caso, extracontractual.

Lo mismo ocurrirá si un empresario o profesional emplea en su actividad un sistema de inteligencia artificial que le provoca *daños patrimoniales*. Pensemos,

---

[17] La actual Directiva solo permite la reparación de los daños materiales causados en cosas "que normalmente se destinan al uso o consumo privado" y, además, han sido utilizados para uso o consumo privado (art. 9). La Propuesta excluye solo los daños provocados en bienes utilizados *exclusivamente* con fines profesionales, por lo que admite la posibilidad de indemnizar los daños que afectan a bienes de uso mixto.

[18] La exclusión de los daños causados a bienes de uso profesional o industrial es criticable, dada la importancia que tienen en la práctica. En este sentido, Atienza Navarro, M. L., "¿Una nueva responsabilidad por productos defectuosos?", cit., p. 39; Spindler, G., ob cit., p. 88.

por ejemplo, en el supuesto planteado en EE. UU., en el que algunos abogados han sido sancionados por haber aportado en un juicio precedentes falsos obtenidos mediante el uso del ChatGTP[19]. Aunque quizás no sea fácil que en España se dé una situación similar, es claro que la sanción económica impuesta como consecuencia del defectuoso funcionamiento del sistema de IA no sería un "daño" susceptible de ser reparado conforme a la Directiva de productos defectuosos. Tampoco lo sería, por poner otro ejemplo, el perjuicio patrimonial sufrido por una empresa que es condenada a indemnizar a un empleado por despido improcedente debido al defectuoso funcionamiento del sistema de IA utilizado para determinar el rendimiento o la correcta ejecución de tareas por parte de los trabajadores.

En estos supuestos, nuevamente, el perjudicado debería acudir a las reglas generales de responsabilidad contractual (si de dirige contra el vendedor o suministrador del sistema de inteligencia artificial causante del daño[20]), o, en su caso, extracontractual (si pretende dirigirse, por ejemplo, contra el fabricante del mismo).

A estas reglas deberá remitirse también el profesional o empresario que sufre la pérdida o destrucción de datos o contenido digital como consecuencia de una aplicación o un programa informático empleados para realizar cualquier tarea. Pese a que tal circunstancia puede ser catastrófica y afectar el funcionamiento general de una empresa[21], lo cierto es que la Propuesta de Directiva, aunque amplía la noción de "daño" para incluir los daños materiales derivados de la pérdida o corrupción de datos, lo limita al supuesto en que estos no sean usados exclusivamente con fines profesionales (art. 4,6,c Propuesta). Ello obliga, nuevamente, al empresario o profesional a obtener la reparación del daño acudiendo a las reglas generales de responsabilidad.

En los supuestos enunciados, y si se demanda al eventual responsable conforme al régimen de responsabilidad por *culpa extracontractual,* podrían entrar

---

[19] Se hace eco de ello el *Diario La Ley* (sección Ciberderecho), de 23-6-2023. Se informa de un suceso similar en el número de la misma revista de 8-1-2024.

[20] En los supuestos ejemplificados cabe pensar que se está, más bien, ante defectos de "calidad", derivados de la falta de aptitud del software o sistema IA empleados para cumplir correctamente la finalidad que se les presupone. En tal caso los daños derivados de ese inadecuado funcionamiento podrían ser reparados de acuerdo con las reglas de la responsabilidad contractual.

[21] Martín Casals, M., ob. cit., p. 87. Cuestiona, asimismo, que se incluya como daño solo la pérdida de datos de uso no profesional; Spindler, G., ob. cit., p. 49.

en juego las reglas de flexibilización probatoria previstas en la Propuesta de Directiva sobre responsabilidad por IA. El problema es que esta propuesta está pensada para el supuesto en que el sujeto demandado es, bien el proveedor del sistema de IA (sujeto equiparable a su "fabricante"), bien el usuario. Ello, como se verá con posterioridad, deja fuera todos aquellos supuestos en que el responsable del inadecuado funcionamiento del sistema de IA es otro sujeto.

d) También será necesario, por último, que no hayan transcurrido más de 10 años desde que el producto causante del daño fue introducido en el mercado o puesto en servicio

Al igual que en la Directiva actualmente vigente, la posibilidad de invocar el régimen de responsabilidad por productos defectuosos está limitada en el tiempo. Según la última versión de la Propuesta de Directiva (24-1-2024) ello sólo es posible en el plazo de 10 años desde la fecha de introducción del producto en el mercado o puesta en servicio a menos que la víctima haya ejercitado la acción con anterioridad (art. 14 a.1). No obstante, en caso de daños personales latentes, el plazo aumenta a 25 años salvo que se haya ejercitado previamente la acción (art. 14 a. 2).

3. LA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS [28 DE SEPTIEMBRE DE 2022, COM (2022) 495]

Como ya se ha mencionado, esta propuesta pretende adaptar la regulación actualmente existente a los daños causados por sistemas de inteligencia artificial y a los productos que llevan integrados sistemas de inteligencia artificial (Smart products –robots, drones, vehículos autónomos, etc.–) con el fin de garantizar que, cuando un sistema de inteligencia artificial sea defectuoso y cause daños el perjudicado, este pueda obtener indemnización del fabricante o desarrollador del sistema IA o del fabricante que lo ha integrado en otros productos (punto 1.2 Memorandum).

La necesidad de modificar la Directiva actual viene dada por diversos factores. El primero de ellos es que los bienes o elementos digitales –v.gr. un software o programa informático–, no encajan en la noción de "producto" utilizada por esta norma, pensada para bienes muebles tangibles, por lo que si causan daños no es posible repararlos acudiendo a este régimen de responsabilidad. Es decir,

cuando el sistema de IA es de tipo software y no está incorporado a un bien corporal, su "fabricante" o desarrollador no podría responder conforme a la actual Directiva de productos defectuosos. Si el sistema de IA estuviese integrado en un objeto físico y este causara un daño, el fabricante del producto final (v. gr. el robot) sí podría ser declarado responsable con base en la Directiva. Pero no podría reclamarse, nuevamente, responsabilidad al fabricante del componente (v. gr. software) que ha provocado el mal funcionamiento del robot[22]. Por otra parte, conforme al régimen actualmente vigente, el fabricante solo responde de los defectos que ya existieran en el producto en el momento de su "puesta en circulación" (art. 7.b Directiva 85/374). Ocurre sin embargo que los productos digitales están sometidos a permanentes mejoras y actualizaciones –por lo general introducidas a instancias del fabricante– que pueden provocar su mal funcionamiento. El problema es que, al no ser el defecto "originario", aquel no podría ser considerado responsable. Resulta por eso necesario restar importancia al momento de la puesta en circulación del producto y modificar las actuales causas de exoneración de responsabilidad del fabricante o productor. Al margen de ello, las particularidades de las tecnologías digitales, a las que se aludió con anterioridad, pueden provocar que el perjudicado tenga dificultades para probar el carácter defectuoso del producto y la relación de causalidad entre este y los daños causados.

De acuerdo con lo indicado, la Propuesta de Directiva Productos Defectuosos incorpora una serie de novedades que se exponen a continuación.

1) Se amplía la noción de producto y se incorpora la de "componente"

El art. 4,1 de la Propuesta de Directiva, incluye ahora expresamente en el concepto de producto *los archivos de fabricación digital y los programas informáticos*[23].

---

[22] Conforme a la Directiva 85/374/CEE, en los casos en que el daño ha sido causado por una materia prima o un elemento integrante del producto final, el perjudicado puede demandar tanto al fabricante del producto final como al del elemento o componente causante del daño, que responden solidariamente (arts. 3 y 5). Esto no sería posible si ese componente fuese un sistema de inteligencia artificial.

[23] Queda excluido, no obstante, además de código fuente de los programas informáticos, el software de código abierto, que se desarrolla de manera compartida y es libremente accesible, salvo que se suministre en el curso de una actividad comercial (Cdo. 13). En el Texto de compromiso de 24-1-2024 se ha añadido un nuevo considerando, el 13 a), que indica que, si un fabricante incorpora a un producto, dentro de su actividad comercial, un software de código abierto,

Los archivos de fabricación digital son aquellos que permiten fabricar un objeto tangible mediante máquinas tales como las impresoras 3D (Cdo. 14). Son, como indica el art. 4.2 una "versión digital o una plantilla digital de un bien mueble". De este modo, si el objeto creado mediante impresión 3D causa daños a una persona debido al carácter defectuoso del archivo de fabricación digital (pensemos por ejemplo que un sujeto fabrica mediante impresión 3D un casco para la moto que resulta ser inseguro por romperse con un leve impacto) el perjudicado podría demandar al creador o "fabricante" del archivo conforme a este régimen de responsabilidad objetiva.

La consideración del software como producto permite igualmente aplicar dicho régimen a los daños causados por sistemas de inteligencia artificial que se presentan de manera autónoma, es decir, aunque no estén incorporados a otros productos, y, como ya se indicó, con independencia de cómo se acceda a ellos (v. gr. a través de la nube). Por tanto, el perjudicado podrá demandar a su desarrollador o productor, que son equiparados al fabricante (Cdo. 12).

Ahora bien, en el supuesto en que el sistema IA esté integrado en otro bien, tendrá la consideración de "componente" del mismo. Así, el art. 4.3 de la Propuesta dispone que tiene la consideración de componente, "cualquier artículo, *tangible o intangible*, materia prima o cualquier servicio conexo que esté integrado en un producto o interconectado con él"[24]. Esta regla va a permitir que la persona que sufre daños causados, por ejemplo por un exoesqueleto robótico que no funciona correctamente, pueda exigir responsabilidad, no solo al fabricante del producto final (el robot) sino también al desarrollador del software

puede ser responsable de los daños causados por el carácter defectuoso de tal software (no así el creador del software de código abierto).

[24] En la versión de 24-1-2024 se ha suprimido la necesidad de que el componente haya sido integrado en el producto por el fabricante o bajo su control, seguramente con el fin de que pueda demandarse a los productores de componentes que han sido integrados *fuera del control del fabricante* con base en la normativa de productos defectuosos (así se desprende de lo indicado en el último párrafo del Cdo. 26). Lo cierto es, sin embargo, que del nuevo art. 7,1 se deduce que para que exista responsabilidad, no solo del fabricante del producto final, sino también del fabricante del componente, sigue siendo necesario que se haya integrado bajo control de aquél, lo cual resulta un tanto contradictorio. Por lo que respecta a la noción de "control del fabricante", la misma alude al supuesto en que el fabricante ha autorizado o consentido la integración o interconexión del componente (art. 4.5).

en cuanto fabricante de un "componente" defectuoso (cfr. art. 7.1), pudiendo ambos responder solidariamente (art. 11).

Aunque en principio la Propuesta de Directiva no se aplica a los servicios, en la actualidad hay productos cuyo funcionamiento depende de que reciban un servicio digital, como sucede, por ejemplo con el suministro de datos de tráfico que precisa un sistema de navegación, o el servicio de control de temperatura de un frigorífico inteligente (Cdo. 15). Por tal motivo el art. 4,3 de la Propuesta considera también como "componentes" los *servicios conexos*, entendiéndose por tales aquellos servicios digitales necesarios para que un producto funcione, siempre que estén integrados en el producto o interconectados con él bajo control del fabricante (cfr. art. 4.4 y Cdo. 15). El hecho de que se considere como componente el "servicio conexo" implica que el fabricante del producto final no podría declinar su responsabilidad aduciendo que el carácter defectuoso del producto ha sido ocasionado por un tercero ajeno al mismo. Por otra parte, esto implica que tanto el fabricante del componente digital como el suministrador del servicio tendrán la consideración de "fabricantes" a efectos de responsabilidad[25].

Se plantean ciertas dudas en torno a los datos de los que se nutren los sistemas de IA. Pensemos por ejemplo en la multitud de imágenes que hay que suministrar a un sistema automático de reconocimiento facial, o en los datos de entrenamiento para un robot médico de rehabilitación. Si los datos son erróneos y provocan un mal funcionamiento del sistema ¿podría ser considerado el suministrador de esos datos como fabricante de un "componente" del sistema IA a efectos de responsabilidad? La Propuesta de Directiva, en la medida que presupone que la "información" no tiene la consideración de producto (Cdo. 12),

---

[25] Si el servicio conexo no se presta bajo control del fabricante la responsabilidad del prestador deberá basarse en su culpa o negligencia. González Beluche, P., "La adaptación de la Directiva 85/374/CEE, de 24 de julio, en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución industrial", *CDT*, octubre 2023, vol. 15, núm. 2, p. 461. El párrafo añadido al Cdo. 26 en el Texto de compromiso de 24-1-2024 parece dar a entender que el fabricante de un componente puede ser demandado conforme a la normativa de productos defectuosos si el componente puede ser calificado, en sí mismo, como "producto". Aunque el añadido es de dudosa interpretación (vid. nota anterior), al no aplicarse la Propuesta de Directiva a los servicios (Cdo. 15), no parece que el servicio conexo, en sí mismo considerado, pueda ser calificado como producto.

parece excluir tal posibilidad[26]. Adviértase, sin embargo, que algunos "servicios conexos" consisten en el suministro de datos y no parece lógico que los datos tengan la consideración de componente cuando se suministran de manera periódica pero no si se introducen de manera puntual[27]. La cuestión no está clara en la Propuesta (ni en la versión original ni en la de 24-1-2024) y sería deseable que se aclarara en el texto final de la futura Directiva. En cualquier caso, la exclusión de los datos suministrados inicialmente y no de forma periódica de la noción de componente llevaría a dilucidar la posible responsabilidad del suministrador de los mismos con base en las reglas generales.

2) Se amplía el elenco de sujetos responsables

La propuesta de Directiva ha aumentado el número de "operadores económicos" que pueden incurrir en responsabilidad a fin de incluir algunas figuras (v. gr. prestador de servicios de tramitación de pedidos a distancia, plataformas online) que han aparecido en el mercado a consecuencia de la creación de nuevos modelos de negocios (art. 7). No obstante, estos sujetos, como más adelante se verá, responden subsidiariamente. Al igual que en la Directiva vigente, los sujetos eminentemente responsables del daño son el fabricante del producto defectuoso o de alguno de sus componentes (art. 7.1) y, en caso de productos fabricados fuera de la UE, el importador, que responderá, en su caso, junto con el "representante autorizado del fabricante" (art. 7.2). La concurrencia de varios sujetos como posibles responsables de un mismo daño se rige por las reglas de la solidaridad (art. 11). Por otra parte, la responsabilidad del suministrador sigue siendo subsidiaria, para el supuesto en que no identifique al operador económico responsable en el plazo de un mes desde que se le solicite la indentificación (art. 7.5).

La ampliación de los sujetos que eventualmente pueden incurrir en responsabilidad no es de especial relevancia en lo que respecta a los daños provocados por sistemas inteligentes, ya que la posibilidad de dirigirse contra su fabricante

---

[26] Atienza Navarro, M. L., "¿Una nueva responsabilidad por productos defectuosos?...", cit., pp. 11-12. El texto de compromiso de 24-1-2024 ha añadido, en el Cdo. 12, algunos ejemplos de lo que se considera mera "información", concretamente, alude al "contenido de archivos digitales tales como archivos multimedias o ebooks" lo que no aclara mucho la situación.

[27] En este sentido, González Beluche, P., ob. cit., pp. 457-458.

o desarrollador es consecuencia de la expansión del concepto de producto y de componente, y no tanto de la inclusión, en el art. 7, de esas nuevas figuras.

El art 4.11, ligeramente modificado en el Texto de compromiso de 24-1-2024, define al fabricante como "toda persona física o jurídica que: a) desarrolla, fabrica o produce un producto; o b) que lo ha hecho diseñar o fabricar o que, poniendo su nombre, marca u otra característica distintiva en el producto, se presenta a sí mismo como fabricante; o que c) desarrolla, fabrica o produce un producto para su propio uso". Esto implica que, aunque en el proceso de fabricación de robots o sistemas de inteligencia artificial de carácter complejo pueden intervenir diversos sujetos: diseñador, desarrollador del software, suministrador de los datos empleados por el sistema inteligente, entrenador del robot, etc., a efectos de la responsabilidad por productos defectuosos, el sujeto responsable es únicamente quien tenga la consideración de "fabricante", que será la persona que haya producido o mandado diseñar o fabricar el bien de que se trate y que presumiblemente lo comercializará bajo su nombre o marca (también cabe la posibilidad que un sujeto comercialice bajo su marca productos fabricados por un tercero, en cuyo caso estaremos ante el denominado "fabricante aparente", que será responsable junto con el fabricante real). Dado que la Propuesta de Directiva solo se aplica a productos que se introduzcan en el mercado en el seno de una actividad comercial (Cdo. 20), la consideración como fabricante de aquel que desarrolla o fabrica un producto *para uso propio,* parece estar referida a la hipótesis en que el producto ha sido fabricado por un sujeto que lo utiliza en la prestación de un servicio[28].

Salvo por lo que respecta al posible desarrollador del software –que en tanto fabricante de un "componente" del producto final podría ser demandado junto con el productor de este último si el defecto reside en dicho componente (art. 7.1)– los demás sujetos mencionados no pueden ser considerados

---

[28] Observa Martín Casals, ob. cit., p. 81, que con ello se da cabida a supuestos como el que tuvo que resolver el TJUE en el caso Veedfald (Asunto C-203/1999). En este supuesto un hospital danés, que debía llevar a cabo un trasplante de riñón, conservó este órgano en un líquido de irrigación fabricado en el mismo hospital, que resultó ser defectuoso y provocó daños en el riñón imposibilitando el trasplante. El hospital demandado intentó exonerarse aduciendo que no había puesto el producto en circulación. El TJUE afirmó, sin embargo, que "el hecho de que un producto utilizado en el marco de una prestación de servicios haya sido fabricado por un tercero, por el prestador del propio servicio o por una entidad con él relacionada no puede por sí mismo tener incidencia en el hecho de que haya sido puesto en circulación".

responsables conforme a la normativa de productos defectuosos[29]. La responsabilidad corresponderá únicamente al fabricante (o, si este es extracomunitario, a quien introduce el producto en la Unión Europea) quien, podrá, en su caso, ejercitar las correspondientes acciones de regreso contra aquellos conforme a las normas de la relación interna que resulte aplicable.

El fabricante responde, asimismo, como antes de indicó, en aquellos casos en que la defectuosidad del producto tiene su origen en un servicio conexo, y lo hará también si se debe a actualizaciones o mejoras que están "bajo su control" (art. 7.1) Esto implica que han debido suministrarse por el propio fabricante o, si lo son por un tercero, con su consentimiento o autorización (art. 4.5, Cdo. 15 y 15a). Así se desprende además del art. 10.2 que le impide eximirse de responsabilidad en tales casos. La misma regla es aplicable cuando el producto ha sido fabricado fuera de la UE y es el importador el sujeto responsable. Ahora bien, si el defecto ha sido ocasionado por un servicio conexo o una mejora o actualización que *no han sido introducidas bajo el control del fabricante*, ni fabricante ni importador responderán[30].

A los sujetos tradicionalmente responsables la Propuesta añade otros no contemplados hasta ahora, pero que responden solo subsidiariamente:

a) El art. 7.1 incluye entre los operadores económicos que pueden ser declarados responsables al denominado "*prestador de servicios de tramitación a distancia",* figura que alude a aquellas personas físicas o jurídicas que, en el ámbito del comercio en línea, se encargan de almacenar, distribuir y/o enviar los productos fabricados por terceros al comprador, sin adquirir

---

[29] Ello no impide que el eventual perjudicado pueda accionar directamente contra ellos invocando las reglas de responsabilidad por culpa, si han actuado negligentemente y existe relación causal entre su comportamiento y el daño causado.

[30] Conforme a la versión inicial de la Propuesta de Directiva cabía pensar que, para imputar responsabilidad al posible causante del daño, había que acudir a las reglas generales (González Beluche, P., ob. cit., pp. 374, 375). Las modificaciones introducidas en el art. 4,3 y el Cdo. 26 por el Texto de compromiso de 24-1-2024 dan a entender que el prestador del servicio conexo o la mejora incorporada fuera del control del fabricante podrá ser demandados conforme a la futura Directiva si tales elementos pueden considerarse productos en sí mismos. Dado que los servicios conexos, aisladamente considerados, no pueden conceptuarse como productos, la responsabilidad del prestador deberá basarse en la culpa. En el caso del desarrollador de la mejora o actualización ello dependerá de que tengan suficiente sustantividad como para ser consideradas "productos" de forma independiente.

previamente su propiedad (art. 4.14). A través de internet y por su mediación, un sujeto puede adquirir productos fabricados en cualquier lugar del mundo. Por eso la Propuesta lo considera responsables, pero subsidiariamente, solo en el supuesto en que el fabricante del producto proceda de un país no europeo y *no exista en Europa un importador ni aquel cuente con un representante autorizado*.

b) También se incluye en el art. 7.6 a las *plataformas on line*. En principio las plataformas *on line* actúan como meros intermediarios conectando a vendedores (profesionales o no) con posibles adquirentes. Sin embargo, hay casos en que la forma en que presentan los productos, publicidad, etc., puede hacer creer al consumidor medio que el producto es suministrado por la propia plataforma en línea (Cdo. 28). En tal hipótesis podrán ser equiparados al suministrador a efectos de responsabilidad. Es decir, responderán subsidiariamente si no identifican al fabricante, importador o representante autorizado (o, en su caso, prestador de servicios de tramitación a distancia) en el plazo de un mes desde la recepción de tal solicitud.

Una última novedad es la posibilidad de considerar como fabricante de un producto a quien lo modifique y lo coloque en el mercado si la modificación es sustancial y se realiza fuera del control del fabricante original[31].

3) Se añaden algunas circunstancias útiles para valorar el carácter defectuoso de un producto

La noción de defecto o defectuosidad no se ha modificado sustancialmente y sigue estando ligada a la seguridad que de un producto cabe esperar. El problema en la práctica, como ya se ha avanzado, puede ser determinar, en el caso concreto de los sistemas de inteligencia artificial, el estándar de seguridad exigible. En cualquier caso, el art. 6 de la Propuesta enumera una serie de circunstancias que han de ser tenidas en cuenta para valorar el carácter defectuoso de un

[31] En la versión de la Propuesta de 24-1-2024 se ha añadido un párrafo al art. 4 (el 17b) para definir qué se entiende por "modificación sustancial", que se refiere a la realizada una vez que el producto ha sido introducido en el mercado o puesto en servicio, si es considerada sustancial conforme a reglas europeas o nacionales sobre la seguridad del producto, o si la modificación cambia su finalidad, crea un nuevo riesgo, aumenta su nivel o modifica la naturaleza del mismo. Los operadores que se limitan a llevar a cabo reparaciones u otras operaciones que no conllevan modificaciones sustanciales no están sujetos a responsabilidad bajo la Directiva (Cdo. 29).

producto. Se incluyen las circunstancias mencionadas en la Directiva vigente, que atañen a la presentación del producto, el uso que razonablemente se le puede dar y el momento de su puesta en circulación[32], respecto de las que se introducen algunas matizaciones[33]. Pero además se añaden otras, algunas de las cuales parecen específicamente pensadas para los sistemas de inteligencia artificial. Así, el art. 6 dispone que deberá tenerse en cuenta para valorar el carácter defectuoso del producto:

a) *El efecto que sobre el producto puede tener su capacidad de autoaprendizaje* o adquisición de nuevas características (art. 6.c). Suele decirse que los sistemas con capacidad de aprendizaje pueden llegar a tener comportamientos imprevisibles incluso para sus creadores[34]. Ello no impide, sin embargo, que el producto pueda ser considerado defectuoso porque, como indica el Cdo. 23, existe una expectativa legítima de que el software y los algoritmos subyacentes sean diseñados *de modo que eviten cualquier comportamiento peligroso del producto.* Como ha observado la doctrina, en este tipo de sistemas es necesario reforzar el aprendizaje y entrenamiento del dispositivo antes de su comercialización de modo que esta no debe producirse hasta que se hayan sobrepasado ciertos umbrales de seguridad que deben ser altos como regla general y tomar en consideración la relevancia del bien jurídico que pueda verse amenazado[35].

b) *El efecto sobre el producto de otros productos que quepa razonablemente esperar que se usen junto con aquel*. Se está haciendo referencia aquí a los defectos que puedan surgir en el contexto del internet de las cosas, donde el inadecuado funcionamiento de un dispositivo puede deberse a fallos de

---

[32] *Vid*. Santos Morón, M. J., ob. cit., pp. 140-141.

[33] Se indica, por ejemplo, que la presentación y las características del producto incluyen, además de su etiqueta, características técnicas, composición, etc., "las instrucciones de instalación, uso y mantenimiento", lo que es de especial relevancia en productos con tecnología avanzada y compleja. Al "uso razonablemente previsible" se añade el "uso indebido" del producto (el cual podría suponer que el daño no es atribuible al carácter defectuoso del producto). La referencia al momento de la puesta en circulación del producto se sustituye, de acuerdo con la terminología empleada en la Directiva proyectada (art. 4.8 y 4.10), por la introducción del producto en el mercado o su puesta en servicio.

[34] Atienza Navarro, M. L., "¿Una nueva responsabilidad por productos defectuosos?", cit., p. 16.

[35] Ataz López, J., ob. cit., p. 38.

conexión (defectos de interconectividad) o, por el contrario, a su interconexión con otros dispositivos y los datos enviados por estos.

c) *Los requisitos "relevantes" de seguridad del producto, incluyendo los de ciberseguridad*. La posibilidad de considerar defectuoso un producto que no cumple con los requisitos de seguridad legalmente establecidos no es nueva. No obstante, la referencia expresa a ellos quizás se explique porque el Reglamento IA pretende fomentar estos requisitos en el ámbito de la inteligencia artificial. En cualquier caso, la alusión a los requisitos de ciberseguridad es útil, ya que permite que el producto se considere defectuoso si no va acompañado de medidas eficaces para evitar brechas de seguridad en ese ámbito. Por ejemplo si no se suministran actualizaciones para atender vulnerabilidades de seguridad[36].

El art. 6 menciona también otras circunstancias que no están específicamente relacionadas con los sistemas de inteligencia artificial, pero que pueden ser relevantes en algunos casos. Concretamente alude a la *intervención de una autoridad reguladora o un operador económico*, supuesto este que se ha planteado en la práctica en casos en que el propio fabricante de un producto o la Administración (v. gr. Agencia Española del Medicamento) han aconsejado la retirada del mismo del mercado (STS 9 diciembre 2010, RJ 2011/1408; 1 marzo 2021, RJ 2021/881).

En segundo lugar, el citado precepto hace referencia también a las "*necesidades específicas del grupo de usuarios a los que se destina el producto*". Con ello se recoge la jurisprudencia sentada por el TJUE (S. 5 marzo 2017, Asuntos C-503/10 y C-404/10) que, en relación con dispositivos médicos, ha incidido en la necesidad de tomar en consideración la situación de los destinatarios del producto. Esta circunstancia es de particular relevancia en aquellos casos en que se utilizan robots de uso médico (v gr. robots quirúrgicos, robots para rehabilitación, exoesqueletos, etc.) ya que implica que, dada la vulnerabilidad de los destinatarios, las expectativas de seguridad de estos dispositivos son particularmente altas.

El elenco de circunstancias mencionadas es útil en la medida que, tomándolas en consideración, puede llegarse a la conclusión de que el producto no reviste la seguridad que cabe esperar, en cuyo caso deberá ser considerado defectuoso. Al respecto conviene advertir que, al menos por lo que respecta al Derecho

---

[36] González Beluche, P., ob cit., p. 468.

español, la jurisprudencia no considera necesaria la prueba del concreto defecto que ha producido el daño, pues basta con convencer al juez de que el producto es *inseguro* (SSTS 19 febrero 2007, RJ 2007/1895; 23 noviembre 2007, RJ 2007\8122; 30 abril 2008, RJ 2009/2686). Esta regla, como fácilmente puede colegirse, de ser aplicada igualmente en el futuro, resultaría extremadamente útil en caso de daños causados por robots o sistemas inteligentes pues eximiría a la víctima de la necesidad de explicar por qué el producto en cuestión ha funcionado incorrectamente provocando el daño[37]. Desde esta perspectiva parece evidente que, si, por ejemplo, un robot quirúrgico como el Da Vinci, provoca quemaduras en los órganos internos del paciente que está siendo operado, como ha sucedido recientemente en Carolina del Norte[38], el producto debería considerarse defectuoso, sin necesidad de probar qué mecanismo o interacción de elementos ha sido la causa concreta de ese daño.

4) Se modifican alguna de las causas de exoneración de responsabilidad

Las causas de exoneración de responsabilidad son básicamente las mismas que en la actualidad, y se sigue manteniendo la relativa a la inexistencia del defecto en el momento en que el producto fue introducido en el mercado[39]. Por ello, para evitar que los posibles sujetos responsables, y en particular el fabricante,

---

[37] No sería necesario, como afirman algunos autores, "probar con precisión el defecto que fue la causa por la que se produjo el daño" (Atienza Navarro, M. L., "¿Una nueva responsabilidad por productos defectuosos?", cit., p. 29).

[38] Puede consultarse la noticia en: https://www.telemundo51.com/noticias/local/demanda-robot-quirurgico-quemo-paciente-intuitive-surgical-florida/2509171/

[39] Dichas causas de exoneración son las siguientes: a) que el producto no ha sido introducido en el mercado por el fabricante o importador o, en el caso del distribuidor, que no lo ha comercializado; b) que el defecto no era originario, es decir, que es probable que no existiera cuando el producto fue introducido en el mercado (o comercializado por el distribuidor); c) que el carácter defectuoso del producto tiene su origen en el cumplimiento de normas coercitivas dictadas por los poderes públicos; y d) que conforme al estado de los conocimiento científicos y técnicos, el defecto no podía detectarse cuando el producto se puso en circulación ni mientras ha permanecido bajo el control del fabricante (riesgos del desarrollo). Además, el fabricante de un componente puede exonerarse demostrando que el carácter defectuoso del producto es imputable al diseño del producto al que se incorpora o a las instrucciones dadas por su fabricante. Y quien modifica sustancialmente un producto puede exonerarse demostrando que el daño tiene su causa en una parte del producto no modificada. Por lo que respecta a la causa de exoneración sobre riesgos del desarrollo, hay que advertir que la última versión de la Propuesta ha incorporado un nuevo precepto dirigido a permitir a los Estados miembros su exclusión.

puedan exonerase de responsabilidad como consecuencia de mejoras o actualizaciones necesarias para que los componentes digitales del producto continúen funcionando correctamente y, para evitar, en segundo lugar, que queden exonerados de responsabilidad a consecuencia de defectos provocados por servicios digitales que son prestados por terceros bajo control del fabricante una vez puesto el producto en circulación (adviértase que, en ambos casos, en la medida que el producto no era inicialmente defectuoso podrían quedar exonerados de responsabilidad) se establece una nueva regla.

Concretamente el art. 10.2 de la Directiva proyectada dispone que un operador económico no quedará exonerado de responsabilidad si el defecto se debe: a) a un servicio conexo; b) al software, incluyendo las actualizaciones o mejoras del mismo; c) a la falta de esas actualizaciones o mejoras si son necesarias para mantener la seguridad del producto. Todo ello siempre que el servicio conexo, las actualizaciones o mejoras estén bajo el control del fabricante. Tampoco habrá exoneración de responsabilidad, según la última versión de la Propuesta, si el defecto se debe a una modificación sustancial realizada bajo el control del fabricante.

5) Se introducen algunas reglas de flexibilización probatoria

La Propuesta de Directiva mantiene la regla tradicional según la cual corresponde al perjudicado probar el defecto, el daño y la relación de causalidad entre ambos (art. 9.1). No obstante, partiendo de que al perjudicado le puede resultar difícil acceder (y comprender) la información sobre cómo se ha fabricado el producto y cómo funciona, especialmente cuando se trata de productos de complejidad técnica o científica (Cdo. 30), se incluyen algunas reglas para facilitar la prueba a los demandantes.

Además de establecerse algunas presunciones a las que a continuación se aludirá, el art. 8,1 faculta a quien presente una demanda de responsabilidad por daños causados por un producto defectuoso –siempre que haya aportado indicios de su verosimilitud–, para solicitar al juez que ordene al demandado que revele "las pruebas pertinentes" de que disponga (se entiende que sobre el funcionamiento del producto, su proceso de fabricación, etc.), si bien tal exhibición de pruebas debe limitarse a lo que según el órgano judicial "sea necesario y proporcionado", debiendo preservarse la confidencialidad de los secretos comerciales (art. 8.2 a 8.4).

Si bien es evidente que esta facultad de solicitar la "exhibición de pruebas" beneficia al posible demandante, hemos de recordar que en España la jurisprudencia no exige la prueba del concreto defecto que ha producido el daño, sino solo demostrar que el producto es inseguro[40]. Por ello (y salvo que modifique esta doctrina en el futuro) la exhibición de pruebas podría ser útil, sobre todo, para determinar si tiene sentido demandar, junto al fabricante del producto final, al fabricante de algún componente, o si puede concurrir alguna causa de exoneración que permita al demandado eludir su responsabilidad[41].

La Directiva proyectada contiene además diversas presunciones de defecto y de relación causal, de carácter "iuris tantum" (art. 9.5).

El art. 9.2 dispone que *se presumirá el carácter* defectuoso del producto cuando se den alguna de las siguientes condiciones:

a) Si el demandado no ha exhibido las pruebas pertinentes de que disponga de acuerdo con lo indicado con anterioridad. Obviamente esto supone un incentivo importante para cumplir tal requerimiento.

b) Si el demandante prueba que el producto no cumple con los requisitos de seguridad establecidos en la normativa interna o europea "que tienen por objeto proteger contra el riesgo del daño sufrido". Esta presunción parece innecesaria pues, si el carácter defectuoso de un producto deriva de su falta de seguridad, es evidente que el incumplimiento de los requisitos

---

[40] En mi opinión, las posibles dificultades probatorias del demandante podrían resolverse mucho más fácilmente recogiendo en la Directiva proyectada una regla similar. En la Respuesta del European Law Institut a la Consulta de la Comisión europea, se planteaba esta posibilidad, aunque limitada a los productos con elementos digitales (European Law Institute, "Response of the European Law Institute to the European Commission's Public Consultation on civil Liability", cit. 2022, p. 18). La duda que puede suscitarse en el futuro, en caso de que se mantenga el texto actual de la Propuesta de Directiva es si, siendo esta una Directiva de máximos, los tribunales españoles podrán seguir interpretando que no es necesario probar el concreto defecto que ha causado el daño y basta con demostrar que el producto es, en su conjunto, inseguro.

[41] La doctrina observa que debería admitirse la posibilidad de ejercitar esta facultad no sólo una vez presentada la demanda de responsabilidad (como parece exigir el art. 8) sino también con anterioridad, como admite la Propuesta de Directiva sobre responsabilidad IA que reconoce a los perjudicados una facultad similar (art. 3.1). En este sentido, Atienza Navarro, M. L., "¿Una nueva responsabilidad por productos defectuosos?", cit., p. 33; Hacker, P., "The European AI Liability Directives. Critique of a Half Hearted-Approach an Lessons for the Future", Working Paper, versión 28-3-2023, p. 28. Sin embargo, la última versión de la Directiva, de 24-1-2024, parece remitirse en este punto al Derecho interno (Cdo. 31 a; art. 8).

de seguridad establecidos legalmente para ese producto debe determinar su carácter defectuoso[42]. De hecho, parece que su finalidad es, más bien, limitar la posibilidad de considerar defectuoso un producto, pues exige que los requisitos de seguridad incumplidos tengan como fin "proteger contra el riesgo del daño sufrido por el perjudicado"[43], con lo que es dudoso que se esté mejorando la situación de la víctima.

c) Si el demandante prueba que el daño fue causado por un evidente mal funcionamiento del producto durante su uso razonablemente previsible o en circunstancias normales. En lo que respecta al Derecho español esta presunción no modifica gran cosa la situación, ya que los tribunales españoles, para determinar el carácter defectuoso del producto, vienen haciendo uso de la prueba de presunciones ex art. 386 LEC (cfr. STS 23-11-2007, RJ 2007\122; 14-9-2018, RJ 2018\3995), entendiéndose en la práctica que si se utiliza un producto de manera correcta y no existe otra explicación para su inadecuado funcionamiento el producto es defectuoso[44].

También establece el art. 9, en su apartado 3, una *presunción de relación causal* entre el daño y el carácter defectuoso del producto en el supuesto en que dicho daño sea "compatible normalmente con el defecto en cuestión". Ahora bien, si para hacer uso de esta presunción fuese necesario demostrar, no el carácter defectuoso del producto en su conjunto, sino el defecto concreto que ha provocado el incorrecto funcionamiento del producto (como parece deducirse del tenor literal de la norma), tal presunción puede ser de poca o escasa utilidad.

Finalmente, el art. 9.4 –algo modificado en la última versión de la Propuesta– dispone que el tribunal nacional presumirá el carácter defectuoso del producto o el nexo causal, si, pese a haberse llevado a cabo la exhibición de pruebas y teniendo en cuenta las circunstancias, el demandante, debido a una complejidad técnica o científica, se enfrenta a excesivas dificultades a la hora de probar el carácter defectuoso del producto o el nexo causal (*vid*. Cdo. 34). Ahora bien,

---

[42] Es decir, debería concluirse, como indica Evangelio Llorca, R., "Causalidad y responsabilidad civil por los daños causados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE", XXII Jornadas APDC, (pdf impreso), p. 27, que el producto es defectuoso, sin necesidad de presumirlo.

[43] *Vid*. González Beluche, ob. cit., p. 478, nota 225.

[44] *Vid*. Santos Morón, ob. cit., p. 142.

para ello es necesario que el demandante demuestre que es probable que el producto sea defectuoso o que su carácter defectuoso ha podido producir el daño. En realidad, la posibilidad de recurrir a presunciones de hecho en casos concretos ya había sido consagrada por el TJUE 21 junio 2017, Asunto C-621\5, en un supuesto en que la demandante alegaba haber contraído esclerosis múltiple como consecuencia del suministro de una vacuna. El tribunal europeo sostuvo que el juez nacional podía considerar probado el defecto y la relación causal por medio de presunciones basadas en la existencia de indicios sólidos. Sin embargo, por lo que respecta al citado art. 9,4 de la Propuesta, la necesidad de demostrar previamente que es probable (¿en qué grado de probabilidad? cabría preguntarse) que el producto sea defectuoso o que el defecto causó el daño, junto con la limitación de la posibilidad de acudir a dicha presunción a los supuestos en que, habiéndose solicitado exhibición de pruebas, aun existan "excesivas" dificultades probatorias, pueden convertir nuevamente en poco útil esta previsión[45].

4. LA APLICACIÓN DE LAS REGLAS DE RESPONSABILIDAD POR CULPA

Pese a las modificaciones proyectadas en la Propuesta de Directiva sobre responsabilidad por productos defectuosos, lo cierto es que en muchos casos será necesario acudir a las reglas generales de responsabilidad por culpa:

a) En primer lugar, y como ya se indicó, el carácter defectuoso de un producto deriva de su falta de seguridad. No, estaremos, por tanto, ante un producto defectuoso cuando no cumpla las expectativas de calidad o no sirva adecuadamente para el uso que se le presupone al contratar. Por otra parte, salvo concretas excepciones, tampoco podrá invocarse este régimen especial de responsabilidad objetiva si han transcurrido más de 10 años desde que el producto causante del daño se introdujo en el mercado.

b) En segundo lugar, en todos aquellos supuestos en que el sistema de IA genere un perjuicio no resarcible de acuerdo con la futura Directiva de productos defectuosos (v. gr. daño a bienes empresariales o de equipo; daño moral derivado de la lesión de derechos de la personalidad, etc.)

---

[45] En este sentido Atienza Navarro, "¿Una nueva responsabilidad por productos defectuosos?", cit., p. 37.

habrá que acudir a los regímenes internos de responsabilidad. Recordemos, además, que las personas jurídicas no están protegidas por la normativa europea, por lo que los daños que puedan sufrir deberán ser reparados conforme a las reglas generales.

c) Cuando el defectuoso funcionamiento del robot o sistema inteligente se deba a un servicio conexo o a una mejora o actualización *no autorizada por el fabricante*, la eventual demanda contra el prestador del servicio conexo parece que deberá basarse en la culpa. La responsabilidad del desarrollador de la mejora o actualización será asimismo exigible conforme a las reglas generales si una y otra no pueden ser consideradas, en sí mismas, como productos[46].

d) También parece que deberá acudirse al régimen general si el defecto tiene su origen en los datos suministrados al sistema inteligente y se pretende responsabilizar al sujeto que los ha proporcionado[47].

e) Por último, cabe la posibilidad de que el daño sea imputable al usuario del robot o sistema de IA, es decir, al sujeto que lo emplea en una actividad profesional o personal. Por ejemplo el médico que manipula un robot quirúrgico en el curso de una operación o el sujeto que dirige un dron. La responsabilidad del usuario, salvo que exista una norma específica que resulte de aplicación, deberá basarse en las reglas generales de responsabilidad.

En relación con este último supuesto, cabe pensar que si quien emplea el sistema inteligente es un empresario o un profesional, puede ser aplicable tanto el art. 1902 Cc. como el art. 1903.5 Cc. La doctrina observa, en este sentido, que un usuario profesional puede ser responsable por los fallos del sistema IA, al menos en la misma extensión que sería responsable por los actos u omisiones de un empleado o dependiente que realizara la misma tarea[48]. Así, si un centro

---

[46] *Vid*. nota 30.

[47] Como ya se dijo, conforme a la redacción actual de la Propuesta de Directiva, parece que los datos necesarios para que el sistema funcione encajarían en el concepto de "pura información" que se excluye de la noción de producto, por lo que tampoco pueden considerarse como "componente". Esta conclusión es, no obstante, controvertida y suscita críticas en la doctrina. González Beluche, P., ob. cit., pp. 459, 461, 462, 475, 476; Atienza Navarro, M.L., "¿Una nueva responsabilidad por productos defectuosos?", cit., pp. 11-12

[48] Wenderhost (2023). "Product Liability or Operator Liability for AI- What is the Best Way Forward?", Lohsse, Schulze y Staudenmayer (eds.), *Liability for IA,* Nomos, p. 121. En similar

hospitalario privado utiliza un robot desinfectante de limpieza que desinfecta erróneamente una habitación sin estar vacía, provocando daños a un paciente, este podría dirigirse contra el fabricante del robot –por ser defectuoso–, pero seguramente también podría reclamar responsabilidad al hospital al amparo del art. 1903.5 Cc[49]. La responsabilidad del empresario, que en teoría está basada en su propia culpa (*in eligendo* o *in vigilando*), pero que en la práctica se ha venido objetivizando, presupone, en principio, el comportamiento negligente del dependiente. Si ese "dependiente" es un robot o sistema inteligente, su comportamiento deberá compararse con el de otros sistemas del mismo tipo. Pero, en todo caso, podrá considerarse objetivamente negligente cuando, de haber actuado del mismo modo un humano, se hubiera llegado a tal conclusión[50]. Aunque hay quien estima que el precepto solo es aplicable si el dependiente que ha causado el perjuicio es una persona[51], creo que la forma en que la jurisprudencia española viene interpretando el art. 1903.5 –no es preciso identificar al concreto dependiente causante del daño ("culpa anónima") pues se entiende que el empresario responde por los daños producidos "en el círculo de actividad de la empresa"[52]– permite englobar en dicho precepto los daños causados por sistemas IA empleados en la actividad profesional o empresarial.

---

sentido se pronuncia el European Law Institute, "Response to the European Commission's Public Consultation...", cit., p. 29 y el informe del Expert Group on Liability and New Technologies, "Liability for Artificial Intelligence and Other Emerging Digital Technologies", cit., Key finding 18.

[49] Tratándose de un hospital también cabría pensar en aplicar el art. 148 TRLC que establece un régimen de responsabilidad objetiva para los servicios sanitarios. Sobre ello, Santos Morón, M. J., "La imputación de responsabilidad médica con base en las normas de protección de consumidores: el art. 148 TRLC", ADC, 2017-I, pp. 128 y ss.

[50] Observa Wenderhorst, C., ob. cit., p. 127 que el empresario debería responder al menos en la misma medida que si hubiese empleado a un auxiliar humano para tal tarea. Si un humano no la hubiese podido realizar, la referencia debe ser el nivel de funcionamiento de tecnología comparable. Asimismo, European Law Institute, "Response to the European Commission's Public Consultation...", cit., p. 31.

[51] Atienza Navarro, M. L. (2023). "La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión", *Responsabilidad extracontractual e inteligencia artificial,* XXII Jornadas APDC, p. 9 (pdf impreso).

[52] Con ello, como observa la doctrina, se interpreta el art. 1903.5 como un supuesto de responsabilidad por *fallos en el funcionamiento de la empresa*, que más bien debería basarse en el art. 1902 Cc. Beluche Rincón, I., "La responsabilidad del empresario por hecho de sus dependientes", *Practicum Daños,* 2019, p. 379; Del Olmo, P. (2023), "Comentario al art. 1903 Cc", *Comentarios del Código civil,* Cañizares Laso (dir.), Tomo V, Tirant lo Blanch, pp. 8575-8576.

Con independencia de lo indicado, el problema en la práctica es que para la víctima que ha de acudir a las reglas generales de responsabilidad (porque por ejemplo el daño provocado por el sistema IA no está cubierto por la normativa de productos defectuosos) puede ser difícil determinar a qué sujeto demandar.

Así, puede ocurrir que sea dudoso si el daño ha sido ocasionado por el usuario del robot o sistema inteligente (v. gr. por no haberlo empleado correctamente o haber introducido datos erróneos...) o es debido a un funcionamiento inadecuado del producto en cuestión. Por otra parte, en los casos en que el sistema inteligente está compuesto por dispositivos interconectados, el fallo puede estar en la conexión de la red o en infraestructuras que forman parte del sistema de IA[53].

La situación puede ser particularmente compleja cuando se trata de sistemas de IA autónomos, con capacidad de autoaprendizaje y, en particular, opacos[54]. Dado que es difícilmente explicable cuál ha sido el proceso decisorio que ha llevado a un determinado resultado, es igualmente complejo concluir que el resultado se debe a la intervención de este o aquel sujeto. ¿Cómo saber si el daño es debido a la actuación del programador, de quien ha suministrado los datos empleados por el sistema inteligente, o del sujeto que lo ha entrenado? En este último caso cabe pensar que, para eludir tal problema, el perjudicado puede demandar al "fabricante" del sistema de IA en su conjunto, pero, tanto si se invoca el art. 1902 Cc., como el art. 1903.5 Cc. sería necesario probar que se ha producido algún tipo de fallo o negligencia en el proceso de fabricación[55].

En este punto conviene aludir a la Propuesta de Directiva de responsabilidad IA, aplicable, como se dijo, en los casos en que se ejercita una acción de responsabilidad extracontractual basada en la culpa. Para facilitar la identificación de la persona potencialmente responsable de los daños causados por sistemas de inteligencia artificial se prevé la posibilidad del demandante, o potencial demandante, de solicitar al órgano judicial que ordene la exhibición de pruebas relativas a dicho sistema IA (art. 3,1; Cdo 17), que se limitará a lo necesario

---

[53] Gil Membrado, C. (2022). "Daños producidos por la IA: La opacidad del algoritmo y el efecto de caja negra", XXII Jornadas APDC, p. 16 (pdf impreso); Evangelio Llorca, R., ob. cit., p. 9 (pdf impreso).

[54] Sobre los problemas que trae consigo la opacidad de los sistemas de IA que emplean técnicas de aprendizaje profundo que les permiten tomar decisiones autónomas, vid. Gil Membrado, ob. cit., pp. 5 y ss.; 8 y ss., 15 (pdf impreso).

[55] *Vid*. nota 52.

y proporcionado para sustentar la posible demanda (art. 3,4). Tal exhibición de pruebas puede ser solicitada del proveedor del sistema IA sospechoso de causar el daño o del usuario del mismo, siempre que el interesado les haya pedido previamente sin éxito tal información[56]. Ahora bien, esta medida está limitada a los sistemas de IA considerados en el futuro Reglamento IA como *sistemas de alto riesgo* (cfr. art. 6 y Anexo III del Reglamento), porque respecto de ellos dicha norma impone determinadas obligaciones de documentación y registro (Cdo. 18). Esto, lamentablemente, restringe su operatividad. Adviértase que la dificultad para determinar al eventual responsable del daño depende, como observa Martín Casals, de la complejidad del sistema de IA y no, necesariamente, de sus riesgos[57], por lo que puede haber casos en que, planteándose igual dificultad, no pueda invocarse esta previsión.

Además, los requisitos para que proceda la exhibición de pruebas pueden hacer que esta medida no sea de gran ayuda para solventar la dificultad para identificar al potencial responsable. En efecto, el art. 3.1 de la Propuesta de Directiva sobre Responsabilidad IA exige que el demandante potencial presente hechos y pruebas suficientes para sustentar la viabilidad de la eventual demanda indemnizatoria (art. 3.1). ¿Cómo debe interpretarse esta exigencia? Si el potencial demandante tiene que demostrar, para que proceda la exhibición de pruebas, que determinado sujeto actuó negligentemente y puede ser el causante del daño en cuestión ¿qué sentido tiene entonces su solicitud?[58]. A menos que se interprete flexiblemente este requisito –siendo suficiente, por ejemplo, demostrar

---

[56] El proveedor, como se verá en el siguiente epígrafe, es equivalente al fabricante. Al proveedor se equiparan ciertas personas que quedan sujetas a sus mismas obligaciones de acuerdo con el Reglamento IA. Así, la exhibición de pruebas puede solicitarse del proveedor del sistema de IA, de las personas sujetas a las obligaciones del proveedor de acuerdo con el Reglamento IA y de los usuarios, con independencia de que sean demandados o terceros respecto de la demanda. No obstante, es necesario que tales sujetos estén obligados a documentar o registrar dichas pruebas de acuerdo con el mencionado Reglamento IA (cfr. Cdo. 19). Además, los terceros solo deben ser requeridos para la exhibición de pruebas si no pueden obtenerse del demandado (Cdo. 20). Para que proceda ordenar judicialmente la exhibición de pruebas es necesario que el interesado haya "realizado todos los intentos proporcionados de obtener del demandado las pruebas pertinentes" (art. 3.1).

[57] Martín Casals, M., ob. cit., p. 72; Hacker, P., ob. cit., pp. 13, 30, observa, en relación con ello, que muchos de los sistemas de IA que no se consideran de alto riesgo en el Reglamento IA son, sin embargo, susceptibles de producir más daños que los conceptuados como tales.

[58] Como observa Navas Navarro, S. (2022). "Régimen europeo en ciernes en materia de responsabilidad derivada de los Sistemas de Inteligencia Artificial", *Revista Cesco,* núm. 44, p. 49, si el

que se ha producido un daño a consecuencia del funcionamiento de un sistema de inteligencia artificial– este mecanismo no va a ser útil para identificar al posible responsable en caso de duda sobre el sujeto a quién demandar.

En realidad, aunque la finalidad de Propuesta de Directiva sobre responsabilidad IA es, según su Cdo. 7, garantizar que las personas que sufran daños por un sistema de IA y deben basar su demanda en los regímenes internos de responsabilidad disfruten de un nivel de protección equivalente a las perjudicadas por otras causas, las medidas en ella articuladas parecen de escasa virtualidad.

Junto a la posibilidad de solicitar la exhibición de pruebas ya comentada, la Propuesta contiene dos presunciones. Una que permite presumir que se ha incumplido un deber de diligencia si, habiéndose ordenado la exhibición de pruebas al demandado, este incumple tal obligación (art. 3.5) y otra presunción dirigida a facilitar la prueba de la relación causal (art. 4), a la que nos referimos a continuación.

4.1. La presunción de nexo causal de la Propuesta de Directiva sobre responsabilidad IA y su limitada operatividad

El art. 4 de la Propuesta de Directiva sobre responsabilidad IA regula una presunción "refutable de relación de causalidad" que requiere que se haya probado la culpa del demandado, lo que en la práctica puede ser tanto o más complejo que la demostración del nexo causal. La presunción no tiene como fin establecer el vínculo causal entre el comportamiento negligente del potencial demandado y el daño sufrido por la víctima (cuya prueba le corresponde), sino entre la culpa del demandado y "los resultados producidos por el sistema de IA o la no producción de resultados" (art. 4.1), es decir, entre la culpa del demandado y el comportamiento del sistema de inteligencia artificial.

En primer lugar y por lo que respecta del ámbito de aplicación de la mencionada presunción hay que tener en cuenta que:

a) La presunción opera cuando el sistema IA causante del daño es de *alto riesgo* de acuerdo con el Reglamento IA. Tratándose de sistemas de IA que no lo sean la presunción solo es aplicable si el juez nacional considera

potencial demandante ya tiene hechos y pruebas suficientes "¿no le sale más a cuenta interponer directamente una demanda reclamando la compensación de los daños ocasionados?".

excesivamente difícil para al demandante probar el nexo causal (art. 4.4). Así podría entenderse, según el Cdo. 28, cuando se trata de sistemas inteligentes autónomos y opacos.

b) La presunción se limita al supuesto en que el demandado es un *"proveedor de sistemas de IA"*, una persona sujeta a sus mismas obligaciones, o un "*usuario*" de ese tipo de sistemas, siempre y cuando estén sujetos a los requisitos establecidos en los capítulos 2 y 3 del título III del Reglamento IA.

El concepto de *proveedor* –para cuya determinación hay que remitirse al art. 3 del Reglamento de IA– es muy similar al definido como "fabricante" en la Propuesta de Directiva de productos defectuosos[59]. Al proveedor se equiparan los sujetos (v. gr. distribuidor, importador, etc.) que coloquen su marca en un sistema IA de alto riesgo ya existente en el mercado, hagan modificaciones sustanciales en dichos sistemas o modifiquen su finalidad haciéndolos de alto riesgo, de modo que quedan sujetos a las mismas obligaciones que el proveedor (art. 25 Reglamento IA –texto aprobado el 13-3-2024– en relación con art. 4.2 Propuesta Directiva responsabilidad IA). Esto implica que no encajan en la noción de proveedor sujetos que participan en el proceso de "fabricación" y desarrollo del sistema IA, como quien programa, suministra los datos de entrenamiento o entrena el sistema IA antes de que sea puesto en el mercado. Aunque podrían ser demandados conforme a un régimen de responsabilidad por culpa, parece que en tal caso no será aplicable la presunción de causalidad establecida en la propuesta.

Por lo que respecta al *usuario*, la presunción se aplica si se trata de una persona que emplea el sistema de IA en una *actividad profesional*. En caso de usuarios no profesionales la presunción solo operará si el sujeto en cuestión ha interferido sustancialmente en las condiciones de funcionamiento del sistema IA (por ejemplo si no respeta las instrucciones de uso) o si tuviese la obligación de determinar esas condiciones y no lo hubiera hecho (art. 4.6, Cdo. 29)[60].

---

[59] El art. 3.2, en la última versión disponible del Reglamento IA (texto aprobado el 13-3-2024) define al proveedor como la persona física o jurídica que desarrolla o hace desarrollar un sistema de IA y lo introduce en el mercado o lo pone en servicio con su propio nombre o marca comercial, ya sea a título oneroso o gratuito.

[60] Evangelio Llorca, R., ob. cit., p. 41.

De lo expuesto se desprende que el potencial ámbito de aplicación de la mencionada presunción de nexo causal es limitado. Pero es que para su operatividad es necesario, además, que se den ciertos requisitos previos:

a) La víctima *debe haber probado* que la información generada por un sistema de IA o la ausencia de esa información *le ha causado un daño* (art. 4.1.c).

b) Es preciso *que se haya probado la culpa del demandado* (bien directamente o a través de la presunción establecida en el art. 3.5 anteriormente aludida)[61]. Pero no basta cualquier tipo de negligencia, es necesario que el demandado haya incumplido un deber de diligencia impuesto por la ley –que debe estar dirigido a proteger frente al daño producido (Cdo. 22)– siempre que, además, sea razonable pensar que ese incumplimiento ha podido influir en los resultados producidos por el sistema de IA[62] (art. 4.1, a y b).

Además, cuando el daño ha sido ocasionado por *un sistema IA de alto riesgo* (recordemos que si no es alto riesgo la presunción solo operará si el juez considera demasiado difícil la prueba de la causalidad), la Propuesta delimita qué se entiende por culpa. Así, solo puede considerarse que el demandado (proveedor o persona sujeta a las obligaciones del proveedor) ha incurrido en culpa si ha incumplido ciertos requisitos –establecidos, según la última versión del Reglamento IA, en el capítulo 3 de su título III– que son enumerados en el art. 4.2 de la Propuesta comentada[63]. Debe entenderse que el hecho de que el demandado

---

[61] El precepto se refiere a la "culpa del demandado o de una persona de cuyo comportamiento sea responsable el demandado" de lo que cabe deducir que la presunción podría ser aplicable igualmente en los supuestos de responsabilidad por hecho ajeno antes mencionados.

[62] A esta convicción parece que podrá llegar el juez a tenor de las circunstancias. No parece que la norma pretenda imponer al demandante la carga de probar que es razonablemente probable que la culpa del demandado haya influido en los resultados producidos o dejados de producir por el sistema de IA (en este sentido Evangelio Llorca, R., ob. cit. p. 39). De entenderse así la norma la presunción de causalidad le serviría de bien poco pues previamente tendría que demostrar la verosimilitud del nexo causal (vid. Navas Navarro, S., "Régimen europeo...", cit., p. 54),

[63] De acuerdo con el art. 4.2 existirá culpa en los siguientes casos: a) El sistema de IA ha sido entrenado con datos que no cumplen los criterios de calidad establecidos el Reglamento IA; b) No cumple los requisitos de transparencia en el establecidos; c) No ha sido diseñado y desarrollado de modo que permita una vigilancia efectiva de una persona física durante el período de utilización del sistema de IA; d) No alcanza el nivel de ciberseguridad exigible de acuerdo con su finalidad; y e) No se han adoptado de forma inmediata las medidas necesarias para poner el

no haya incumplido ninguno de estos requisitos no significa que no pueda considerarse negligente conforme al Derecho interno que resulte aplicable (Cdo. 11)[64]. Pero no podrá invocarse, para demostrar el nexo causal, la presunción establecida en la Propuesta de Directiva de responsabilidad IA.

Por lo que respecta al supuesto en que el demandado es un *usuario de un sistema de IA* de alto riesgo, para que pueda entenderse cumplido el requisito de la culpa (que permite desencadenar la presunción de causalidad), será necesario, nuevamente, que haya incumplido las obligaciones que le impone el Reglamento de IA (art. 4.3)[65].

La limitación de los supuestos en que el comportamiento del proveedor, sujeto sometido a sus obligaciones, o usuario puede ser considerado negligente, restringe la operatividad de la presunción de causalidad en ella incorporada. No obstante, la doctrina observa que, dado que la proyectada Directiva es de mínimos, nada impediría al legislador nacional ampliar el catálogo de faltas de diligencia[66].

Por otra parte, conviene advertir que según el art. 4.4 la presunción de causalidad no operará si el demandado demuestra que el demandante puede acceder "razonablemente" a pruebas y conocimientos especializados "suficientes" para demostrar el nexo causal, lo que suscita la duda sobre cuándo se dará tal situación de razonabilidad y suficiencia.

A la vista de lo expuesto puede decirse que la presunción de causalidad analizada tiene limitada operatividad. Como ha puesto de relieve Navas Navarro,

---

sistema de IA en conformidad con las obligaciones que establece la Propuesta de Reglamento IA, o, en su caso, retirarlo del mercado.

[64] El Cdo. 11 de la propuesta indica que la misma no pretende armonizar los aspectos generales de la responsabilidad civil regulados en las normas nacionales "como la definición de la culpa o la causalidad, los diferentes tipos de daños", etc. Además, el Cdo. 14 señala que la Propuesta sigue un enfoque de armonización mínima, que permite al perjudicado invocar normas más favorables del derecho nacional.

[65] Concretamente, será necesario que se demuestre que: a) No empleó o supervisó el sistema de IA de acuerdo con sus condiciones de uso o no suspendió o interrumpió su uso de acuerdo con el Reglamento IA; y b) Expuso al sistema de IA a datos de entrada que no eran pertinentes conforme al Reglamento IA.

[66] Evangelio Llorca, R., ob. cit., p. 38.

aunque la Propuesta de Directiva responsabilidad IA pretende aliviar la carga de la prueba de la víctima, en realidad lo hace en escasa medida[67].

En cualquier caso, las reglas de la Propuesta no impiden la aplicación de normas más favorables para los demandantes en el Derecho interno, siempre que sean compatibles con el Derecho de la Unión. Así, se entiende que en España sería aplicable, como norma más beneficiosa, la inversión de la carga de la prueba prevista en el art. 30 Ley 14/2022 de 12 de julio, integral para la igualdad de trato y no discriminación por los daños causados a una persona por los sesgos discriminatorios que presenta el sistema de IA[68].

5. CONCLUSIONES

La postura actual en la Unión Europea parece apostar por concentrar la responsabilidad por los daños causados por sistemas IA en la figura del fabricante, que responderá objetivamente si el producto es defectuoso. Este planteamiento tiene sentido si se piensa que, siendo los robots y sistemas de inteligencia artificial cada vez más autónomos, lo más probable es que los daños que puedan causar se deban a las características del producto y no al comportamiento del usuario[69]. Desde este punto de vista parece sensato que quien emplea un sistema de inteligencia artificial no deba responder por el mero hecho de usarlo en su beneficio, sino únicamente cuando actúa negligentemente[70].

Además, la responsabilidad objetiva del "fabricante" permite obviar algunos de los problemas que plantean los sistemas de IA con capacidad de aprendizaje y decisión autónoma. El hecho de que produzcan daños que sus creadores (por ejemplo el diseñador, programador, formador, etc., de la máquina que aprende por sí sola) no pudieron prever, no parece que permita concluir que ha existido un comportamiento negligente por su parte[71]. Sin embargo, si el sistema autónomo causa daños que sobrepasan el nivel de seguridad que cabe esperar,

---

67 Navas Navarro, S., "Regimen europeo...", pp. 55, 65.

68 Evangelio Llorca, R., ob. cit., pp. 33-34; Gil Membrado, C., ob cit., p. 23; Navas Navarro, S., "Régimen europeo en ciernes...", cit. p. 51.

69 Wendenhort, C., ob. cit., p. 126.

70 No obstante, hay quien, como Spindler, G., ob. cit., p. 88, critica que los usuarios de sistemas de inteligencia artificial se beneficien del "privilegio" de la responsabilidad por culpa.

71 En este sentido Gil Membrado, C., ob. cit., p. 10.

no debería haber dificultad para considerar el producto defectuoso, e imputar, por consiguiente, responsabilidad a su fabricante.

Las modificaciones que la Propuesta de Directiva pretende introducir en la actual regulación de productos defectuosos resultan suficientes para adaptarla a las peculiaridades de las nuevas tecnologías. No obstante, las presunciones establecidas en el art. 9 para aligerar la carga de la prueba del demandante no parece que vayan a mejorar mucho la situación actual. En concreto, las dificultades para probar el "defecto" a las que, con tanta frecuencia alude la doctrina, y que parecen también estar en la mente de los redactores de la Propuesta, podrían solucionarse más fácilmente entendiendo, como ha venido haciendo la jurisprudencia española, que el perjudicado solo tiene que convencer al juez de que el producto es inseguro, sin necesidad de demostrar el concreto defecto causante del daño.

Es de notar, por otra parte, que los empresarios y profesionales (así como las personas jurídicas) no podrán beneficiarse del régimen de responsabilidad objetiva previsto en la normativa de productos defectuosos a menos que sufran daños personales. Ello es cuestionable, pues no se ve por qué, si sufren otro tipo de daños causados por sistemas de IA, sus demandas habrán de basarse, como regla general, en la negligencia del posible responsable, con las dificultades probatorias que ello conlleva. Aunque la Propuesta de Directiva sobre responsabilidad IA pretende teóricamente facilitar la prueba al perjudicado que invoca un régimen de responsabilidad por culpa, como hemos visto, tiene un limitado ámbito de aplicación. Esto, unido a los requisitos necesarios para que proceda la exhibición de pruebas u opere la presunción de causalidad que establece, hacen dudar de que vaya a ser de mucha utilidad para la víctima que deba basar su demanda en las reglas generales de responsabilidad.

BIBLIOGRAFÍA

Ataz López, J. (2020). "Daños causados por las cosas: una nueva visión a raíz de la robótica y de la inteligencia artificial", *Working Paper,* núm. 4.

Atienza Navarro, M. L. (2023). "La responsabilidad civil por daños causados por inteligencia artificial. Estado de la cuestión", *Responsabilidad extracontractual e inteligencia artificial,* XXII Jornadas APDC, p. 9 (pdf impreso).

Atienza Navarro, M. L. (2023). "¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del

Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)", *InDret,* núm. 2.

Atienza Navarro, M. L. (2022). *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier.

Beluche Rincón, I. (2019). "La responsabilidad del empresario por hecho de sus dependientes", *Practicum Daños*.

Del Olmo, P. (2023). "Comentario al art. 1903 C.c.", *Comentarios del Código civil, Comentarios del Código civil,* Cañizares Laso (dir.), Tomo V, Tirant lo Blanch.

European Law Institute (2022). "Response of the European Law Institute to the European Commission's Public Consultation on civil Liability. Adapting Liability Rules to the Digital Age and Artificial Intelligence".

Evangelio Llorca, R. "Causalidad y responsabilidad civil por los daños causados por sistemas de inteligencia artificial: las presunciones de causalidad en las propuestas normativas de la UE", XXII Jornadas APDC (pdf impreso).

Expert Group on Liability and New Technologies (2019). "Liability for Artificial Intelligence and Other Emerging Digital Technologies".

Gil Membrado (2022). "Daños producidos por la IA: La opacidad del algoritmo y el efecto de caja negra", XXII Jornadas APDC, p. 16 (pdf impreso).

González Beluche, P. (2023). "La adaptación de la Directiva 85/374/CEE, de 24 de julio, en materia de responsabilidad por daños causados por productos defectuosos a la cuarta revolución industrial", *CDT*, octubre, Vol. 15, núm. 2.

Hacker, P. (2023). "The European AI Liability Directives. Critique of a Half Hearted Approach and Lessons for the Future", *Working Paper*, version 28-3-2023.

Martín Casals, M. (2023). "Las propuestas de la UE para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial", *Indret,* núm. 2.

Navas Navarro, S. (2022). *Daños ocasionados por sistemas de inteligencia artificial. Especial atención futura regulación,* Comares, Granada.

Navas Navarro, S. (2022). "Régimen europeo en ciernes en materia de responsabilidad derivada de los Sistemas de Inteligencia Artificial", *Revista Cesco,* núm. 44.

Platero Alcón, A. (2021). "Breves notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix", *Ius et Scientia,* Vol. 7, núm. 1.

Santos Morón, M. J. (2022). "La responsabilidad por daños causados por productos defectuosos", *Derecho de consumo. Visión normativa y jurisprudencial actual,* Tecnos.

Santos Morón, M. J. (2017). "La imputación de responsabilidad médica con base en las normas de protección de consumidores: el art. 148 TRLC", ADC, 2017-I.

Spindler, G. (2023). "Different approaches for liability of Artificial Inteligence - Pros and Cons", *Liability for AI,* Lohsse, Schulze y Staudenmayer (eds.), Nomos, p. 44.

Wenderhost (2023). "Product Liability or Operator Liability for AI- What is the Best Way Forward?", Lohsse, Schulze y Staudenmayer (eds.), *Liability for IA,* Nomos.

Tercera Parte

ESTUDIOS SOBRE ALGORITMOS Y BIG DATA

Capítulo 7
EL USO DE ALGORITMOS POR LAS ADMINISTRACIONES PÚBLICAS

Alejandro Huergo Lora
Catedrático de Derecho Administrativo
Universidad de Oviedo
https://orcid.org/0000-0003-3159-7981

1. INTRODUCCIÓN

Partiendo del convencional concepto de los "algoritmos", vamos a desarrollar a continuación un panorama del uso de la inteligencia artificial por las Administraciones Públicas y un esbozo de lo que debería ser –y, en parte, ya es– su régimen jurídico[1]. Las Administraciones Públicas tienen una especial vinculación al ordenamiento jurídico (sometimiento pleno a la Ley y al Derecho, en los términos del artículo 103.1 de la Constitución) y afectan, de manera unilateral y vinculante, a los derechos de los ciudadanos, por lo que su utilización de medios tecnológicos como la inteligencia artificial plantea exigencias adicionales.

2. DE QUÉ HABLAMOS CUANDO HABLAMOS DE ALGORITMOS

2.1. Los "algoritmos" y su limitada utilidad como concepto jurídico

En el lenguaje común, los "algoritmos" van unidos a la inteligencia artificial[2]. El "algoritmo" sería el razonamiento que toma las decisiones cuando se utilizan instrumentos de inteligencia artificial. A veces incluso se les da nombre, como el

---

[1] Este trabajo se enmarca en el proyecto de investigación PID2021-126881OB-I00, financiado por el Ministerio de Ciencia e Innovación y titulado "Herramientas algorítmicas para ciudadanos y administraciones públicas".

[2] Así se comprueba en titulares como: "Cuando un algoritmo decide si tu startup obtiene financiación", "Un algoritmo decide lo que pagarás por un producto", "Policía predictiva: cuando el que decide es un algoritmo", "Su ascenso lo decide un algoritmo", etc.

algoritmo "Max", que utiliza el Ministerio de Trabajo para sus inspecciones, o el algoritmo "Frank", que utilizaba Deliveroo para asignar trabajo a sus *riders* y que dio lugar a una famosa sentencia de un tribunal laboral de Bolonia (de 31 de diciembre de 2020).

El Reglamento de Inteligencia Artificial no utiliza la palabra "algoritmo" en su articulado. Hay varias menciones en el preámbulo y una en su Anexo IV, en la que se dice que la documentación técnica que es necesario aportar en los sistemas de inteligencia artificial de alto riesgo debe incluir "[u]na descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo, incluidos (...) las especificaciones de diseño del sistema, a saber, la lógica general del sistema de IA *y de los algoritmos*". Los algoritmos no son, por tanto, un concepto jurídico relevante en el Reglamento, sino un elemento más de los sistemas de inteligencia artificial.

El diccionario de la RAE define algoritmo como "[c]onjunto ordenado y finito de operaciones que permite hallar la solución de un problema". Como he escrito en otro lugar, "[e]n todo caso, el origen inmediato de la palabra "algoritmo" es la inglesa *algorithm*, que hace referencia a cualquier procedimiento formalizado en una serie de pasos para solucionar un problema o conseguir un resultado. Aunque puede haber (y hay) algoritmos al margen de los ordenadores, es decir, algoritmos no gestionados por ordenadores, lo cierto es que la palabra algoritmo se ha desarrollado (y ha llegado a la lengua castellana) en relación con la informática, pues los ordenadores necesitan ser programados y un programa de ordenador consiste, precisamente, en una sucesión ordenada de pasos que el ordenador ha de llevar a cabo. Los seres humanos pueden actuar mediante algoritmos o no; los ordenadores sólo pueden funcionar siguiendo un algoritmo"[3].

La inteligencia artificial, como todo procedimiento o instrumento informático, utiliza algoritmos, pero no todos los algoritmos tienen que ver con la inteligencia artificial. Un procedimiento en el que se describen los distintos pasos para llegar a un determinado resultado es un algoritmo (hasta una receta de cocina puede serlo). Con frecuencia, esos algoritmos son "árboles de decisiones", en el sentido de que, en ciertos pasos, recogen distintas opciones en función del

---

[3] Huergo Lora, A., "Una aproximación a los algoritmos desde el Derecho administrativo", en Huergo Lora, A. (dir.), Díaz González, G. M. (coord.). (2020). *La regulación de los algoritmos*, Aranzadi, Cizur Menor, pp. 23-87, p. 27.

resultado del paso anterior. Por ejemplo, un algoritmo que explique cómo realizar la declaración del IRPF puede indicar como primer paso saber si el contribuyente ha residido 183 días en España el año anterior, y partir de ahí se bifurca entre la declaración del IRPF para residentes y para no residentes.

En la jurisprudencia se habla con frecuencia de algoritmos. A veces se trata de baremos que se utilizan para ponderar de una forma organizada y predeterminada los distintos factores que pueden influir en un determinado proceso y emitir un juicio objetivo acerca de su causa[4]. También se habla de ellos en la legislación, normalmente para referirse a fórmulas que se utilizan en la toma de decisiones. A veces el algoritmo se establece en la propia norma, cuando esta especifica la fórmula que debe aplicarse para llegar al resultado final: por ejemplo, en revisiones de precios (contratos), actualizaciones de tarifas (concesiones) o, con frecuencia, para la distribución de recursos escasos (ponderación de notas y otros méritos para la asignación de becas, por ejemplo) y a veces en la norma se establecen obligaciones de transparencia relativas al algoritmo[5].

Desde este punto de vista, los algoritmos son un modo de codificar la toma de decisiones, ordenando los factores que van a tenerse en cuenta. El algoritmo facilita la objetividad y la despersonalización en esa toma de decisiones, además de reducir el riesgo de errores. Obviamente, ese automatismo en la toma de decisiones también tiene sus inconvenientes: si se desliza un error en el algoritmo

---

[4] Por ejemplo, en asuntos de responsabilidad patrimonial se habla de "algoritmos" para aplicar la *lex artis* y determinar la causa de un determinado fenómeno (es decir, si es imputable a la Administración). Los algoritmos serían una forma de esquematizar los conocimientos sobre esa materia y de aplicarlos de manera uniforme y previa aceptada en la comunidad científica (porque el algoritmo suele estar previamente publicado o aprobado). Un ejemplo, en la sentencia de la Sala de lo Contencioso-Administrativo de Valladolid de 8 de febrero de 2024 (sentencia 114/2024).

[5] La Ley 3/2023, de 28 de febrero, de Empleo, en su artículo 17, se refiere a las herramientas informáticas que, a partir de la información contenida en el Sistema Público de Información de los Servicios de Empleo, pueden generar decisiones y recomendaciones que sean facilitadas a los demandantes de empleo.

El apartado 4 dice que "[e]l conjunto de instrucciones que compondrán el algoritmo subyacente a las decisiones y recomendaciones basadas en el análisis de datos y las evidencias estadísticas, de conformidad con los criterios expresados en este artículo, se desarrollarán reglamentariamente".

Por su parte, el Real Decreto 813/2023, de 8 de noviembre, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión, en su artículo 152, menciona, entre la información que es obligatorio suministrar en ciertos casos, "en su caso, el hecho de que un algoritmo informático haya sido responsable de la decisión de inversión y de la ejecución de la operación".

(por ejemplo, se olvida tener en cuenta un factor relevante), los efectos del error se multiplican y son mucho más graves que cuando se produce una equivocación al tomar una decisión individual. En segundo lugar, la "algoritmización" de las decisiones puede reducir la capacidad para reaccionar ante nuevas circunstancias que no fueron tenidas en cuenta al elaborar el algoritmo.

En todo caso, el concepto de algoritmo es poco útil jurídicamente, porque hay muchos tipos de algoritmos. El algoritmo puede estar en la norma y, en ese sentido, sólo es un modo más de expresar sus contenidos normativos. El algoritmo puede ser una forma de traducir la norma para que se aplique con apoyo informático, y en ese caso no innova nada (lo veremos en el epígrafe siguiente). Y puede ser algo creado al margen de las normas (por ejemplo, con inteligencia artificial, aunque no sólo) para tomar decisiones en ejercicio de los poderes otorgados o reconocidos –y, a la vez, limitados y regulados– por las normas. Por tanto, no tiene sentido o no es útil un régimen jurídico de los algoritmos, porque el núcleo común a todos ellos es mínimo[6].

2.2. Apoyos informáticos para aplicar normas

Con frecuencia, se utilizan aplicaciones informáticas para elaborar decisiones cuyo contenido viene predeterminado por el marco normativo (decisiones regladas). El objetivo es mejorar la eficiencia, consiguiendo que se dicten más decisiones, más rápidamente y con menos errores sin aumentar los recursos humanos que, en el caso de la Administración, son difíciles de incrementar. Hablamos de actividad administrativa reglada y de aplicaciones informáticas

---

[6] Sobre la cuestión de la "naturaleza jurídica de los algoritmos" se ha producido un debate en nuestra doctrina, a partir del trabajo pionero de Boix Palop, A. "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones", *Revista de Derecho Púbico: Teoría y Método*, núm. 1, 2020, pp. 223-270. En el trabajo antes citado, pp. 64-68, he defendido la opinión contraria. También se han pronunciado, entre otros, Arroyo Jiménez, L. "Algoritmos y reglamentos" (entrada del blog Almacén de Derecho, 25 de febrero de 2020) o Berning Prieto, A. "La naturaleza jurídica de los algoritmos", en Gamero Casado, E. (dir.); Pérez Guerrero, F. L. (coord.). (2023). *Inteligencia artificial y sector público: retos, límites y medios*, Tirant, Valencia, pp. 95-130. En mi opinión, y como ya he expresado, los algoritmos no son reglamentos porque los hay de muy diferentes tipos (por lo que no todos tendrían la misma naturaleza jurídica). Salvo los algoritmos que forman parten de normas (que ya están sometidos a las reglas de éstas), los demás no cumplen los requisitos de los reglamentos ni les es exigible, porque su función no es crear normas.

en las que se vuelca el marco jurídico de la decisión en cuestión. Si no se trata de actividad reglada, sino que existe un margen de decisión no agotado por la norma, entonces un instrumento informático que se limita a codificar la norma es insuficiente para la toma de la decisión y se requiere una decisión humana. Es una intervención informática que muchas veces resulta *invisible* (porque el destinatario de la decisión no sabe que se ha elaborado con una aplicación informática) y (jurídicamente) *irrelevante*.

La clave es que, cuando se trata de actuaciones administrativas individuales en las que se aplica la norma a un caso concreto (por ejemplo, cálculo del importe de un tributo o de una ayuda pública), para su control jurídico no se necesita conocer si se ha utilizado una aplicación informática y si la misma ha funcionado bien o mal, porque la legalidad de la decisión se deduce de su comparación con el marco normativo. Eso no significa que la aplicación informática no pueda producir sus propios problemas (básicamente, un error de programación conduce a la producción de decisiones ilegales). Pero no existe ningún elemento "autonomía" del sistema, que es un concepto utilizado por el Reglamento de Inteligencia Artificial (artículo 3, apartado 1): el modelo o sistema no aporta nada que no esté previamente en la norma.

Esta técnica de programación o robotización de la actividad administrativa opera en entornos de *actividad reglada*, en los que se puede crear un programa que recoja los parámetros normativos que guían a la Administración. El robot o la aplicación informática reproducen el hilo lógico que también debería seguir un operador humano y llegan al mismo resultado al que este tendría que llegar. El programador no introduce ninguna innovación (salvo que cometa un error, cuya consecuencia será que se dicten decisiones sistemáticamente ilegales por no ajustarse al marco normativo). Con frecuencia, el verdadero problema está en la calificación de los hechos a la hora de introducirlos en el modelo y, en la medida en que aquí hay factores que requieren una decisión o una apreciación, esta vuelve a quedar en manos de un operador humano (así sucede, por ejemplo, en el caso de las decisiones de seguridad social).

La utilización de estas técnicas parece totalmente recomendable. Más bien habría que preguntarse si tiene sentido que, estando disponibles estos apoyos, un operador humano emplee su tiempo en preparar decisiones tan sencillas. Parece casi obligatorio hacer uso de la tecnología para acelerar este tipo de decisiones administrativas, de forma que el operador humano se ocupe de vigilar el

funcionamiento de la aplicación, facilitar el acceso de la misma a los ciudadanos o facilitar la comprensión de sus resultados. Todo ello, lógicamente, con las garantías adecuadas, incluida la posibilidad de obtener información o explicación humana sobre la solución elaborada por el sistema informático, así como también la previsión de mecanismos ágiles que permitan corregir sus posibles errores, que es previsible que se produzcan y que pueden tener más gravedad al multiplicarse automáticamente por el propio funcionamiento del sistema.

Otra cosa son las actuaciones complejas, en las que no podemos reproducir la aplicación de la norma (y controlar, por tanto, la decisión administrativa) sin comprobar el funcionamiento de la aplicación (el "algoritmo"). Es lo que sucede, por ejemplo, con sistemas de distribución de plazas (MIR, concursos de traslados de funcionarios) o incluso con las aplicaciones informáticas que realizan sorteos para determinar la composición de la comisión que decidirá un concurso. Aquí un concursante individual no puede saber qué plaza le habría tocado a él (porque depende de todo el proceso) y no es posible saber si el resultado arrojado por la aplicación es realmente aleatorio sin conocer cómo funciona. En estos casos, es decir, donde la aplicación informática –aun estando obligada a seguir estrictamente los parámetros normativos, sin poder añadir nada– es uno de los elementos que contribuye a determinar el producto jurídico-administrativo, es necesario un acceso suficiente a la misma, para comprobar si se ajusta al marco normativo o no, si ha funcionado bien. Es algo que se desprende de la normativa vigente, porque forma parte del expediente administrativo. Para que ese control pueda producirse es imprescindible, naturalmente, saber que se ha utilizado un sistema de este tipo.

El test es sencillo: en la informatización o automatización "simple", la decisión administrativa no necesita citar la aplicación informática, ni siquiera como antecedente. En cambio, en los otros casos sí.

2.3. Instrumentos para tomar decisiones

Se puede dar un paso más, que es el uso de inteligencia artificial para producir decisiones (utilizando, entre otros instrumentos técnicos, algoritmos). En este caso, la inteligencia artificial no se limita a aplicar las normas para elaborar decisiones regladas, sino que ayuda a quienes disponen de un margen de actuación que les permite optar entre unas y otras decisiones, a tomar una concreta decisión que se perfila como más adecuada desde algún punto de vista. Existe, por tanto,

una diferencia neta con el supuesto anterior: no se trata de aplicar la norma para producir, sin errores, la única decisión posible de acuerdo con la norma, sino que se trata de elaborar una decisión, lo que supone que la norma deja un margen de actuación con varias decisiones posibles, margen que el sujeto llamado a decidir prefiere ejercer en el sentido que le recomienda un modelo o sistema de inteligencia artificial o al menos utilizándolo como un elemento de apoyo más.

La manifestación más conocida de la inteligencia artificial son las predicciones algorítmicas, muchas veces relacionadas con el perfilado. En definitiva, se trata intentar responder a una pregunta analizando los datos del pasado (cómo sucedieron las mismas cosas de las que ahora intentamos saber cómo van a ocurrir), para encontrar en esos datos correlaciones (rasgos que se registraron con más frecuencia en aquellos casos en que sucedió lo que estamos intentando prever) y fabricar, de esa forma, una especie de retrato robot que podemos tomar como base para futuras decisiones administrativas. Es muy importante darse cuenta de que la utilización de estos modelos supone, a veces, sustituir una actuación administrativa *uniforme* (tratar a todos igual, hacer muestreos aleatorios) por una actuación *personalizada* (así sucede, por ejemplo, con las "carpetas ciudadanas" que sirven para suministrar informaciones personalizadas a los ciudadanos, en función de lo que se supone que les puede interesar) y, en otros casos, sustituye a la toma de decisiones basadas en criterios subjetivos (como se hace cuando se inspecciona a quienes parece que tienen mayor perfil de riesgo, en lugar de elegir los objetivos al azar o según la iniciativa del órgano competente). La inteligencia artificial promete eficiencia (al sector privado ya se la ha dado), en el sentido de que, en la actuación tradicional, se lanzan al viento muchas semillas y sólo germinan unas pocas, mientras que la inteligencia artificial permitiría identificar cuáles son las que van a germinar, de forma que sólo se planten esas. Por otro lado, también es importante retener que la inteligencia artificial suele ser aproximativa (ayuda a reducir la incertidumbre inicial, a pasar de 100 a 10), no dirigida a tomar decisiones definitivas y cerradas, para las que suele ser necesaria la intervención humana y la confrontación con datos reales, no sólo con predicciones[7].

---

[7] Por utilizar un símil minero, la inteligencia artificial es muy útil en la fase de "exploración" e "investigación" de los recursos, porque permite concentrarse rápidamente en un ámbito concreto, pero no suele permitir pasar directamente a la de "explotación", porque hacen falta comprobaciones adicionales.

Otro campo, relacionado con el anterior, porque también se basa en predicciones, es el de los "modelos de inteligencia artificial de uso general" (expresión utilizada finalmente por el Reglamento de Inteligencia Artificial) o "grandes modelos de lenguaje" –*large language models*– (GPT, Gemini, etc.). Pueden tener (a qué negarlo) un uso instrumental en el acceso y organización de la información, como lo tienen los buscadores, que son un instrumento mucho más conocido. En todo caso, aunque el modelo responda a una pregunta y nos ofrezca un texto similar al que pudiera elaborar un operador humano (o incluso, según los casos, mejor), el camino seguido es distinto. El modelo de inteligencia artificial generativa "sólo" intenta predecir cuál es la respuesta que es más probable que se dé en la práctica a la pregunta formulada, a la vista de la información acumulada que se ha utilizado para elaborar y entrenar el sistema.

En todos estos casos, el modelo informático influye sobre el contenido de la decisión administrativa (algo que no sucede en el caso anterior, en el que no añade nada al resultado que, en todo caso, es decir, "a mano o a máquina", arrojaría en todo caso la aplicación del marco normativo). En la medida en que se utilice un modelo predictivo o cualquier otro sistema de inteligencia artificial para *justificar* una decisión que produzca efectos jurídicos, el control de dicha decisión (control que es imprescindible en un Estado de Derecho, en virtud, entre otras cosas, del derecho fundamental a la tutela judicial efectiva), incluirá un control acerca de si el sistema ha funcionado correctamente (es decir, si ha funcionado de acuerdo con sus objetivos) y de si su diseño es correcto, es decir, si los criterios que se le ha pedido que busque suponen una traslación o traducción adecuada del concepto jurídico que se está aplicando.

En definitiva, una cosa es utilizar un modelo informático para *elaborar* una decisión y otra cosa es utilizarlo para *justificarla*. El grado de visibilidad, relevancia jurídica y exigencias no puede ser el mismo en un caso y en otro. Sobre ello voy a insistir en los apartados siguientes.

2.4. Actividad administrativa automatizada

En el supuesto analizado en el epígrafe 2.1, un sistema informático en cuya programación se ha incorporado o "volcado" la normativa reguladora de un determinado asunto (por ejemplo, la que regula quién tiene derecho a una pensión de jubilación o cuál es la cuantía de esta) aplica la norma a los casos concretos y dice qué contenido debería tener la decisión que debe tomar un determinado

órgano administrativo. Ello no significa que la decisión se tome de forma automatizada, si entendemos como decisión administrativa automatizada la que responde a la definición del artículo 41.1 de la Ley 40/2015, de Régimen Jurídico del Sector Público: "cualquier acto o actuación *realizada íntegramente a través de medios electrónicos* por una Administración Pública en el marco de un procedimiento administrativo y *en la que no haya intervenido de forma directa un empleado público*". En la mayoría de los casos, un operador humano es quien "firma" la decisión, utilizando los resultados que arroja el sistema informático, pero sin estar vinculado por él. Oficialmente, no estamos ante una decisión automatizada y el sistema informático permanece en un segundo plano. ¿Es esto realmente así?

Antes de que se regulara la inteligencia artificial, se reguló la actividad administrativa automatizada, entendida como aquella que se produce sin intervención humana[8]. Tanto la legislación nacional (en España, el ya citado artículo 41 de la Ley 40/2015; en Alemania, el parágrafo 35a de la Ley Federal de Procedimiento Administrativo; existe también regulación autonómica) como –para las decisiones automatizadas en general, no sólo administrativas– el RGPD (artículo 22) establecen una normativa para las decisiones automatizadas[9]. El artículo 22 del RGPD se ha convertido, de hecho, en la norma imperativa más relevante en el abordaje de la actividad automatizada y, por extensión, de la utilización práctica de la inteligencia artificial, debido, como vamos a ver a continuación, a la interpretación extensiva que se ha hecho del mismo[10].

---

[8] Siempre existe (también en la actividad automatizada) una intervención humana, sólo que se sustituye la intervención humana "artesanal" por una intervención previa y general de diseño y programación del sistema, después de la cual se coloca una "máquina", previamente programada, en el puesto del operador humano. A la actividad automatizada se refiere, de forma pionera, Martín Delgado, I. (2009). "Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada", *RAP*, 180, pp. 353-386.

[9] Sobre la aplicación de esta regulación a la iniciación de procedimientos sancionadores de forma automatizada, que actualmente está prevista en el ordenamiento español por normas de rango legal y reglamentario, Izquierdo Carrasco, M., "Actuaciones automatizadas en la sanción de irregularidades en el orden social", en Cotino Hueso, L. / Todolí Signes, A. (coord.) (2022). *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente*, Tirant, Valencia, pp. 261-288.

[10] El artículo 22.1 establece que "[t]odo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Las excepciones (apartado 2) son: que la decisión automatizada sea "necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento", que esté "autorizada por el

En la práctica, el artículo 22 RGPD condiciona la adopción de decisiones que: 1) estén basadas únicamente en el tratamiento automatizado de datos; y que, además, 2) produzcan efectos jurídicos sobre el interesado o le afecten significativamente de modo similar, a que estén autorizadas por Derecho de la Unión o de los Estados miembros (salvo que estén consentidas explícitamente por el interesado o son necesarias para el cumplimiento de un contrato) y a que esa habilitación normativa contenga medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Se trata de una regulación transversal, que afecta tanto a decisiones públicas como privadas. El artículo 22 (con el precedente del artículo 15 de la Directiva 95/46) viene a considerar que el hecho de que un tratamiento automatizado de datos dé lugar por sí solo (sin intervención humana, o sin intervención humana significativa) a una decisión, constituye en sí mismo una inmisión en la libertad del ciudadano, adicional a la que deriva del propio tratamiento, por lo que está sometido a requisitos específicos a los que se exigen al tratamiento, requisitos entre los que se incluye esa exigencia de una habilitación normativa para la toma de la decisión automatizada, habilitación que deberá establecer garantías, entre las que deberá incluirse "como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión".

No hay espacio para una exposición, ni siquiera resumida, de los problemas que plantean las actuaciones (en este caso, administrativas) automatizadas o para un comentario al artículo 22. Ciñéndonos al caso de las decisiones administrativas, parece indiscutible que es necesaria una habilitación normativa para que una decisión que legalmente está atribuida a un órgano administrativo (por ejemplo, un Alcalde) sea tomada por un sistema informático y llegue directamente, sin intervención humana, desde el sistema informático al buzón del ciudadano. Cuando la norma atribuye a un determinado órgano de la competencia para dictar un acto (que es algo que existe en todos los casos como habilitación normativa a la Administración), se supone, salvo que se indique lo contrario, la competencia se ejercerá de forma personal (es decir, humana) por

---

Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado" o que se base "en el consentimiento explícito del interesado". Sobre esta norma es fundamental la obra de Palma Ortigosa, A. (2022). *Decisiones automatizadas y protección de datos. Especial atención a los sistemas de inteligencia artificial*, Dykinson, Madrid.

ese órgano. Para que eso cambie (y, por tanto, para que un acto que en realidad deriva de un sistema informático se entienda como imputable o procedente de un determinado órgano administrativo), es necesario que una norma lo autorice y también es necesario que se establezcan garantías, incluida la cadena de legitimación y también algún tipo de garantía frente a posibles errores.

En la práctica, se está ensanchando el ámbito de aplicación del artículo 22, a través de una interpretación amplia tanto de lo que se entiende por decisión que produce efectos jurídicos, como de cuándo se entiende que la decisión está "basada únicamente en el tratamiento automatizado"[11]. Se tiende a aplicar este artículo a todo supuesto de empleo de inteligencia artificial (aunque no suponga automatización) y también a los casos de influencia "casi decisiva" del sistema sobre el operador humano (sesgo de automatización), aunque tampoco haya, en sentido estricto, automatización. Un hito relevante es la sentencia del TJUE en el asunto SCHUFA (sentencia de 7 de diciembre de 2023, asunto C-634/21), que, en el fallo, establece que el artículo 22 del RGPD "debe interpretarse en el sentido de que la generación automatizada, por una agencia de información comercial, de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de la capacidad de esta para hacer frente a compromisos de pago en el futuro constituye una «decisión individual automatizada», en el sentido de la mencionada disposición, cuando de ese valor de probabilidad dependa de manera determinante que un tercero, al que se comunica dicho valor, establezca, ejecute o ponga fin a una relación contractual con esa persona". En los párrafos 42-68 se analiza muy detenidamente la interpretación de los requisitos del artículo 22, destacando que "existiría un riesgo de elusión del artículo 22 del RGPD y, en consecuencia, una laguna en la protección jurídica, si se optara por una interpretación restrictiva de esta disposición según la cual la generación del valor de probabilidad debiera considerarse un mero acto preparatorio y solo el acto adoptado por el tercero pudiera, en su caso, calificarse de «decisión», en el sentido del artículo 22, apartado 1, de dicho Reglamento" (párrafo 61). El Tribunal entiende que no es necesario que la predicción automatizada sea la decisión final del banco (es decir, no sería necesario que estemos ante una "decisión automatizada" en sentido estricto), siendo suficiente que ejerza una influencia determinante sobre la decisión[12].

---

[11] Como desarrolla monográficamente Palma Ortigosa, pp. 63-65.

[12] Ese concepto (influencia "determinante") procede de la formulación de la cuestión prejudicial por el órgano judicial nacional, no del Tribunal.

Posiblemente, la automatización, con ser importante a la hora de categorizar un fenómeno y de establecer las necesidades que deben atenderse en su regulación, no sea tan decisivo como otras circunstancias (por ejemplo, que se utilice, o no, inteligencia artificial para determinar el contenido de la decisión administrativa). La aplicación extensiva del artículo 22 puede estar llevando a que se traten de forma igual fenómenos que son diferentes. Habrá que ver en qué medida la aplicación del Reglamento de Inteligencia Artificial cubre necesidades que ahora se abordan, a falta de otra norma, por el artículo 22.

3. POSIBLES USOS DE LA INTELIGENCIA ARTIFICIAL EN LA ACTIVIDAD ADMINISTRATIVA

3.1. Concreción de conceptos legales de tipo probabilístico o predictivos

Las predicciones algorítmicas pueden ser útiles para concretar conceptos legales de tipo probabilístico o predictivo, que son abundantes en la legislación administrativa. Por ejemplo, si uno de los requisitos necesarios para que la Administración pueda o deba tomar una determinada decisión es que se produzca una situación de "riesgo", que es un concepto predictivo y probabilístico, no parece haber ningún problema en que, en lugar o junto a otras técnicas que permitan verificar ese riesgo, se utilice un sistema de inteligencia artificial, un modelo predictivo basado en el análisis de datos pasados. Lo mismo, por ejemplo, para determinar si un área es inundable o si una fusión empresarial para producir una grave limitación de la competencia en el mercado.

Salvo que la norma diga otra cosa, no existe una lista tasada de tecnologías que permitan concretar los conceptos legales. De hecho, la regla de libertad de medios de prueba que se establece en el artículo 77.1 LPAC ("Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba admisible en Derecho, cuya valoración se realizará de acuerdo con los criterios establecidos en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil") cubre perfectamente la utilización de esta técnica, como de cualquier otra de las muchas que se usan en la práctica.

Cuando se enfatiza que los modelos predictivos son "cajas negras", en el sentido de que la complejidad de las "redes neuronales" o estructuras matemáticas que les sirven de base (el número de capas que contienen y de parámetros que se tienen en cuenta) impide recorrer de forma exhaustiva e integral el recorrido que lleva

desde los datos de entrada hasta la respuesta proporcionada por el modelo, tal vez no tenemos en cuenta cuál es la realidad de otros medios técnicos que se utilizan en la aplicación del Derecho administrativo o en la actividad administrativa en general. El fenómeno de la "caja negra" hace referencia a una limitación tecnológica, a un grado de incertidumbre residual que no puede evitarse. Pero también (por poner varios ejemplos) los modelos de predicción meteorológica o demoscópica tienen márgenes de error. Del mismo modo, los sistemas de geolocalización tienen limitaciones en su grado de exactitud, a veces buscados deliberadamente por razones de privacidad o seguridad. Igualmente, los modelos físicos que predicen la trayectoria de proyectiles tienen márgenes de incertidumbre. De eso estamos hablando, no de algo que sea exclusivo de los sistemas de inteligencia artificial.

La consecuencia jurídica que, en mi opinión, debe extraerse de ese fenómeno de la "caja negra" es no admitir el uso de ese medio de prueba cuando ese margen de error pueda ser relevante para la decisión. Si utilizo un modelo predictivo para decidir si llevo un paraguas al salir de casa o al hacer el equipaje (como hacemos con frecuencia al mirar la predicción meteorológica en el teléfono móvil), el hecho de que exista un margen de error del 10% es irrelevante, porque lo peor que puede pasar es que me moje o que cargue con un paraguas en vano, y en la mayoría de los casos el sistema me da un consejo acertado. Del mismo modo, si utilizo un sistema similar para decidir a quiénes inspecciono, un margen de error similar puede ser asumible, porque lo peor que puede pasar es que se inspeccione a alguien que no ha cometido ninguna infracción (inspeccionar no es sancionar; sencillamente, no se descubrirá ninguna infracción y no se iniciará ningún procedimiento sancionador)[13]. En cambio, si se utilizara un sistema de inteligencia artificial para dictar resoluciones con efectos jurídicos sobre terceros, y el asunto pudiera ser dudoso y depender de ese margen de error, no se podría utilizar ese medio porque llevaría a conclusiones no fiables.

En la aplicación de las normas (y, concretamente, en la concreción de conceptos indeterminados que estas utilizan) ya se emplean tecnologías que plantean

---

[13] Todo ello con la matización de que hay que estar atentos ante posibles discriminaciones (inspección sistemática de determinados colectivos). Pero esas posibles discriminaciones ya existen con los sistemas actuales, no han llegado, como a veces parece, con la inteligencia artificial. En todo caso, la sensibilidad demostrada hacia los abusos producidos con IA debe llevar a un salto de calidad en el control de estas actuaciones en general, y no a una disparidad de garantías en función de que se realicen con medios digitales o no.

problemas similares. Por ejemplo, en asuntos relativos a obras (ejecución de contratos de obras, responsabilidad patrimonial por accidentes, etc.) o en responsabilidad patrimonial en el ámbito sanitario, se utilizan con frecuencia, tanto en vía administrativa (y en la posterior contencioso-administrativa) como en la civil, técnicas y saberes que tienen parecidos márgenes de incertidumbre o cuyas conclusiones están sujetas a discusión en términos similares. Normalmente, esos conocimientos son incorporados a los procedimientos a través de informes periciales, frecuentemente varios que se oponen entre sí. Al final decide un lego (el juez, el titular del órgano administrativo) a partir de las explicaciones de los técnicos. En la práctica se produce una "tormenta perfecta" que hace que la decisión final (administrativa o judicial) se aleje bastante de una aproximación científica a la verdad. A lo que más se parece es al resultado de una batalla o de un enfrentamiento deportivo, que dependen de múltiples factores: la estrategia, la motivación de los contendientes o incluso el azar, y no sólo la fuerza o habilidad que teóricamente tienen los participantes. Con frecuencia, la convicción final de quien decide (órgano administrativo o judicial) está condicionada o determinada por las explicaciones que ofrecen los distintos peritos, enfrentados en un interrogatorio siempre limitado en el tiempo, lo que arroja varios problemas: desde la desigual elocuencia de los peritos (que a veces tiene más importancia que la solidez de sus tesis) al hecho de que pueden hacer afirmaciones carentes de fundamento, pero que pueden calar si no son adecuadamente desenmascaradas (lo que a veces es sencillamente imposible por la propia ordenación procesal de los tiempos y los turnos de intervención). Esta elemental constatación de la realidad hace que las habituales lamentaciones sobre los límites de los modelos predictivos y de su explicabilidad pierdan, una vez puestas en contexto, buena parte de su fuerza.

3.2. Decisiones aproximativas o preparatorias

Los sistemas de inteligencia artificial pueden utilizarse, como hemos visto, para concretar conceptos probabilísticos, por ejemplo, para demostrar que existe una situación de "riesgo" (cuando este sea el presupuesto que permite adoptar una determinada decisión) o que se va a producir una reducción de la competencia en un sector (hecho que es relevante para autorizar, o no, una fusión). También puede utilizarse, por ejemplo, en la elaboración y justificación de un plan urbanístico o de una norma reglamentaria.

Pero puede suceder, y es lo más frecuente, que esas técnicas se utilicen para tomar otra clase de decisiones o para realizar otras actuaciones, y estoy pensando

sobre todo en dos posibilidades. En primer lugar, actuaciones materiales, típicas en la actividad prestacional: asignar prioridades en la atención, incluir a personas en un concreto procedimiento, realizar un diagnóstico, etc. En segundo lugar, y ya en el campo de la actividad jurídica, actuaciones de carácter preparatorio o incluso provisional: distribuir los recursos materiales o humanos que van a dedicarse a esa actuación (refuerzos en uno u otro lugar) o identificar objetivos para la inspección.

En el campo de la actuación material o prestacional, y sin entrar ahora ni siquiera a resumir todo un sector del Derecho administrativo, hablamos de actuaciones que normalmente no están formalizadas en un procedimiento administrativo dirigido a la producción de un acto administrativo. Eso no quiere decir que carezcan de relevancia jurídica: pueden tenerla por la vía de la responsabilidad patrimonial e incluso pueden formalizarse o convertirse en contenciosas cuando el ciudadano presenta una reclamación[14]. Algunas de estas actuaciones en las que se utiliza la inteligencia artificial ni siquiera se refieren directamente a ciudadanos concretos, como, por ejemplo, cuando se utiliza para la asignación de recursos (en qué oficinas se va a situar más personal, por ejemplo, a partir de las necesidades predichas por un modelo informático). En el campo de los procedimientos administrativos, hablamos normalmente de actos de trámite, que, debido a que no producen efectos jurídicos directos sobre los ciudadanos y que son preparatorios, están sometidos a un control o programación normativos muy ligeros (no es una afirmación subjetiva, es lo que se deriva de que no se admita la impugnación autónoma de los actos de trámite no cualificados). Decisiones en las que la Administración tiene un margen de maniobra amplio, calificado o no de discrecionalidad (puesto que esta categoría suele reservarse para las resoluciones o actos finalizadores del procedimiento).

---

[14] Una referencia importante es la sentencia de 16 de diciembre de 2021 del Tribunal Constitucional Federal alemán (Sala Primera) que, en el contexto de la pandemia, estimó un recurso de amparo y estableció que, en aquellos casos en que tratamientos médicos necesarios o importantes para la vida (respiradores, por ejemplo) no estén disponibles para todos, los criterios para su asignación deben estar establecidos por Ley. Normalmente, los modelos de inteligencia artificial no se aplican para tomar estas decisiones, sino para otras previas o aproximativas, como decidir a quiénes se aplica un determinado medio de *detección* (no de tratamiento), para evitar tener que aplicarlo de forma indiscriminada, o bien a la hora de interpretar los resultados de los medios de detección.

Es fácil estar de acuerdo en que la utilización de medios tecnológicos no puede suponer en absoluto un paso atrás en el control y en las garantías de la actuación administrativa. Pero, ¿deben establecerse más garantías o más controles, más desconfianza, en suma, sólo por el hecho de que se haya actuado "digitalmente"? Cuando la tecnología se utiliza para "justificar" la decisión, desde luego que es necesario someter a control esa tecnología (como ya se hace actualmente con cualquier otra), pero, ¿tiene sentido que una tecnología esté prohibida o se le exijan unos elevados requisitos sólo por el hecho de que puedan producirse en su aplicación errores que no tienen consecuencias cuando los comete un operador humano?[15]. Sería necesario, en todo caso, repensar los niveles de exigencia para ese tipo de decisiones en general, no sólo cuando en su elaboración se utiliza la IA.

3.3. ¿Resoluciones o normas elaboradas mediante inteligencia artificial?

¿Tiene sentido utilizar sistemas de inteligencia artificial para tomar decisiones públicas, más allá de estos dos supuestos analizados, es decir, la concreción de conceptos de tipo probabilístico y la preparación de decisiones preparatorias o aproximativas? En mi opinión, es muy discutible, porque, fuera de esos dos casos concretos, las decisiones públicas deben basarse, porque así lo impone su correspondiente programación normativa, en un determinado hilo argumental que no puede ser replicado por la inteligencia artificial salvo que admitamos la sustitución de ese hilo argumental por un equivalente o alternativo algorítmico que, en realidad, supone incumplir la programación normativa.

De nuevo acudo, para apoyar esta afirmación, a las normas atributivas de potestades (como se ha hecho previamente para admitir la utilización de programas

---

[15] Es significa la sentencia de 19 de febrero de 2020 (recurso de casación 240/2018). Un contribuyente que fue inspeccionado y sancionado impugna los actos administrativos porque sostiene que, al no encontrarse entre los objetivos señalados en el plan de inspección, no debería haber sido inspeccionado. El TS entiende que ese posible incumplimiento del plan de inspección es irrelevante, lo importante es que se detecten hechos constitutivos de infracción tributaria: "La introducción de los planes de actuación, de control, parciales, pueden tener la finalidad de facilitar a la Administración Tributaria su funcionamiento, especialmente mediante la aplicación de programas informáticos que permitan un tratamiento más ágil de la fiscalización de un determinado sector de contribuyentes, pero su previsión, quizá no muy acertada, en normas legales y reglamentarias, no puede traducirse sin más en un derecho subjetivo del contribuyente a no ser investigado si no se encuentra incluido en dichos planes y programas, pues ello supondría el incumplimiento por parte de la Administración del deber de fiscalización de que todos los ciudadanos cumplan con el deber de contribuir, previsto en el artículo 31.1 de nuestra norma constitucional".

que ayuden a elaborar decisiones regladas y para admitir el uso de inteligencia artificial para elaborar y justificar decisiones en las que se concreten conceptos normativos de tipo probabilístico, como el de riesgo, o se hará para exigir base normativa para la actuación automatizada).

Las normas atributivas de potestades (que forman esa programación normativa de la Administración) suelen establecer un supuesto de hecho y también la decisión o decisiones que la Administración puede tomar cuando el mismo se verifique. Partimos de la base de que el supuesto de hecho no es probabilístico (pues en ese caso nos encontraríamos en el supuesto ya estudiado previamente), sino que se trata de un hecho que es necesario verificar. Resulta difícil aplicar aquí un sistema de inteligencia artificial, porque este acredita probabilidades, no hechos. Todo lo más, puede aplicarse para probar o acreditar indicios, que, como es sabido, pueden servir como prueba en algunos casos[16]. Probar hechos no es lo mismo que acreditar probabilidades. Por eso, lo normal es que la inteligencia artificial se utilice para aproximarse, para saber dónde y cuándo iniciar un procedimiento, pero que la decisión final se tome posteriormente sin inteligencia artificial, en función de hechos probados.

Si pasamos a la segunda parte de la norma habilitante de la potestad, es decir, la que especifica qué decisión puede o debe tomar la Administración ante la constatación del presupuesto de hecho, la Administración tiene que razonar por qué elige, de entre todos los posibles, un determinado contenido para la decisión. Si no hay margen decisional, se tratará de decisiones regladas, en las que tendrá cabida otro tipo de apoyo tecnológico ya analizado previamente. Pues bien, el razonamiento "valorativo", que es el que se lleva a cabo para justificar la elección, es totalmente ajeno al ámbito de la inteligencia artificial. Por ejemplo, una vez constatado el riesgo de contagio de Covid, una comunidad autónoma decide imponer restricciones a la actividad hostelera para reducir los contagios y otra opta, en cambio, por lo contrario (libertad de horarios y aforos) porque entiende que el riesgo es asumible, que también se van a producir contagios en otros ámbitos —aunque se cierre la hostelería— y que un parón de la actividad económica es igualmente indeseable y dañino. Son ejemplos reales, como todos sabemos. ¿Qué papel puede jugar aquí

---

[16] Como he intentado explicar en "Inteligencia artificial y sanciones administrativas", en Rebollo Puig, M., Huergo Lora, A., Guillén Caramés, J., Cano Campos, T. (dir.). (2022). *Anuario del Derecho Administrativo Sancionador (2022)*, Civitas, Cizur Menor, pp. 275-309.

la inteligencia artificial? A mi juicio, ninguno, salvo el de verificador de hipótesis: cuantificar el riesgo de contagio, cuantificar los daños que sufriría la economía con una reducción de la actividad hostelera, etc. Pero, en la medida en que haya juicios de valor o preferencias entre intereses enfrentados entre sí, no veo cómo podrá sustituirse el juicio humano (la preferencia humana) por un juicio informático. Una vez que alguien decida (valorativamente) una opción (por ejemplo, minimizar el riesgo de contagio, al precio que sea), se podrá convertir esa decisión en una función matemática y utilizar tecnología (incluidos modelos de inteligencia artificial) para calcularla, pero hay un paso previo (valorativo, decisional) que es necesariamente humano, no ya por razones legales, sino puramente estructurales[17].

3.4. Inteligencia artificial generativa

A pesar de lo que se ha sostenido hace un momento, alguien podría decir que también se puede redactar una resolución judicial o administrativa con inteligencia artificial generativa (me refiero a los *large language models*, tipo Gemini o GPT). Sin embargo, a mi modo de ver tampoco aquí se produciría ningún cambio, porque la decisión valdría porque detrás de ella hay un operador humano (que es el que ha decidido utilizar el modelo de inteligencia artificial) que hace suyo ese texto, y no porque este tenga esa procedencia tecnológica.

Es importante distinguir entre el uso de la inteligencia artificial para "justificar" o motivar decisiones jurídicas, y su uso para elaborar decisiones. Aunque sea banal, hemos visto con frecuencia noticias que hablan de "demandas escritas con ChatGPT" y lo mismo podemos decir de sentencias o incluso, recientemente, de leyes. ¿Qué decir en estos casos, además de subrayar un evidente uso propagandístico, por un lado, en favor de una determinada aplicación informática que está en el mercado y compite con otras, y, por otro lado, como forma de que un determinado operador jurídico (despacho de abogados) obtenga notoriedad, algo que en

---

[17] Este análisis se basa en la estructura de las decisiones públicas y de los sistemas de inteligencia artificial, y es por tanto independiente de la construcción de una "reserva de humanidad" como postulado ético y jurídico, como han desarrollado Poncé Solé, J., "Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana", Gamero Casado, E. (dir.), Pérez Guerrero, F. L. (coord.). (2023). *Inteligencia artificial y sector público: retos, límites y medios*, Tirant, Valencia, pp. 195-225 y Gallone, G. (2023). *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Wolter Kluwer CEDAM, Milano.

estos momentos se consigue, con frecuencia, incluyendo la expresión "inteligencia artificial" en cualquier noticia?[18]. Para empezar, conviene destacar las dudas sobre la fiabilidad de estos sistemas, que los convierten en una buena herramienta para acceder a información que ya se conoce, pero no tan buena como forma de investigar sobre un tema que no se conoce[19]. Del mismo modo que antes hemos visto que los modelos de inteligencia artificial pueden ser útiles como aproximación, más que para tomar una decisión definitiva que afecte a personas concretas (o, por poner otro ejempo, que un equipo deportivo muy económico puede ser más que suficiente para una excursión de senderismo, pero tal vez no para una expedición más exigente), cuando hablamos de tomar decisiones importantes, la información que proporcionan estos sistemas no resulta fiable (y, si es necesario comprobarla sistemáticamente, puede ser poco eficiente utilizarlos).

En todo caso, imaginemos que el titular de un órgano administrativo utiliza un modelo (recordemos que no existe sólo uno) para elaborar el texto de una resolución administrativa. Como las decisiones suelen basarse en informes técnicos, que constituyen su motivación, lo más probable sería que un técnico utilizara el modelo para preparar el informe. Para ello, haría la correspondiente "pregunta" o "prompt" al modelo, suministrándole unos parámetros o datos para que este cree un texto. ¿Qué supone eso desde el punto de vista jurídico? En mi opinión, prácticamente nada.

En la situación que estoy planteando, el técnico o el titular del órgano administrativo "enfocan" el asunto, seleccionando un determinado marco (y unas fuentes) para su solución, y piden a un modelo de inteligencia artificial que redacte el texto. O bien se inclinan, en virtud de un juicio personal, por una u otra de las soluciones en presencia (legalizar una determinada construcción o bien considerarla ilegalizable), y encargan la redacción del texto a un sistema de inteligencia artificial, del mismo modo que, antes de la aparición de estos modelos, podía encargarse la redacción

---

[18] Baste pensar en lo que sucede en un entorno muy sometido a la competencia y en el que se busca continuamente la publicidad y la notoriedad, como es el de los despachos de abogados, sobre todo en la abogacía "de negocios". Tan pronto se destacan –con razón– los ciber-riesgos, que llevan a adoptar precauciones muy rigurosas (algo razonable), como se publicita la utilización de inteligencia artificial, incluida la generativa, a pesar de sus problemas de fiabilidad e incluso de seguridad.

[19] Como explica la reciente (12 de diciembre de 2023) y bastante razonable guía sobre inteligencia artificial para jueces y magistrados aprobada en el Reino Unido.

a una persona del equipo. ¿Podemos decir que "la decisión la ha tomado un modelo de inteligencia artificial"? Evidentemente, no, aunque de él proceda el texto.

Profundizando en el análisis, diríamos que hay tres elementos o fases. El primero es la toma de la decisión, que es un proceso puramente personal del titular del órgano (o, en muchos casos, del técnico que elabora el informe, cuyo criterio va a ser seguido por el órgano que toma la decisión). Ese proceso decisional tiene un margen de maniobra, de holgura, en el sentido de que se puede optar por la decisión A o por la decisión B, siendo ambas jurídicamente admisibles siempre que se justifiquen adecuadamente (algo que no es imposible ni difícil). En unos casos hablamos de potestad discrecional, otras veces de margen de apreciación y en otros casos ni siquiera se formaliza la calificación con tanta precisión porque no se trata de resoluciones en sentido estricto, sino de actos de trámite o incluso de decisiones ajenas a un procedimiento administrativo, pero el hecho cierto es que existe ese margen y que la opción la toma el operador humano en un proceso subjetivo.

¿Qué factores son los que "pesan más" en ese proceso subjetivo? Es imposible saberlo: el intelecto humano es una auténtica "caja negra" mucho más difícil de descifrar que cualquier sistema de inteligencia artificial. Pueden ser decisivas consideraciones jurídicas (que después aparecerán en la motivación de la decisión): el operador puede sentirse vinculado (siguiendo el ejemplo de las restricciones por el Covid) por la protección de la salud, o, en sentido contrario, por la necesidad de limitar al máximo las restricciones a la actividad económica, pero también pueden entrar en juego muchos otros factores, incluidos los de tipo político (favorecer a unos determinados responsables políticos o erosionarlos), ideológico, de carrera, etc. Por supuesto que en algunos casos podríamos hablar de auténtica desviación de poder, pero es casi imposible demostrarla ni siquiera indiciariamente. Y también es cierto que algunas técnicas organizativas (de selección de personal) pueden, al incidir sobre el sistema de incentivos, favorecer o perjudicar que las decisiones se tomen por razones más "alineadas" con los intereses públicos, pero lo cierto es que, en mayor o menor intensidad, la decisión se toma al margen de su justificación, que es un elemento posterior. En todo caso, lo que me parece clave es que se pueden justificar jurídicamente distintas decisiones (no sólo una), de modo que la toma de la decisión no se explica por razones jurídicas (que las hay para justificar distintas decisiones), sino por otras razones personales previas. En el mejor de los casos, esas razones coinciden con las que se utilizarán en la motivación (eso indica que el operador humano "se cree" esas razones jurídicas y no incurre en desviación de poder), pero hay algo previo que le

ha llevado a optar por esas razones y no por otras (que le habrían permitido llegar a una decisión diferente, igualmente susceptible de ser motivada).

La segunda fase es la redacción y justificación de la decisión, que es un proceso condicionado o determinado por la decisión misma, en el sentido de que cada una de las posibles decisiones se justificará en función de un argumento distinto. Si se opta (por continuar con la analogía de las medidas de prevención de contagios Covid) por el cierre de establecimientos, se hará hincapié en la protección de la salud y el riesgo de contagio, mientras que, si se opta por reducir al máximo las restricciones, se insistirá en las dudas sobre el riesgo real de contagio, en la posibilidad de que también se produzcan contagios por otras vías y en la importancia de la responsabilidad individual y la libertad de empresa. Es, como digo, una labor condicionada por la anterior. Aunque, en un análisis puramente lógico, pueda parecer lo contrario (aparentemente, las premisas jurídicas conducen a una decisión concreta), la realidad es que es la decisión previamente tomada la que obliga a seguir un determinado hilo argumental para su justificación. Esta segunda fase no es creativa, puesto que lo relevante es la toma de la decisión, no tanto su motivación. Por lo tanto, el hecho de que la redacción se realice se con la ayuda de inteligencia artificial generativa no supondría un cambio cualitativo con consecuencias jurídicas importantes: no más, en todo caso, que el hecho de encomendar a una persona del equipo la redacción del texto de la decisión, cosa que es frecuente en la forma de trabajo en la Administración e incluso en algunos órganos judiciales.

El tercer elemento es el del control, desarrollado en muy distintas instancias, incluidas (pero no sólo) las de tipo judicial. Ese control consiste, fundamentalmente, en verificar si la decisión se ajusta al marco jurídico a que se encuentra sometida, a la programación normativa de la misma, a fin de llegar a una conclusión positiva (que lleva a admitir su validez) o negativa (cuya consecuencia puede ser, en algunos casos, la anulación o revocación de la decisión). En cierto modo, lo que se verifica es la motivación de la decisión, que es, a su vez, el conjunto de argumentos utilizados por el operador humano que dicta la decisión para demostrar que la misma se ajusta a su marco jurídico. El control supone una especie de revisión de la motivación (una motivación a la inversa), o una forma de "remontar" la motivación para comprobar si la decisión se ajusta al marco jurídico[20].

---

[20] De hecho, a veces la motivación es indiferente para el control, como sucede cuando el controlador suple deficiencias u omisiones en la motivación del acto y llega a la conclusión de que

En ese esfuerzo argumentativo, que va de la decisión al marco jurídico para ver si la primera se ajusta al segundo, el hecho de que la decisión se haya elaborado con un modelo de inteligencia artificial generativa es irrelevante, no se tiene en cuenta. Esa utilización no opera en ninguna de dos dimensiones posibles en que podría ser relevante para la justificación de la decisión. No se ha utilizado el modelo para "traducir" un concepto normativo de tipo probabilístico (es lo que se estudió en el epígrafe anterior, así como sus consecuencias). Y, por otro lado, el hecho de que el texto se haya elaborado con la ayuda de un modelo informático es indiferente, porque lo relevante para la verificación de la legalidad de la decisión (que es el núcleo de la función de control) es lo que ella dice y cómo se justifica jurídicamente, pero no cómo se haya elaborado la misma.

Cabría objetar y defender una tesis alternativa. Para la validez de una decisión administrativa, no importa sólo el "qué" (la parte dispositiva) y el por qué (la justificación o motivación), sino también el cómo. Esto se manifiesta jurídicamente en instituciones como las causas de abstención y recusación, las normas sobre formación de voluntad de los órganos colegiados, etc. Precisamente porque existe un elemento decisional, es decir, porque la decisión no es una "función" del ordenamiento jurídico (algo que se derive "matemáticamente" de la norma y de los hechos), y porque se pueden justificar jurídicamente distintas decisiones, es importante que ese proceso decisional, que es anterior al Derecho, no esté viciado y se realice de la forma legalmente prevista. La inserción en ese proceso de un modelo de inteligencia artificial lo viciaría y afectaría a la legalidad y validez de la decisión adoptada.

Sin embargo, creo que este análisis no sería acertado, porque el sistema de inteligencia artificial opera *después* de que se haya tomado la decisión, y, por tanto, para labores instrumentales. Por decirlo en términos de análisis lingüístico, lo que importa de una decisión administrativa no son sus palabras (que pueden ser perfectamente predecibles), sino el "metadato" de que el órgano competente haya optado por esa decisión y no por ninguna otra alternativa.

Un tribunal puede tener, para un tipo de pleito más o menos predecible (pensemos en una acción reivindicatoria, o en una petición de reequilibrio de una concesión por riesgo imprevisible, o, por mencionar un ejemplo absolutamente

---

el mismo es conforme con el ordenamiento jurídico, aunque no por las razones indicadas en su motivación (o a pesar de la falta de razones en su motivación).

real, conceder o denegar la suspensión cautelar del acto administrativo impugnado en un proceso contencioso-administrativo), dos plantillas, una para la decisión estimatoria y otra para la desestimatoria. El contenido de las sentencias es totalmente previsible y la labor de redacción no existe, puesto que se apoya en la correspondiente plantilla. Pero ello no resta un ápice de importancia a la sentencia como decisión, puesto que lo importante no son las palabras de la resolución, sino la decisión de optar por una u otra plantilla[21].

Por tanto, el uso de inteligencia generativa como elemento auxiliar para la redacción del texto de decisiones que producen efectos jurídicos (incluidos, por ejemplo, informes que indirectamente producen efectos jurídicos por su influencia sobre la resolución) carece de relevancia jurídica.

Es cierto que el instrumento utilizado puede tener su importancia, en el sentido de que por esta vía se produzca un texto que no sea igual al que saldría "de la pluma" de un operador humano, pero son efectos que se producen en cualquier contexto y que se consideran despreciables, de modo que no me parece justificado que se les dé importancia sólo porque en este caso el instrumento sea un modelo de inteligencia artificial generativa. También influye, lógicamente, que sea una u otra persona la que redacte materialmente el texto, y no por eso se exige, como condición de validez de las decisiones administrativas y judiciales, que sólo hayan intervenido en su redacción el o los titulares del órgano. Por no hablar de otros instrumentos que se utilizan sin ningún problema o prevención y que también influyen en el contenido de la decisión, e incluso de forma más incisiva. Por ejemplo, el uso de buscadores para el acceso a la información (siendo el de Google el más difundido, con una enorme diferencia sobre los demás) puede influir en la información a la que se accede, y no por ello se prohíbe su uso ni se exige su exhaustiva documentación[22].

---

[21] Esto se puede ver con facilidad en las demandas que se presentan en la jurisdicción civil o social, en las que, con frecuencia, el apartado de "fundamentos de derecho" es una simple enumeración de los artículos aplicables al caso (artículos del Código civil, o del Estatuto de los Trabajadores, por ejemplo), lo que indica que el núcleo del asunto está en la valoración de los hechos y que, una formada en el órgano judicial la convicción de que, por ejemplo, existe relación laboral, la argumentación jurídica está dada.

[22] Como recoge el ya mencionado informe para los jueces británicos sobre la utilización de inteligencia artificial, "[p]or lo general, los jueces no están obligados a describir la investigación o el trabajo preparatorio que se haya realizado para dictar sentencia. Siempre que estas pautas se sigan adecuadamente, no hay ninguna razón por la que la inteligencia artificial generativa no pueda ser una herramienta secundaria potencialmente útil" (p. 5).

Incluso el hecho de que *no se utilice un buscador*, y se limite la información a la que figura en una determinada biblioteca, también influye, pero se considera algo despreciable o irrelevante (aunque pueda no serlo, como saben, por ejemplo, las empresas que invierten en realizar actos de difusión de información favorable a sus tesis, puesto que saben que esa labor de "concienciación" es relevante).

Sería posible, teóricamente, que el operador no utilizase inteligencia artificial generativa para *redactar* la decisión que ha tomado (elaborando lingüísticamente el material que se le suministra), sino para *tomar* la decisión. El sistema arrojaría, en principio, la decisión más previsible a la vista de los datos con los que se ha entrenado, es decir, en principio, la decisión más parecida a las que suelen tomarse en esos casos. De nuevo se trata de algo que puede ser comprendido con categorías conocidas o que se parece a fenómenos que ya conocemos. Por ir a un ejemplo extremo, en el sistema actual es posible (y no siempre descartable) que el operador humano, cuando puede –de hecho– elegir entre dictar una resolución estimatoria o desestimatoria de la solicitud (o de la demanda) y justificar cualquiera de ellas sin incurrir en prevaricación, tome su decisión en función de circunstancias aleatorias, desde lanzar una moneda al aire a hipótesis mucho más probables, como la mayor o menor simpatía o arrogancia mostradas por el abogado o representante del interesado, la respuesta mediática que una u otra decisión pueden provocar o sus efectos sociales o económicos (por ejemplo, la mayor o menor simpatía por la instalación de parques eólicos o fotovoltaicos en el medio rural puede llevar a interpretar en un determinado sentido la normativa aplicable, aunque no sea un factor relevante en el marco jurídico de la decisión que en ese caso deba tomarse). ¿Invalidan la decisión adoptada esas consideraciones que no se exteriorizan y que no influyen en su justificación jurídica? Sólo en aquellos casos extremos en que puedan acreditarse y nos encontremos en desviación de poder, lo que no sucede casi nunca. Lo mismo deberíamos decir en estos casos.

También cabría una objeción más fundamental, que tal vez exigiría un epígrafe independiente. Los modelos no "piensan", sino que arrojan un resultado (por ejemplo, un texto) que es el que el modelo "sugiere" a la vista de la pregunta formulada y a partir de los datos que se le hayan suministrado para su entrenamiento. Algo parecido (aunque con un nivel muy superior de complejidad, obviamente) a lo que hace un teléfono móvil cuando, mientras el usuario está escribiendo un mensaje, le "sugiere" cuál podría ser la próxima palabra. El operador humano no actúa de la misma manera, puesto que antes de escribir "decide" qué quiere hacer y después lo escribe, sin limitarse a reproducir patrones. En este sentido, surge la objeción de

que, en realidad, también los operadores humanos, cuando aparentemente deciden, no hacen otra cosa que arrojar el resultado previsible a partir de una serie de condicionantes, como su ideología, formación académica, origen social, expectativas e intereses, etc. Es la objeción determinista, permanentemente actualizada[23]. Es una tesis defendible en términos filosóficos, pero creo que se puede afirmar que el ordenamiento jurídico no la comparte. Si realmente los comportamientos humanos estuvieran tan influidos por factores previos, habría que cambiar reglas básicas del ordenamiento, que distinguen entre comportamientos "libres" y comportamientos obligados (por ejemplo, el consentimiento prestado a una cláusula abusiva es irrelevante, la cláusula no obliga, mientras que sí obligan otras cláusulas a las que se entiende que se ha prestado un consentimiento libre) y que hacen a las personas responsables de aquellos de sus comportamientos considerados libres (por ejemplo, se obliga a cumplir los contratos).

La clave, en mi opinión, se encuentra en que, aunque la decisión que tome un operador humano pueda ser la misma que se tome si se le hace la pregunta a un modelo (a fin de cuentas, una sentencia estimatoria tiene el mismo texto tanto si es el resultado de una sesuda y honrada reflexión como si se ha escrito con una pistola apuntando a la cabeza de quien la redacta y la firma), su significado es diferente. El operador humano introduce un elemento decisional o volitivo que está ausente del modelo y también puede evolucionar o cambiar o de opinión, o reaccionar ante nuevas circunstancias, mientras que el modelo depende de los datos con los que se le haya entrenado, que pueden estar actualizados o no.

4. LA REGULACIÓN DEL USO DE LA INTELIGENCIA ARTIFICIAL

4.1. Aplicación del marco jurídico regulador de la actividad en la que se utiliza la inteligencia artificial

Una de las formas erróneas de presentar la inteligencia artificial y su impacto es el símil antropomórfico. Hablar de "inteligencia artificial" ya es un antropomorfismo, porque, aunque estos sistemas puedan producir un objeto (un texto, una imagen) que es similar o idéntico a otro que podría producir un humano, el procedimiento es diferente, en la medida en que el sistema de inteligencia artificial

---

[23] Sapolsky, R. (2018). *Compórtate. La biología que hay detrás de nuestros mejores y peores comportamientos*, Captain Swing.

no hace otra cosa que buscar la respuesta que parezca más adecuada o parecida a la que se deduzca de un conjunto de datos con el que ha sido previamente entrenado[24]. Pero, con frecuencia, sobre ese antropomorfismo cabalga otro, cuando se la presenta como un ser omnisciente que podría dominar a los humanos[25].

Esta presentación es, a mi juicio, equivocada, porque la inteligencia artificial es, hoy por hoy, un *instrumento* en manos de los humanos (de unos más que de otros), a los que permite actuar de manera más eficiente, utilizando los datos para estar un poco menos a ciegas. El empresario utiliza la inteligencia artificial para ejercer el poder que ostenta en las relaciones laborales, a la hora de llevar a cabo acciones como seleccionar a su personal, organizar su trabajo, concretar sus retribuciones o aplicar sanciones y despidos. Pero la inteligencia artificial no le da ni le quita ningún poder, simplemente le suministra criterios (no vinculantes para él) a la hora de ejercerlo.

Lo mismo sucede con cualquier otro ámbito en el que se utiliza la inteligencia artificial, incluida la Administración. Al tratarse de un *instrumento*, la inteligencia artificial se encuentra sometida a las mismas normas, al mismo marco jurídico, que regula la actividad o la potestad en la que se utiliza. Por tanto, es rotundamente falso que la inteligencia artificial carezca de regulación. Discriminar con inteligencia artificial es igual de inconstitucional que hacerlo sin inteligencia artificial. No es necesario retocar el artículo del Código Penal que castiga el homicidio cada vez que se inventa una nueva arma o un nuevo procedimiento para matar. Otra cosa es, por supuesto, que algunas armas o algunos procedimientos

---

[24] "Empecemos por contar la verdad: las máquinas no aprenden. Lo que hace un sistema típico de "machine learning" es encontrar una fórmula matemática que, cuando es aplicada a un conjunto de inputs (llamados "datos de entrenamiento"), arroja los resultados esperados. Esta fórmula matemática también arroja resultados correctos cuando se aplica a otros inputs (distintos de los datos de entrenamiento), siempre que esos inputs tengan la misma distribución estadística (o una similar) que los datos de entrenamiento.
¿Por qué eso no es aprender? Porque si se cambian ligeramente los inputs, es muy probable que el resultado sea completamente erróneo. No es la forma en la que aprenden los animales. Si alguien aprende a jugar a un videojuego mirando a la pantalla, seguirá jugando bien si alguien gira ligeramente la pantalla. En cambio, un algoritmo de "machine learning", si ha sido entrenado "mirando" a la pantalla, no podrá jugar en una pantalla girada, salvo que haya sido entrenado también para reconocer la rotación" (Burkov, A. (2019). *The hundred-page machine learning book*, XVII).

[25] Algo así se planteaba en la carta a la opinión pública de marzo de 2023, encabezada por Harari, en la que se pedía una moratoria de seis meses en la investigación en esta materia.

generen tantos riesgos que sea necesario establecer una regulación preventiva que reduzca al máximo la posibilidad de que se utilicen para causar daños.

No hay nada que, estando prohibido en el mundo analógico, pase a estar permitido sólo porque se actúe en un entorno digital o con inteligencia artificial. Otra cosa es que pueda ser más difícil aplicar determinadas normas o detectar su incumplimiento, pero conviene no poner el carro delante de los bueyes y no dar impresiones engañosas.

Cuando una decisión (de cualquier tipo) se toma con inteligencia artificial, se encuentra sometida al mismo marco jurídico, que será lo primero que haya que aplicar para ver si es admisible la utilización del instrumento, en la línea que hemos seguido al principio en relación con las decisiones administrativas.

4.2. El marco jurídico específico de la inteligencia artificial: justificación

La contraposición entre ética y derecho es constante cuando se habla de la regulación de la inteligencia artificial. De hecho, las discusiones sobre la posible regulación son etiquetadas normalmente como "ética", sobre todo cuando se abordan en el marco de estudios y titulaciones de tipo técnico, o en el interior de las empresas. Creo que se trata de una falsa dicotomía. Toda regulación legislativa tiene como fundamento una postura ética, unos determinados principios morales, pero va más allá de ella porque la dota de un sistema sancionador que distingue a lo jurídico de lo ético. Es algo que de puro obvio resulta sonrojante, pero no sobra recordarlo en estos momentos. La inteligencia artificial reclama, pues, una regulación jurídica y no sólo unos principios éticos, aunque siempre que se utiliza la inteligencia artificial para tomar una decisión con efectos jurídicos, se aplica también la regulación o el marco jurídico de la decisión en la que se utiliza la inteligencia artificial.

Precisamente a partir de esa constatación (lo que está prohibido en general lo está igualmente cuando se actúa con inteligencia artificial), cuando el uso de la inteligencia artificial genera daños surgen las mismas responsabilidades que cuando esos daños se causan por otros medios. La discriminación o la vulneración de normas sobre protección de datos dan lugar a sanciones penales o civiles (como están buscando ahora, por ejemplo, los editores de periódicos con la demanda colectiva contra Meta). Ese tipo de normas suelen tener un efecto disuasorio, en el sentido de que llevan a los sujetos a adoptar medidas de prudencia para evitar incurrir en esas responsabilidades. De hecho, las grandes empresas tecnológicas han adoptado criterios de autorregulación similares a las exigencias

que establece el Reglamento de Inteligencia Artificial precisamente para evitar asumir responsabilidades por daños.

Cuando los riesgos son demasiado altos es cuando tiene sentido una regulación preventiva, aquí y en cualquier otro campo. Ese es el sentido del Reglamento de Inteligencia Artificial, que prohíbe algunos usos de la inteligencia artificial y que, para aquellos que, estando permitidos, son de "alto riesgo" por el contexto en que se utilizan (es decir, porque las decisiones que ayudan a adoptar afectan más directamente a humanos en asuntos sensibles o pueden producir accidentes o daños materiales), establece unos requisitos de precaución y calidad que deberían minimizar el riesgo de que se produzcan predicciones o resultados erróneos y, por tanto, perjudiciales.

Sin embargo, esa regulación preventiva general no impide la aplicación de la normativa sectorial, que creo que acabará siendo tanto o más importante. El cumplimiento del Reglamento será algo fundamental, que sucederá "aguas arriba". Ningún producto de inteligencia artificial podrá ponerse en funcionamiento sin ese control, pero es algo previo a la solución de los problemas concretos que se planteen en su uso. La aplicación de inteligencia artificial, por ejemplo, a la actividad administrativa, exigirá el cumplimiento del Derecho administrativo, tanto de sus normas generales como de las que se establezcan (o incluso deban establecerse previamente) para el uso de la inteligencia artificial.

4.3. El Reglamento de Inteligencia Artificial

El Reglamento de Inteligencia Artificial (Reglamento 2024/1689, de 13 de junio) se enfrenta a la dificultad de regular un objeto en movimiento, que ha cambiado desde que se presentó el proyecto (abril de 2021) hasta su aprobación (2024). Además, intenta regular la inteligencia artificial (saliendo de la situación de anomia o autorregulación en la que nos encontramos y que algunos pretenden que es la mejor) sin matar la innovación con exigencias excesivas. Su proceso de elaboración ha sido muy complejo y ha sido visible la presión tanto de las tecnológicas que producen sistemas de inteligencia artificial como de los partidarios de una regulación restrictiva. Europa intenta favorecer la innovación, pero también es un espacio donde se "consume" inteligencia artificial creada fuera, lo que probablemente influye en este planteamiento restrictivo.

La aproximación elegida por la Comisión parte, en primer lugar, de distinguir entre tres tipos de sistemas de inteligencia artificial. Algunos de ellos

(o, más bien, algunas utilizaciones de la inteligencia artificial) están directamente prohibidas. Este apartado incluye los sistemas de tipo subliminal que provocan que las personas se hagan daño, o los que aprovechan vulnerabilidades individuales o colectivas. También se prohíben los sistemas "de recompensa", que perfilan a los ciudadanos en función de sus datos y les aplican un tratamiento determinado en entornos que nada tienen que ver con esos datos (sería el caso de sistemas que, por ejemplo, utilizan la falta de atención demostrada por un sujeto en su navegación por internet o al estudiar cursos online, para emitir un informe desfavorable sobre él y vendérselo a agencias de empleo). Durante la elaboración de la norma se añadieron otros ejemplos, como el uso de sistemas de detección de emociones en entornos laborales o educativos, o ciertas limitaciones a la policía predictiva. Alguna de las prácticas prohibidas es más bien una práctica sometida a regulación, como sucede con la identificación biométrica en tiempo real, que los Estados pueden aprobar, con garantías, para la prevención de delitos.

El núcleo de la regulación del Reglamento se centra en los sistemas de alto riesgo, que son aquellos que, o bien son accesorios a productos que están sometidos a normas europeas precisamente por los riesgos que producen (ascensores, explosivos, juguetes, etc.) o bien pueden producir riesgos precisamente por afectar a derechos de los ciudadanos (sistemas que inciden en el empleo, el acceso a los servicios públicos, la educación, la justicia, el control de fronteras, etc.). Para estos sistemas se establecen unos requisitos en cuanto a los datos con que son entrenados, la información que ha de suministrarse tanto a la autoridad como a quienes van a utilizarlos, el registro de su funcionamiento (a modo de "caja negra" que permita conocer cómo han funcionado y si han producido errores o desviaciones), la resistencia a ciberataques, el sometimiento efectivo a control humano, etc. Se trata de requisitos que en cierto modo son genéricos (ello al margen de los principios que proclama el Reglamento, por ejemplo, en el artículo 1 y en los párrafos 7, 8 y 27 del preámbulo), porque pueden concretarse de formas diversas y porque exigen una decisión en cuanto al nivel de riesgo asumible (cuanto más se quiera limitar el riesgo, más intensas deberán ser las medidas preventivas que se establezcan). El artículo 9, apartados 3 y 4, lo reconoce. Por tanto, con independencia de cuál es el procedimiento que en cada caso se establezca para el control del cumplimiento de esos requisitos (a veces con intervención de terceros), se trata de una obligación de justificar la forma concreta en que se pretende cumplir esos requisitos.

4.4. Aplicación del Reglamento a las Administraciones Públicas

El Reglamento regula el uso de la inteligencia artificial por sujetos públicos o privados, por lo que se puede afirmar que es una norma transversal. Su artículo 3 deja claro que tanto el proveedor como el "responsable del despliegue" de un sistema de inteligencia artificial (esta última figura es que pasa a utilizar el sistema en su actividad) pueden ser entidades privadas o públicas.

Es cierto que los sistemas de inteligencia artificial que se utilizan en algunas actividades que llevan a cabo autoridades públicas son de alto riesgo o incluso pueden ser prácticas prohibidas. Es decir, los sistemas de inteligencia artificial que utilizan autoridades públicas tienen más probabilidades de ser sistemas de alto riesgo que los que utilizan sujetos privados, pero ello no se debe a razones subjetivas (a que el sujeto sea una autoridad pública o una entidad privada), sino a la tarea o función de que se trate. Así, en el Anexo III, que enumera algunos de los sistemas de alto riesgo (también son de alto riesgo, de acuerdo con el artículo 6.1, sistemas que se utilizan junto con productos sometidos a regulación europea por ser productos de riesgo) se enumeran bastantes sistemas que son utilizados por entidades públicas, como los que se utilizan para evaluar la admisibilidad de personas físicas a servicios esenciales, en la aplicación de la Ley (entendida como sinónimo de la persecución de infracciones penales), control de fronteras, así como, por supuesto, los utilizados por la administración de justicia (yendo, en este caso, más allá de lo administrativo).

Existe una exigencia adicional que sólo se aplica a las entidades de derecho público que "desplieguen" un sistema de inteligencia artificial de alto riesgo, es la de realizar una evaluación de impacto relativa a los derechos fundamentales, regulada en el artículo 27 (e introducida durante la tramitación del proyecto). Esta evaluación sí constituye un elemento diferencial de los entes públicos, porque no se exige a personas jurídicas privadas que desplieguen sistemas de alto riesgo. Se pretende que esta evaluación sea un análisis prospectivo de los riesgos que el sistema puede producir para los derechos fundamentales, así como una previsión de las medidas adecuadas para mitigarlos. En cierto modo, ese instrumento se solapa con el sistema de gestión de riesgos que es necesario en todos los sistemas de alto riesgo y que se regula en el artículo 9.

Se contienen algunas otras especialidades en el caso de sistemas de inteligencia artificial utilizados por autoridades públicas. Así, la obligación de registro del sistema es más intensa que en los demás casos, porque no sólo hay que registrar el

sistema (eso debe hacerlo el proveedor), sino también su utilización por una autoridad pública (artículos 26.8 y 49.3). También hay una norma transitoria especial (más generosa) para la adaptación al Reglamento, que se fija en 6 años desde su entrada en vigor (artículo 111.2).

Es importante destacar que estas normas, aunque tienen una vocación armonizadora (evitar que los Estados puedan aprobar normas nacionales más exigentes o restrictivas, que puedan dificultar el funcionamiento del mercado único en este campo, como dice el párrafo 3 del preámbulo), de modo que las posibilidades de aplicar normas nacionales que se desvíen del Reglamento están enumeradas expresamente (protección de datos, normas de protección de los trabajadores...), el cumplimiento del Reglamento no es la única norma que se aplicará cuando las Administraciones utilicen sistemas de inteligencia artificial. Como he adelantado, también será necesario aplicar la legislación sobre procedimiento administrativo (entre otras), porque es la que regula la actividad administrativa en la que se utiliza como instrumento la inteligencia artificial.

5. CONCLUSIONES

Los sistemas de inteligencia artificial se construyen para suministrar información (por ejemplo, predicciones) que sirva para responder a una pregunta, todo ello a partir del análisis y el hallazgo de correlaciones en datos del pasado. El sistema tendrá más probabilidades de acertar en la medida en que esos datos se parezcan a la situación actual a la que se aplica. La inteligencia artificial pretende reducir la incertidumbre y, por tanto, tendría cabida –técnicamente– en actividades (también de tipo jurídico o administrativo) en las que exista un margen de actuación, en las que sean posibles varias alternativas.

Los modelos de inteligencia artificial pueden servir para concretar conceptos normativos que son probabilísticos o de pronóstico, como los relacionados con el riesgo. Es un instrumento técnico cuyo encaje jurídico no sería muy diferente del de otros métodos técnicos que se utilizan en la actividad pública.

Otro campo habitual sería el de ayudar a centrar la actividad administrativa, como una aproximación que le indique campos en que puede ser más oportuna, necesaria o efectiva (parámetros definidos previamente por operadores humanos), pero sin tomar decisiones o resoluciones.

Ir más allá resultaría estructuralmente muy difícil (con independencia de que se admita legalmente o no) porque, o bien incumpliría el marco normativo

(sustituyendo la constatación de hechos por una predicción o una probabilidad), o en realidad la intervención del sistema de inteligencia artificial sería instrumental de una decisión humana previa, que es la que elige las preguntas que va a responder el sistema o fija los parámetros con los que este realizará una actividad auxiliar.

Una cosa es utilizar un modelo informático para *elaborar* una decisión a partir de un marco jurídico que la vincula y determina, y otra cosa es utilizarlo para *justificarla*, es decir, para argumentar por qué se elige una concreta opción. El grado de visibilidad, relevancia jurídica y exigencias no puede ser el mismo en un caso y en otro.

Cuando una decisión jurídicamente relevante se *justifica*, al menos en parte, en que es el resultado que ha producido un sistema de inteligencia artificial, en los procedimientos de control de dicha decisión se podrá y deberá verificar si ese sistema de inteligencia artificial ha funcionado de forma adecuada, lo que supone, al menos, dos cosas: que su diseño sea adecuado al marco jurídico que se está aplicando (es decir, que se le haya programado para buscar justamente aquello que es jurídicamente relevante, y no otra cosa distinta) y que su funcionamiento en concreto haya sido coherente con ese diseño.

El hecho de que en la *elaboración* de una decisión jurídicamente relevante se haya utilizado algún producto o procedimiento tecnológico (por ejemplo, un sistema de inteligencia artificial, incluidos los de tipo generativo) no necesariamente afecta a la validez de dicha decisión ni supone que en su control sea necesario analizar a fondo el funcionamiento de ese sistema de inteligencia artificial, porque el mismo permanece en un segundo plano y resulta irrelevante para verificar la legalidad de esa decisión.

La inteligencia artificial no es un ente que se enfrente a los humanos o amenace con dominarlos, sino un instrumento utilizado por algunos humanos para ejercer sus poderes, derechos y potestades (que son los mismos con independencia de que se utilice, o no, ese instrumento). La utilización de inteligencia artificial se encuentra automáticamente sometida al marco jurídico de esas potestades. Lo que está prohibido cuando se realiza de forma humana también lo está cuando se hace con inteligencia artificial. El marco jurídico o programación normativa de la actividad administrativa, que incluye normas sobre su contenido y sobre el procedimiento necesario para su producción, así como vías de impugnación y recurso, se aplica con independencia de que en su elaboración se hayan utilizado modelos de inteligencia artificial, que son un simple instrumento.

La inteligencia artificial es una actividad tecnológicamente compleja en la que pueden producirse resultados erróneos por múltiples razones. Si esos resultados son tomados como base para la toma de decisiones que afecten a personas, las decisiones podrán ser inadecuadas y contrarias al ordenamiento jurídico de muchas formas, empezando por la discriminación, pero no exclusivamente. Esto justifica que se haya elaborado una normativa específica para la inteligencia artificial, que intenta prevenir esos errores. Pero, con independencia de ella, el problema fundamental es que esas posibles decisiones inadecuadas están prohibidas por el marco jurídico que regule cada decisión en la que se haya utilizado inteligencia artificial, marco que debe aplicarse en todo caso, también cuando se utilice la IA.

BIBLIOGRAFÍA

Álvarez González, E. M. (2022). *La función normativa y la técnica legislativa en España. Una nueva herramienta: la inteligencia artificial*, Tirant, Valencia.

Arias, J., Moreno-Rebato, M., Rodríguez-García, J. A. y Ossowski, S. (2023). "Automated legal reasoning with discretion to act using s(LAW)", *Artificial Intelligence and Law*, 20-11-2023.

Barona Vilar, S. (2022). "La seductora algoritmización de la justicia. Hacia una justicia poshumanista (Justicia+) ¿utópica o distópica?", *El Cronista*, 100, pp. 36-47.

Boix Palop, A. (2020). "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones", *Revista de Derecho Púbico: Teoría y Método*, núm. 1, pp. 223-270.

Burkov, A. (2019). The hundred-page machine learning book.

Campuzano Fernández, S. y Vega Vicente, P. (2021). "Riesgos y oportunidades de la inteligencia artificial desde la perspectiva de la competencia. Un análisis desde la CNMC", *Boletín Económico de ICE* (Información Comercial Española), núm. 3131, julio, pp. 43-55.

Castets-Renard, C. y Eynard, J. (dir.). (2023). *Un Droit de l'intelligence artificielle. Entre règles sectorielles et régime général. Perspectives comparées*, Bruylant, Bruxelles.

Cerrillo I Martínez, A. (2019). "El impacto de la inteligencia artificial en el Derecho administrativo. ¿Nuevos conceptos para nuevas realidades técnicas?", *RGDA*, núm. 50.

Cotino Hueso, L. (2023). "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", en Gamero Casado (dir.) y Pérez Guerrero (coord.), pp. 257-351.

Cotino Hueso, L. y Todolí Signes, A. (coords.). (2022). *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente*, Tirant, Valencia.

Cubero Marcos, J. I. (2022). "Potestad administrativa de inspección e inteligencia aritificial: cuestiones controvertidas", en *VESTRI*, pp. 139-156.

De La Sierra, S. (2020). "Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración Pública", *Revista General de Derecho Administrativo*, núm. 53.

Degli-Esposti, S. (2023). *La ética de la inteligencia artificial*, CSIC-Catarata, Madrid.

Díaz González, G. M. (2020). "Algoritmos y actuación policial: la policía predictiva", en Huergo Lora (dir.) y Díaz González (Coord.), pp. 181-234.

Díez Sastre, S. (2008). *El precedente administrativo. Fundamentos y eficacia vinculante*, Marcial Pons, Madrid.

Dimatteo, L. A., Poncibò, C. y Cannarsa, M. (ed.) (2022). *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge.

Ebers, M. y Cantero Gamito, M. (ed.) (2021). *Algorithmic Governance and Governance of Algorithms. Legal and ethical Challenges*, Springer, Berlin.

Fernández Farreres, G. (2022). "El control judicial de la administración ante algunas cuestiones problemáticas", *REDA*, núm. 219, pp. 13-24.

Fernández Salmerón, M. (2019). "De la reutilización de sentencias al big data judicial. Aproximación a la metamorfosis experimentada por los modelos de uso de la información en el marco de la actividad jurisdiccional", en Gómez Manresa, F., Fernández Salmerón, M. y Arenas Ramiro, M. (dir.), Aranzadi, Cizur Menor, pp. 63-102.

Frosini, V. (2019). *Cibernética, Derecho, internet y sociedad*, Ediciones Olejnik, Santiago de Chile.

Gallone, G. (2023). *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Wolter Kluwer CEDAM, Milano.

Gamero Casado, E. (dir.) (2021). *La potestad administrativa. Concepto y alcance práctico de un criterio clave para la aplicación del Derecho administrativo*, Tirant, Valencia.

— (2023). "Las garantías de régimen jurídico del sector público y del procedimiento administrativo común frente a la actividad automatizada y la inteligencia artificial", en Gamero Casado (dir.) y Pérez Guerrero, Francisco (coord.), pp. 397-461.

Gamero Casado, E. (dir.) y Pérez Guerrero, F. (Coord.) (2023). *Inteligencia artificial y sector público: retos, límites y medios*, Tirant, Valencia.

García Fernández, M. (2022). "Collusion detection in public procurement auctions with machine learning algorithms", *Automation in Construction*, núm. 133.

— (2023): "European public procurement (2012-2022): indicators and competition & SME maps for crossborder analysis based on TED data", Research project for the Publications Office of the EU.

García Mexía, P. (2022). "Contra el «ciberfatalismo». Beneficio y riesgo en la sociedad digital", *Revista de las Cortes Generales*, núm. 114, pp. 285-354.

Guckelberger, A. (2019). *Öffentliche Verwaltung im Zeitalter der Digitalisierung. Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht*, Nomos, Baden-Baden.

Hernández Peña, J. C. (2022). *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cizur Menor.

Huergo Lora, A. (dir.) y Díaz González, G. M. (coord.) (2020). *La regulación de los algoritmos*, Aranzadi, Cizur Menor.

Huergo Lora, A. (1995). "La desigualdad en la aplicación de potestades de gravamen: remedios jurídicos", *RAP*, núm. 137, pp. 189-238.

— (2019). "Regulation versus tort. La función y los límites del Derecho administrativo", *Almacén de Derecho*, 12 de mayo.

— (2020). "Una aproximación a los algoritmos desde el Derecho administrativo", en Huergo Lora, A. (dir.) y Díaz González, G. M. (coord.), *La regulación de los algoritmos*, Aranzadi, Cizur Menor, pp. 23-87.

— (2022). "Inteligencia artificial y sanciones administrativas", en Rebollo Puig, M., Huergo Lora, A., Guillén Caramés, J. y Cano Campos, T. (dir.), *Anuario del Derecho Administrativo Sancionador (2022)*, Civitas, Cizur Menor, pp. 275-309.

— (2024a). "Por qué aciertan las sentencias sobre el «algoritmo» del bono social eléctrico", entrada publicada en el blog *Almacén de Derecho*, 10 de mayo de 2024.

— (2024b). "Distopía y algoritmos", entrada publicada en el blog *Almacén de Derecho*, 15 de mayo de 2024.

Izquierdo Carrasco, M. (2022). "Actuaciones automatizadas en la sanción de irregularidades en el orden social", en Cotino Hueso y Todolí Signes, pp. 261-288.

Kearns, M. y Roth, A. (2020). *The ethical algorithm. The science of socially aware algorithm design*, Oxford University Press, Oxford.

Kohl, U., Eisler, J. (ed.) (2021). *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge University Press, Cambridge.

Llano Alonso, F. y Garrido Martín, J. (ed.) (2021). *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital*, Aranzadi, Cizur Menor.

Martín Delgado, I. (2009). "Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada", *RAP*, núm. 180, pp. 353-386.

Martín López, J. (2023). *Inteligencia artificial y comprobación tributaria: transparencia y no discriminación*, Aranzadi, Cizur Menor.

Martini, M. (2019). *Blackbox Algorithmus - Grundfragen einer Regulierung Künstlicher Intelligenz*, Springer, Berlin.

Menéndez Sebastián, E. (2023). *From bureaucracy to artificial intelligence*, Wolters Kluwer CEDAM, Milano.

Miranzo Díaz, J. (2023). *Inteligencia artificial y Derecho administrativo. Especial referencia a los instrumentos de colaboración público-privada y contratación pública*, ICA-Tecnos, Madrid.

Moreno Rebato, M. (2021). *Inteligencia artificial (umbrales éticos, Derecho y Administraciones Públicas)*, Aranzadi, Cizur Menor.

Nieto, A. (2000). *El arbitrio judicial*, Ariel, Barcelona.

— (2019). *Una introducción al derecho*, Tirant, Valencia.

Nikolanikos, N. Th. (2023). *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*, Springer, Berlin.

Orofino, A. G. (2020). *La trasparenza oltre la crisi. Accesso, informatizzazione e controllo civico*, Circolo Editore, Bari.

Palma Ortigosa, A. (2022). *Decisiones automatizadas y protección de datos. Especial atención a los sistemas de inteligencia artificial*, Dykinson, Madrid.

Poncé Solé, J. (2023). "Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana", en Gamero Casado (dir.) y Pérez Guerrero (coord.), pp. 195-225.

— (2024a). "Por qué se equivocan las sentencias sobre el algoritmo del bono social eléctrico", entrada publicada en el blog *Almacén de Derecho*, 13 de mayo de 2024.

— (2024b). "Utopía y algoritmos", entrada publicada en el blog *Almacén de Derecho*, 17 de mayo de 2024.

Presno Linera, M. A. (2022). *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid.

Puentes Cociña, B. y Quintiá Pastrana, A. (2019). *El derecho ante la transformación digital. Oportunidades, riesgos y garantías*, Atelier, Barcelona.

Ribes, A. (2021). "La posición del contribuyente ante los Sistemas de Inteligencia Artificial utilizados por la Administración", *Quincena Fiscal*, 2021/18.

Rivero Ortega, R. (2023). *Derecho e inteligencia artificial. Cuatro estudios*, Olejnik, Santiago de Chile.

Sanchez-Graells, A. (2021). "Procurement Corruption and Artificial Intelligence: Between the Potential of Enabling Data Architectures and the Constraints of Due Process Requirements", October 29, to be published in S. Williams & J. Tillipman (eds.), Routledge Handbook of Public Procurement Corruption (Routledge, Forthcoming), Available at SSRN: https://ssrn.com/abstract=3952665 or http://dx.doi.org/10.2139/ssrn.3952665

Sapolsky, R. (2018). *Compórtate. La biología que hay detrás de nuestros mejores y peores comportamientos*, Captain Swing.

Schmidt-Assmann, E. (2003). *La Teoría General del Derecho administrativo como sistema. Objeto y fundamentos de la construcción sistemática*, Marcial Pons, Madrid.

Solar Cayón, J. I. (2019). *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*, Aranzadi, Cizur Menor.

Soriano Arnanz, A. (2021). *Data protection for the prevention of algorithmic discrimination. Protecting from discrimination and other harms caused by algorithms through privacy in the EU: possibilities, shortcomings and proposals*, Aranzadi, Cizur Menor.

— (2022). "El uso de sistemas automatizados por los poderes públicos. El caso del sistema empleado por el servicio público de empleo austriaco", en Cotino Hueso y Todolí Signes, pp. 193-2011.

Todolí Signes, A. (2022). "Inspección de trabajo, algoritmos, inteligencia artificial y su uso en la planificación inspectora", en Cotino Hueso y Todolí Signes, pp. 236-259.

Valero Torrijos, J. (2020). "The Legal Guarantees of Artificial Intelligence in Administrative Activity: Reflections and Contributions from the Viewpoint of Spanish Administrative Law and Good Administration Requirements", *ERDAL*, núm. 1, pp. 55-62.

— (2023). "Las singularidades del tratamiento de datos de carácter personal en entornos de inteligencia artificial en el sector público", en Gamero Casado (dir.) y Pérez Guerrero (coord.), pp. 353-396.

Velasco Rico, C. (2019). "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", en Puentes Cociña y Quintiá Pastrana, pp. 73-90.

Vestri, G. (dir.) (2022). *La disrupción tecnológica en la Administración Pública. Retos y desafíos de la inteligencia artificial*, Aranzadi, Cizur Menor.

Wischmeyer, T. y Rademacher, T. (eds.) (2020). *Regulating Artificial Intelligence*, Springer, Berlin.

Capítulo 8
ALGORITMOS E INTELIGENCIA ARTIFICIAL EN EL DERECHO DIGITAL DEL TRABAJO

Jesús R. Mercader Uguina
Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad Carlos III de Madrid
https://orcid.org/0000-0001-6301-6788

1. LA ARQUITECTURA DEL DERECHO DIGITAL DEL TRABAJO

La arquitectura del Derecho digital del Trabajo se está reconstruyendo sobre nuevos pilares de sustentación. Los algoritmos y la Inteligencia Artificial (IA) son las piezas maestras desde las que la empresa post-material se lanza hacia una transformación radical de sus tradicionales estructuras. Por el momento son las grandes las que implementan de modo generalizado estos sistemas, pero es cuestión de tiempo que los mismos se expandan al resto. Esta "gran delegación empresarial"[1], se produce, además, a un ritmo incontenible en el que el futuro se convierte en pasado a enorme velocidad.

Pero ¿qué es un algoritmo? Se entiende por algoritmo, según el Diccionario de la Real Academia Española de la Lengua, el "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema"[2]. Una tecnología

---

[1] De estas y otras muchas cuestiones vinculadas con este conjunto de transformaciones, me he ocupado en mi monografía, J. R. Mercader Uguina, *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Valencia, Tirant lo Blanch, 2022. Posteriormente, en "*En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo*", *El Cronista del Estado Social y Democrático de Derecho*, 2022, núm. 100 (ejemplar dedicado a: Inteligencia artificial y derecho), pp. 136-145. Muchas reflexiones y contenidos de este trabajo son tributarios de esos antecedentes.

[2] La Resolución de 21 de septiembre de 2016, de la Comisión de Garantía del derecho de acceso a la información pública de Cataluña, en la reclamación 123/2016, se define el algoritmo como el "procedimiento de cálculo que consiste en cumplir un conjunto ordenado y finito de instrucciones con unos datos especificados para llegar a la solución del problema planteado"

intelectual, se ha dicho, que supone, en última instancia, la sustitución de juicios intuitivos por una respuesta objetivada. Y ello en la medida en que un algoritmo es una receta, un conjunto de instrucciones matemáticas, una secuencia de tareas destinada a conseguir un cálculo o un resultado. Hablando informalmente, un algoritmo es la descripción precisa de los pasos que nos llevan a la solución de un problema planteado. Estos pasos son, en general, acciones u operaciones que se efectúan sobre ciertos objetos. La descripción de un algoritmo afecta a tres partes: entrada (datos), proceso (instrucciones) y salida (resultados). En este sentido, un algoritmo se puede comparar a una función matemática.

Desde nuestra limitada perspectiva, tan alejada de las ciencias exactas, resulta imposible conocer qué son exactamente los algoritmos, aunque sí podemos saber para qué sirven, qué hacen, cuál es su lógica, etc. Si ensayáramos una definición podríamos decir que los algoritmos son formulaciones matemáticas que analizan experiencias pasadas de las que sabemos qué resultado produjeron utilizando para ello grandes cantidades de datos (no "muestras")[3], de modo que por medio de lenguaje algebraico y el uso de determinados "indicadores" ("*proxy*"), se extraen predicciones, correlaciones o aproximaciones (no inferencias causales) a partir de las cuáles se identifica qué características o grupo de características han llevado a los mejores resultados que, sobre esta base, permitirían adoptar decisiones automáticas o humanas[4].

La Inteligencia Artificial (**IA**) ha recibido, por su parte, una precisa definición jurídica en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifica el Reglamento (CE) núm. 300/2008, [en adelante, **RIA**]. Una noción que se alinea definitivamente con la realizada por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en mayo de 2019, y que define como sistema de IA a "*un sistema*

---

o "conjunto finito de reglas que, aplicadas de manera ordenada, permiten la resolución sistemática de un problema, el cual se utiliza como punto de partida en programación informática".

[3] Mayer-Schónberger, V. y Cukier, K. (2022). *Big data. La revolución de los datos masivos*, Turner, Madrid, 2013, pp. 49-98. De enorme interés en Peña, D., *Observación y cálculo en estadística con datos masivos*, Madrid, Real Academia de Ciencias Exactas, Físicas y Naturales de España.

[4] Pues como señala Byung-Cul Han (2021), *No cosas. Quiebras del mundo de hoy*, Barcelona, Taurus, p. 59, "no sale de lo antes dado hacia lo intransitado" y "resulta ciega para los acontecimientos".

basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales" (art. 3.1). La norma también busca dotar de un régimen jurídico propio a los que califica de "modelos de IA de uso general" (art. 3.63), denominados en versiones anteriores del RIA como "modelos fundacionales", esto es, la inteligencia artificial generativa que tiene en ChapGPT su mascarón de proa.

No está de más recordar que, tanto los sistemas algorítmicos, como los de IA descansan en los datos y en la capacidad de computación. Una noción, la de "dato", que aparece precisamente definida Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos), entendiendo por tal: "toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual". Los datos son el aire de los nuevos ecosistemas productivos, su nutriente fundamental y se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso social. Por su parte, el formidable desarrollo de la capacidad de computación que marca fronteras inimaginables con los ordenadores cuánticos, convierte en irresistible esta lógica transformadora que tiene en el trabajo uno de sus centros de gravedad.

2. LA EMPRESA Y EL EMPLEADOR ALGORÍTMICO: LA ERA DE LA EMPRESA POST-MATERIAL

Los algoritmos han venido a revolucionar la idea misma de empleador. Gráficamente, se ha llegado a decir que "mi jefe es un algoritmo"[5]. Es lo cierto que los algoritmos se encuentran en el corazón de las empresas y son, en muchos casos, un elemento esencial de muchas de ellas. La utilidad de los algoritmos en el sector privado, donde han propulsado a los gigantes tecnológicos, en especial Facebook, Amazon, Google y Netflix, es incuestionable y en este mundo empresarial han florecido los algoritmos predictivos que producen un enorme

[5] Al respecto puede verse, http://www.xataka.com/legislacion-y-derechos/sistemas-predictivos-cuando-tu-jefe-se-convierte-en-un-algoritmo

incremento de eficiencia que ha catapultado a estas empresas. Estas formas avanzadas de inteligencia de algunos algoritmos ("agentes autónomos") tendrían los atributos necesarios para poder desarrollar negocios. Estas "entidades algorítmicas" ya existen. Funcionan por impulso de un software de IA autónomo y carecen por entero de participación humana de manera continua, sin humanos en la posición de accionistas o miembros de las entidades[6].

Una realidad que plantea numerosos problemas desde la perspectiva mercantil, fiscal, laboral y de propiedad intelectual. Lo que ha llevado a plantear, incluso, la necesidad de controlar el desarrollo de estas nuevas empresas algorítmicas. Así, la Comisión Alemana de Ética de Datos ha publicado propuestas para la regulación de algoritmos[7] basadas en ese riesgo y ha propuesto la separación estructural de la parte de la organización responsable de administrar el algoritmo. Se recomienda, así, que esta unidad de actividad podría ubicarse en una unidad de negocio separada, con objetivos e incentivos claramente definidos, y hacerse independiente de las partes de la empresa favoreciendo, por ende, un mayor control de la parte segregada. Existe un precedente en la regulación de telecomunicaciones de la UE que contiene una fórmula de "separación funcional" destinada a escindir las funciones y departamentos[8]. Sin embargo, se trata de un remedio complejo.

Desde el punto de vista laboral, la gran cuestión está en si las reglas de imputación de responsabilidades empresariales, que favorecen la tutela de los trabajadores, se proyectarán también sobre este ámbito. Es cierto que la idea de empresa regulada por nuestra legislación es material, física, tangible, pero también lo es la tendencia hacia la ingravidez empresarial. Pero no debe olvidarse que, en muchos casos, detrás de los algoritmos y de su gestión existen importantes equipos de personas destinadas, precisamente, a dar soporte, desarrollo y mantenimiento a dicha realidad. Por el momento, los elementos personales siguen estando en la base de las empresas algorítmicas.

---

[6] Muñoz Pérez, A. F. (2020). *La "inteligencia artificial (IA) autónoma" en el órgano de administración*, Revista de Derecho de Sociedades, núm. 60. BIB 2020\36730.

[7] Como recoge Muñoz Ruiz, A., *¿Se deben regular los algoritmos? Un breve análisis a la propuesta normativa alemana: la pirámide de criticidad basada en el riesgo*, Foro de Labos, 11 de diciembre de 2019.

[8] En los términos del art. 16 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

3. LA GRAN DELEGACIÓN EMPRESARIAL: LA GESTIÓN ALGORÍTMICA DEL EMPLEO

3.1. Procesos de selección de trabajadores sospechosos

Como señalábamos las empresas comienzan a delegar aspectos claves de la gestión laboral en los algorítmicos. Estos sistemas se reivindican como un instrumento eficaz a la hora de valorar a un amplio conjunto de individuos de idéntica manera y, por tanto, vienen a constituirse en un eficaz aliado para el desarrollo de las políticas de gestión empresarial (también conocidas como "*people analytics*" o "*Big Data HR*"). Lo mejor de los algoritmos es que son hiperlógicos: extrapolan o extraen conclusiones para maximizar la eficiencia. Su uso permite, a priori, garantizar que las contrataciones o las extinciones de contratos ya "no se basen en corazonadas, impresiones o prejuicios"[9].

El uso de los algoritmos se está generalizando como un método de selección del personal. Así lo pone de manifiesto la Recomendación CM/Rec (2020) 1, cuando señala que los sistemas algorítmicos se emplean "con fines predictivos (...) en entornos laborales (...), incluso como parte de los procesos de contratación y selección públicos y privados". En nuestro país, la Carta de Derechos Digitales, presentada en julio de 2021, cuyo apartado XIX ("Derechos en el ámbito laboral"), además de reconocer el derecho de las personas trabajadoras a sus derechos fundamentales, precisaba también "la garantía de sus derechos frente al uso por la entidad empleadora de procedimientos de analítica de datos, inteligencia artificial y, en particular, los previstos en la legislación respecto del empleo de decisiones automatizadas en los procesos de selección de personal".

Como señalara el WP251rev.01 del GT 29, en sus "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679" (en adelante, WP251), las decisiones automatizadas descritas en el art. 22.1 del Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ("RGPD") también pueden ser necesarias para el desarrollo de procesos precontractuales. Algunas empresas han puesto en manos de un software los procesos de selección de sus trabajadores en

---

[9] Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information.* Harvard University Press, 2015. http://www.jstor.org/stable/j.ctt13x0hch, p. 35.

la medida en que "los seres humanos son muy buenos en especificar lo que se necesita para un determinado puesto y obtener información de los candidatos, pero son muy malos en la ponderación de los resultados"[10]. Las funciones algorítmicas permiten, una vez definido en detalle un perfil profesional determinado (titulación, años de experiencia, etc., y unos pesos asociados a cada una de esas características), extraer de los "currícula" de los candidatos la información relevante y calcular el más preciso ajuste al perfil deseado.

Pero los algoritmos se emplean también en pruebas de selección gamificadas que incluyen preguntas, rompecabezas u otros desafíos utilizados para realizar evaluaciones predictivas sobre un empleado o solicitante de empleo, o para medir características de los mismos que incluyan características como la destreza, el tiempo de reacción u otras capacidades o características físicas o mentales. Estas evaluaciones, también conocidas como evaluaciones psicométricas basadas en juegos o reclutamiento gamificado, se están convirtiendo en una herramienta de reclutamiento cada vez más común. Estas evaluaciones se utilizan junto con las soluciones de pruebas psicométricas tradicionales o como una alternativa a ellas para hacer que el proceso de contratación sea más efectivo y eficiente para los empleadores y brindar una experiencia atractiva para los candidatos. Sus riesgos, sin embargo, son evidentes[11].

Pero el uso de los sistemas de IA va más allá, y los modelos decisión automatizada pueden limitar o excluir, a los solicitantes de empleo a través de más complejas fórmulas. Por ejemplo, un sistema de decisión automatizado que mide el tiempo de reacción de un solicitante puede que excluya injustificadamente a personas con ciertas discapacidades. Ello debería llevar, a menos que concurra una causa justificada, a que el empleador demuestre que un tiempo de reacción rápido durante el uso de un dispositivo electrónico está relacionado con el trabajo y es coherente con la necesidad de la empresa, las decisiones tomadas

---

[10] Nathan, N. R., Once, D. S. y Klieger, D. M. *In Hiring, Algorithms Beat Instinct* https://hbr.org/2014/05/in-hiring-algorithms-beat-instinct

[11] Sobre lo que llama la atención el California's Fair Employment and Housing Council en sus draft regulations regarding automated-decision systems. https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2022/03/AttachB-ModtoEmployRegAutomated-DecisionSystems.pdf

o facilitadas por sistemas de decisión automatizados pueden constituir una discriminación en virtud de la Ley[12].

El riesgo es aún mayor en el caso de algunos tipos de IA que utilizan técnicas en las que las herramientas de IA "aprenden" extrayendo patrones de los datos, en lugar de que los programadores decidan qué "proxies" son relevantes y qué peso darles. Los algoritmos resultantes son a menudo excesivamente complejos y completamente opacos, de tal manera que es difícil para los humanos su interpretación. Como consecuencia, los empleadores que confían en estos tipos de algoritmos no pueden ni siquiera conocer ni explicar las razones de sus selecciones. En todo caso, esta situación conduciría a una discriminación prohibida.

Los efectos que en el terreno que venimos analizando puede producir la introducción de algoritmos fueron puestos de relieve por el WP251, que subrayó los riesgos de estas fórmulas al señalar que: "la elaboración de perfiles y las decisiones automatizadas pueden plantear riesgos importantes para los derechos y libertades de las personas que requieren unas garantías adecuadas. Estos procesos pueden ser opacos. Puede que las personas no sean conscientes de que se está creando un perfil sobre ellas o que no entiendan lo que implica. La elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren (...). En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada". En esta línea se sitúa también la Recomendación CM/Rec (2020) que ha sentado que debe evitarse que los "desequilibrios sociales y laborales que aún no se han eliminado de nuestras sociedades no se perpetúen deliberada o accidentalmente a través de sistemas algorítmicos".

Lo cierto es que, aunque los ingenieros de software definen parámetros de análisis de minería de datos, crean los clusters, enlaces, y árboles de decisión que generan los modelos predictivos aplicados, los valores humanos están incrustados en cada paso en su diseño, por lo que el establecimiento de sistemas automatizados de decisión y los datos que les sirven de base pueden encontrarse sesgados en su origen, con lo que su tratamiento debe encontrarse sometido a importantes cautelas. La discriminación algorítmica en el acceso al empleo es

---

[12] Como también pone de manifesto el California's Fair Employment and Housing Council en sus drafts regulations regarding automated-decision systems.

una realidad y los derechos de los interesados deben contar con garantías reforzadas en estos casos. Así lo ha venido a subrayar el apartado VIII de la Carta de Derechos Digitales donde expresamente se señala que: "*Se fomentará que los procesos de transformación digital apliquen la perspectiva de género adoptando, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados*".

Las discriminaciones por razón de género han aparecido con especial intensidad en las primeras implementaciones de estos sistemas, pero los riesgos de ampliación a otras formas interseccionales, esto es, cuando concurren o interactúan diversas causas generando una forma específica de discriminación [en los términos de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación ("Ley 15/2022")], es más que evidente. Por poner el ejemplo más conocido, Amazon trató de crear un algoritmo para seleccionar candidatos potenciales para trabajos de desarrollador de software y otros puestos técnicos, pero lo abandonó después de apreciar que sistemáticamente solicitantes femeninas cualificadas eran excluidas. La razón de ello se encontraba en que sus modelos informáticos estaban entrenados para examinar a los solicitantes mediante la observación de patrones en los currículos enviados a la empresa durante un período de diez años. Durante este período la mayoría provenía de hombres, un reflejo del dominio masculino en la industria tecnológica[13].

Pero es importante tener presente que este tipo de resultados discriminatorios no pueden ser evitados simplemente eliminando de los algoritmos atributos especialmente protegidos como el género u otros factores discriminatorios. Cuando las herramientas de IA se construyen utilizando perfiles ricos en datos, pueden terminar confiando en distintos indicadores ("*proxies*") a la hora de concretar los criterios de selección. El concepto es relevante jurídicamente, porque esos indicadores son los presupuestos de hecho en cuya virtud se va a tomar una decisión[14]. Así, los algoritmos pueden tomar en consideración criterios adicionales como el lugar de residencia, que está estrechamente relacionado con determinadas circunstancias sociales o personales en muchas ciudades. Un algoritmo

---

[13] Dastin, J. *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*. https://perma.cc/T6NZ-T4ZW

[14] Huergo, A. (2021). "Una aproximación a los algoritmos desde el Derecho Administrativo", en AA.VV., *La regulación de los algoritmos*, Pamplona, Aranzadi, p. 45.

que clasifica a los candidatos según el código postal podría situar a numerosos colectivos en desventaja. Del mismo modo, un algoritmo de contratación que selecciona candidatos comparándolos con los empleados actuales puede discriminar si las prácticas pasadas del empleador excluyeron a ciertos grupos. Si, por ejemplo, el empleador tiene muy pocas mujeres trabajando como computadora o programadora, el algoritmo probablemente reproducirá ese patrón cuando trate de predecir las contrataciones más exitosas. De manera similar, un algoritmo que trate de maximizar el "ajuste cultural" recomendará a los solicitantes que son similares a los empleados actuales lo que podría excluir a los candidatos que no se adapten a ese patrón histórico[15].

3.2. Los algoritmos dirigen la empresa

3.2.1. La dependencia algorítmica

Pero la promesa de un trabajo hipereficiente da un paso adelante y se inserta también en la propia raíz del poder de dirección empresarial. Los algoritmos están pasando a convertirse en un instrumento básico en la ordenación y gestión de los poderes empresariales. Aunque el recurso a estas fórmulas contaba con antecedentes como criterio matemático de identificación y clasificación, lo cierto es que el desarrollo de estas técnicas permite no solo repetir un proceso mecánicamente, sino además aprender de la experiencia, redefinir las reglas e, incluso, como observábamos líneas atrás, poder llegar a independizarse de su creador a la hora de definir la toma de decisiones.

La "*on-demand economy*" representa la última ola de una también nueva economía digital y un terreno en el que los algoritmos han alcanzado un más extenso desarrollo. Este sector económico posee una amplia definición, pero son las plataformas "*gig*" las que concentran el interés en materia laboral, al permitir a los proveedores individuales proporcionar directamente sus servicios al mercado. Estas plataformas profesionales basan su actuación en algoritmos y, a través de los mismos, efectúan asignaciones de actividades a los profesionales incluidos dentro de las mismas. Los usuarios registrados son clientes de la plataforma y corresponde a esta elaborar una

---

[15] Ejemplos que se toman de Kim, P. T. y Bodie, M. T. (2021). *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, Journal of Labor and Employment Law, Vol. 35, núm. 2, pp. 294-296.

planificación perfecta que permite la asignación más eficiente entre la oferta y la demanda de servicios. En otras palabras, el sistema informático procede a la asignación de tareas asignando el servicio al profesional que en cada momento concreto reúna los requerimientos mejor adaptados a las necesidades del cliente.

En estas plataformas, las finalidades a las que sirven los algoritmos se concretan, esencialmente, en tres específicas funciones[16].

En primer lugar, procede a la asignación de la concreta actividad, de modo que a través de la app se asignan al prestador de servicios los trabajos más cercanos. El sistema funciona mediante el rastreo de la proporción de trabajos que el prestador ha aceptado y realiza un promedio de la evaluación/puntuación que los usuarios han otorgado a quien ha desarrollado el servicio. Se produce, en cierto modo, una cierta subasta de servicios que el algoritmo se encarga de coordinar.

En segundo lugar, estos sistemas asignan tarifas y modifican los precios de los servicios durante los picos de demanda. El precio está determinado por una tarifa estándar y fluctúa de acuerdo con un algoritmo de precios dinámico. Por ejemplo, cuando la demanda supera la oferta, los algoritmos de precios dinámicos lo aumentan hasta que se alcanza el equilibrio de mercado. Su extraordinaria capacidad de análisis les permite establecer precios dinámicos[17]. Como es obvio, su interés estriba no solo en la originalidad de su cometido, sino en su extraordinaria velocidad y precisión, al analizar una inmensa cantidad de datos. Pero este modo de gestión es bilateral. Los prestadores de servicios pueden utilizar también estos instrumentos para valorar de forma precisa el momento óptimo en el que prestar sus servicios, al poder controlar también los precios de los ofertantes.

Finalmente, el algoritmo permite la evaluación algorítmica del rendimiento puesto que estos sistemas permiten clasificar y valorar el grado de aceptación de la prestación de los servicios[18]. En efecto, entre las singularidades que ofrecen

---

[16] Kyung Lee, M., Kusbit, D., Metsky, E. y Dabbish, L. *Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers*. http://www.cs.cmu.edu

[17] Cuestión que también se proyecta en el ámbito mercantil, Pérez Hernández, A. (2019). "Algoritmos y derecho de la competencia: un estudio sobre la alineación automática de precios", *Revista de Derecho Mercantil*, núm. 311.

[18] Todolí Signes, A. (2020). *The evaluation of workers by customers as a method of control and monitoring in firms: Digital reputation and the European Union's regulation on data protection*, International Labour Review.

estas fórmulas se encuentra el establecimiento de sistemas para garantizar la confianza en los prestadores de servicios a través de la valoración de los usuarios. Es una práctica generalizada en todas estas plataformas la existencia de sistemas de evaluación de las tareas. A título de ejemplo, en las plataformas especializadas en transporte de viajeros, después de cada viaje, a los pasajeros y conductores se les da la oportunidad de evaluarse los unos a los otros en base a su experiencia durante el viaje. Es importante tener presente que el valor añadido del modelo de negocio empleado por las plataformas digitales se encuentra, también, en la capacidad de emplear la plataforma para extraer datos sobre el uso del servicio[19].

La "gestión algorítmica del empleo" se ha convertido en un elemento que puede ser utilizado, incluso para definir el propio concepto de trabajador[20]. Así, la Ley 12/2021 incorpora una nueva Disposición adicional vigesimotercera al ET de acuerdo con la cual: "Por aplicación de lo establecido en el art. 8.1, se presume incluida en el ámbito de esta ley la actividad de las personas que presten servicios retribuidos consistentes en el reparto o distribución de cualquier producto de consumo o mercancía, por parte de empleadoras que ejercen las facultades empresariales de organización, dirección y control de forma directa, indirecta o implícita, mediante la gestión algorítmica del servicio o de las condiciones de trabajo, a través de una plataforma digital". También camina por esta misma senda la Directiva para mejorar las condiciones laborales de las personas que trabajan a través de plataformas digitales[21], que sitúa en la dirección algorítmica uno de sus focos centrales de interés. La directiva hará más transparente el uso de algoritmos en la gestión de recursos humanos, prohibirá el uso de sistemas automatizados de seguimiento o toma de decisiones para el tratamiento de determinado tipo de datos personales de las personas que realizan trabajos en plataformas, como datos biométricos o su estado emocional o psicológico

---

[19] Srnicek, N. (2017). *Platform capitalism*, Cambridge, Polity Press, p. 47.

[20] Entre los muchos trabajos que han analizado los presupuestos de la laboralidad en estas relaciones, remito especialmente a Ginés I Fabrellas, A. (2021). *El trabajo en plataformas digitales. Nuevas formas de precariedad laboral*, Pamplona, Aranzadi.

[21] Resolución legislativa del Parlamento Europeo, de 24 de abril de 2024, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales [COM(2021)0762 – C9-0454/2021 – 2021/0414(COD)]. Profundizando y enmarcando la misma en una reflexión conjunta sobre el cambio digital, también D. Perez del Prado, *Derecho, Economía y digitalización*, Valencia, Tirant lo Blanch, 2023.

y, en fin, buscará garantizar la supervisión y evaluación humana de las decisiones automatizadas, incluido el derecho a que dichas decisiones sean explicadas y revisadas.

La "discriminación algorítmica en el empleo" puede ocupar también importantes espacios en este ámbito. Buen ejemplo es la sentencia del Tribunale Ordinario di Bologna, que en su sentencia de 31 de diciembre de 2020 (N. R.G. 2949/2019) declaró discriminatorio el algoritmo Frank utilizado por Deliveroo en su plataforma online para clasificar o definir el "ranking reputacional" de los riders[22]. Según quedó acreditado, los repartidores gozan de dos vías para recibir encargos de viajes por parte de la empresa: pueden reservar sesiones con antelación a través del sistema de reserva SSB ("Self-Service Booking") o pueden iniciar sesión en tiempo real. El sistema de reserva SSB proporciona a los riders un calendario de disponibilidad de la semana entrante para poder recibir encargos de viaje de acuerdo con un ranking (una clasificación) establecido. Los parámetros de dicha clasificación son la llamada "tasa de fiabilidad" (número de veces en el que el rider no atendió una sesión que previamente reservó) y la "tasa de participación en los picos" (número de veces en que el prestador estuvo disponible para los horarios más relevantes, es decir, de las 20 h. a las 22 h. de viernes a domingo). Sobre esta base, la empresa utiliza un algoritmo que, a juicio del referido Tribunal, penaliza de igual forma y sin distinción alguna tanto a los riders que se ausentan temporalmente por motivos injustificados como a los que lo hacen por motivos justificados de enfermedad, cuidado de menores o para ejercer su derecho de huelga. Tal diferencia, concluye el Tribunal, encubre una discriminación algorítmica en el empleo. Y llega a esta conclusión indicando que es indiferente que a los repartidores se les considere trabajadores por cuenta ajena o trabajadores autónomos, dado que en cualquiera de los casos estarán protegidos frente a la discriminación en el acceso al trabajo.

Pero el espacio de los algoritmos no solo se encuentra en las economías de plataforma. Estamos seguros de que los mismos están llamados a instalarse en

---

[22] Seguimos el excelente resumen que realiza de este pronunciamiento, Oliva León, R. *¿Es discriminatorio el algoritmo de Deliveroo que «rankea» a sus riders?*, https://www.algoritmolegal.com/tecnologias-disruptivas/es-discriminatorio-el-algoritmo-de-deliveroo-que-rankea-a-sus-riders/. Para una contextualización del pronunciamiento, Fernández Sánchez, S. (2020). *Relaciones laborales y derechos fundamentales en la era digital. Una visión desde el derecho italiano*, Temas Laborales, núm. 155, p. 188.

el conjunto de empresas como instrumentos a los que estas van a recurrir y por lo que están llamados a convertirse en un instrumento de gestión capaz de proyectar su uso sobre cualquier tipo y modelo de actividad económica. Pensemos en el uso que puede darse a los mismos en cualquier proceso de decisión que requiera elecciones complejas y uso masivo de datos: procesos de evaluación del desempeño y evaluación de objetivos tan utilizados a la hora de establecer sistemas de retribución variable. Aquí los riesgos tampoco desaparecen. La IA también puede producir resultados sesgados si se entrena con métodos sesgados. Un algoritmo entrenado usando las evaluaciones subjetivas de un supervisor sesgado hará predicciones sistemáticamente sesgadas del futuro desempeño laboral[23].

3.3. El control algorítmico del trabajo en la era del capitalismo de la vigilancia[24]

El control a través de sistemas de videovigilancia, microfónicos y telefónicos, el rastreo a través de sistemas de geolocalización; los controles biométricos; el control informático de los niveles de productividad de los trabajadores en tiempo real; el seguimiento de los correos electrónicos y de las navegaciones por internet, conforman una realidad en permanente transformación en la que la vigilancia empresarial se ha convertido en algo más impersonal, pero no por ello menos invasivo. Ciertamente, la idea de la empresa panóptica se hace cada vez más fuerte y los mecanismos de control y seguimiento empresarial adquieren nuevos contenidos y también nuevas dimensiones[25].

La importancia de esta materia aparece subrayada por el art. 88.2 RGPD cuando precisa que los tratamientos de datos en el ámbito laboral "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los

---

[23] Como señalan, Kim, P. T. y Bodie, M. T. (2021). *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, Journal of Labor and Employment Law, Vol. 35, núm. 2, p. 295.

[24] Parafraseando la conocida obra de Zuboff, S. (2020). *La era del capitalismo de la vigilancia*, Barcelona, Paidós.

[25] Una evolución que empecé a analizar en Mercader Uguina, J. R. (2001). "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones Laborales*, núm. 10, pp. 11-31. La idea del "panóptico" sigue siendo usada por la doctrina como muestra la obra de Fernandez Ramírez, M. (2021). *El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa "neopanóptica"*, Pamplona, Aranzadi.

interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a (...) los sistemas de supervisión en el lugar de trabajo". La LOPD ha venido a incorporar importantes novedades que se proyectan de forma especial en el ámbito que nos ocupa. Ha sido, sin duda, su Título X, en materia de garantías de los derechos digitales, en el que se ha puesto más intensamente el foco de atención. Garantías a las que se añadirían las que incorporase el futuro Reglamento sobre Ley de Inteligencia Artificial que, como venimos recordando, añade también entre los sistemas de alto riesgo los que "*se utilizan (...) para la asignación de tareas y el seguimiento o la evaluación de personas en relaciones contractuales de índole laboral*".

La introducción de nuevas tecnologías en el mundo laboral ha ayudado a reforzar la visión panóptica de la relación de trabajo, así como la idea de un remozado feudalismo virtual. El inspector que ve sin ser visto y los vigilados que no pueden escapar a la mirada vigilante y omnipresente que parece situarse en un mundo incorporal, aunque penetre en el mundo corporal hasta hacerlo transparente. Por ello, los límites a este control invasivo resultan especialmente relevantes en una relación donde los ojos empresariales se encuentran siempre presentes. El uso de algoritmos puede suponer un salto adelante en muchos de estos sistemas y son muchos los ejemplos.

3.3.1. La expansión del control biométrico

El desarrollo de la tecnología, en su más amplio y extenso sentido, está convirtiendo al cuerpo humano en un espacio de computación y, por tanto, de control. Como gustaba decir a los existencialistas, el cuerpo no es una pantalla entre yo y el mundo, sino que da forma a nuestra forma primaria de ser-en-el-mundo. El ser humano es una máquina (en la conocida expresión de Le Metrrie) en la que todos y cada uno de los factores anatómicos y actuaciones personales ligadas a su funcionamiento tienen señas diferenciales, propias y específicas, que hacen a cada individuo radicalmente distinto de todos los demás de su especie. Ello permite construir una métrica de cada concreto individuo: la biométrica. Y es que los sistemas biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación. Mientras que los datos biométricos de una persona pueden suprimirse o alterarse, la fuente de la que se han extraído en general no puede ser modificada ni suprimida. Los sistemas biométricos quedan, de este modo, referidos a características de los individuos que son universales

(todos los individuos las tienen), unívocas (distinguen a cada individuo), permanentes (en el tiempo y en distintas condiciones ambientales) y mensurables (son medibles de forma cuantitativa)[26].

La identidad biológica es propia de cada sujeto y, por tanto, cualquier instrumento que la utilice permitirá, a quien de él se sirva, internarse en el terreno más recóndito que cada ser humano tiene. Podría decirse que, a su través, se puede entrar en la intimidad de la intimidad. Ese carácter invasivo entraña numerosos riesgos para la dignidad humana, riesgos que alcanzan mayor voltaje si tenemos en cuenta que el uso de los sistemas biométricos se está convirtiendo, por momentos, en una potente herramienta de control empresarial[27]. No sorprende por ello que RIA mire con especial intensidad los usos biométricos de la IA. Un repaso de las categorías empleadas por el RIA en relación con estos sistemas ["datos biométricos" (art. 3.34), "identificación biométrica" (art. 3.35), "verificación biométrica" (art. 3.36), "sistema de reconocimiento de emociones" (art. 3.39), "sistema de categorización biométrica" (art. 3.40), "sistema de identificación biométrica remota" (art. 3.41), "sistema de identificación biométrica remota en tiempo real" (art. 3.42), o "sistema de identificación biométrica remota en diferido" (art. 3.43)] muestra su relevancia. Una relevancia que se proyecta sobre los distintos modelos que se vinculan con los también distintos niveles de riesgo. La era del capitalismo de la vigilancia supone un enorme desafío al que viene a tratar de poner coto esta norma.

En un libro de lectura imprescindible [*Ser o no ser (un cuerpo)*], Santiago Alba Rico señala cómo "millones de imágenes capturadas por cámaras ajenas o servidas por nuestros propios teléfonos móviles han acabado por depositarse en un mundo paralelo mucho más poblado y mucho más frecuentado que el de nuestros espacios corporales, y ello, añade, hasta el punto de que puede decirse sin exagerar que hoy son mucho más visibles nuestras imágenes que nuestros cuerpos". El resultado es que "el espejo ha triunfado sobre el cuerpo y se ha emancipado de él". Este nuevo dualismo entre el "cuerpo físico" (con su parte física y su dimensión emocional) y el "cuerpo imagen" nos debe hacer reflexionar sobre el

---

[26] Más extensamente me he ocupado de esta cuestión en "*El "big bang" de la biometría laboral. De la huella dactilar a los neurodatos*", Labos, 2024, Vol. 5, núm. 2, pp. 4-23.

[27] Buen ejemplo es el reconocimiento de las emociones, tema del que se ha preocupado Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*, Valencia, Tirant lo Blanch.

alcance de los retos que tenemos por delante y en los que el "cuerpo" en sus más diversas y plurales dimensiones cobra y cobrará un protagonismo esencial.

3.3.2. El control de la conducta del trabajador: Minority Report laboral

Un ámbito en el que, sin duda, el control algorítmico está llamado a tener un papel relevante es el trabajo a distancia[28]. En el teletrabajo interactivo, el trabajador se encuentra expuesto a vigilancia directa en tiempo real y, en otros casos, sin conexión telemática, este control también es posible, aunque diferido en el tiempo, mediante la utilización de determinados programas *in accounting*. El control computerizado, especialmente utilizado sobre trabajadores informáticos, permite a los supervisores efectuar chequeos periódicos a la actividad del supervisado controlando el número de tecleos por minuto, el número de errores y el tiempo total pasado en el ordenador. En efecto, el llamado *software "in accounting"* permite, previa identificación personal del operador, memorizar el número de operaciones efectuadas por el mismo, el número de errores cometidos al efectuarlas, el tiempo empleado para cada una, el tiempo total de trabajo, la memoria utilizada, el número de frecuencia y la duración de las interrupciones. El seguimiento algorítmico puede llevar consigo soluciones excesivamente invasivas y, por ende, desproporcionadas, que conlleven una vulneración de la intimidad de las personas al producir una parametrización integral del trabajador. Una reforzada exigencia de proporcionalidad deberá, sin duda, requerirse cuando las empresas acudan a este tipo de sistemas.

Un terreno en el que está llamado a proyectarse el control mediante algoritmos de la actividad laboral es el de las amenazas internas (*Insider Threat*). Las mismas tienen por finalidad prevenir, identificar y mitigar las amenazas internas que tengan su origen en las propias personas trabajadoras, que de forma consciente o inconsciente puedan comprometer la actividad empresarial en procesos esenciales de su actividad. De este modo, y a través de la ponderación de una serie de indicadores, los algoritmos predicen la posibilidad de que exista o no una amenaza. Sobre esta base, la empresa podrá tomar medidas adicionales de control sobre los trabajadores que queden identificados. Un modelo de intervención que entra de lleno en las situaciones de alto riesgo

---

[28] Casas Baamonde, M. E. (2020). "El Derecho del Trabajo, la digitalización del trabajo y el trabajo a distancia", *Derecho de las relaciones laborales*, núm. 11, pp. 1413-1437.

("*seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones*") que, como venimos diciendo, identifica el futuro Reglamento sobre Ley de Inteligencia Artificial. Este tipo de instrumentos son mirados con reticencia y algunos análisis recomiendan que se debe prohibir a los empleadores hacer inferencias sobre el desempeño de un trabajador. Del mismo modo, se afirma que las empresas no deberían utilizar fórmulas algorítmicas para predecir o emitir juicios sobre el desempeño de un trabajador, sus emociones, personalidad o salud[29].

Los algoritmos pueden colaborar a reconstruir el ser más profundo de los trabajadores a través de métodos de gestión digitalizados que permiten integrar datos, patrones e interacciones cibernéticamente esparcidas por ellos con el uso de los sistemas informáticos dentro y fuera de la empresa. Nuestro rastro algorítmico compone, al fin y a la postre, nuestro ser social y laboral. Los riesgos del desarrollo de estas nuevas fórmulas se proyectan como sombras en el ámbito empresarial al permitirse una mayor capacidad de transmisión de datos y de combinación de los mismos, con el peligro añadido de la descontextualización de la información, lo que puede crear un clima psicosociológico de control e invasión de su privacidad, esto es, la conciencia en los trabajadores de poder ser conocidos en todos los aspectos de su personalidad, el trabajador se hace plenamente transparente.

3.4. La neurotecnología llega al lugar de trabajo

Los riesgos de la neurovigilancia laboral no es una cuestión nueva. La persona trabajadora está y ha estado particularmente expuesta a estos controles a través de los test psicológicos, pruebas grafológicas, detectores de mentiras, polígrafos y otras técnicas de exploración de la personalidad que se utilizan o han sido utilizados en los procesos de selección de personal y durante la ejecución de la prestación laboral. No sorprende, por ello, que la Recomendación núm. 150 de la OIT sobre el desarrollo de recursos humanos de 1975 (hoy sustituida por la 195 de 2004), estableciera limitaciones al uso de pruebas de aptitud que utilizasen factores psicológicos, ni que en 1988 se dictase en Estados Unidos una Ley específica –la Employee Polygraph Protection Act– que contenía limitaciones, tanto respecto al ámbito de utilización, como respecto del método de uso del polígrafo.

---

[29] Bernhardt, A., Kresge, L. y Suleiman, R. (2021). *Data and Algorithms at Work: The Case for Worker Technology* Rights, UC Berkeley Labor Center, p. 23.

Pero lo cierto es que esa tendencia es cada vez más expansiva e invasiva. El uso de la tecnología wearable habitualmente referenciada como WT (*Wearable Technology*), y los dispositivos asociados como WD (*Wearable Devices*) o, simplemente, wearables, que capturan sensores o técnicas afines, información sobre el funcionamiento cerebral a través de las señales nerviosas, lo pone de manifiesto. A modo de ejemplo, recientemente se ha advertido sobre el uso de pulseras en conductores del transporte público de Pekín con el fin de registrar sus estados emocionales durante su jornada A ello se unen fórmulas de contenido diverso como los cascos de seguridad o gorras que forman parte del uniforme que permiten monitorear en forma permanente las ondas cerebrales del trabajador, los auriculares multipropósito o los escaneos faciales que, de forma inédita, facilitan la obtención masiva de datos de las personas trabajadoras a partir de la observación de su actividad cerebral. A ello se une la capacidad de estos dispositivos para la recopilación simultánea de datos del corazón, la piel, los músculos, los ojos y el cerebro del usuario, y la combinación de esta capacidad con dispositivos de realidad aumentada y virtual, lo que proporciona nuevas formas de interactividad y control en tiempo real.

El RIA ha venido a prohibir expresamente, entre otras cosas: la IA manipuladora y la IA que explota las vulnerabilidades de una persona o de un grupo de personas. Señala el artículo 5.1 f) RIA: "*Quedan prohibidas las siguientes prácticas de IA: (...) La introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad*". Y es que los juicios y cogniciones afectan a las emociones y son la causa de que estas tengan lugar. En suma, son disposiciones mentales que generan actitudes y estas pueden ser objeto de control, valoración y seguimiento.

Existe, por ello, un vínculo estrecho entre los sistemas neurotecnológicos y los datos personales de la persona trabajadora en la medida en que los primeros se alimentan de los neurodatos[30]. Existe evidencia que indica que estos datos permiten identificar de forma única a las personas, por lo que, sin lugar a duda, los neurodatos de los seres humanos son datos personales. Los mismos que han sido definidos como la información que se recoge del cerebro y/o del sistema nervioso, pueden

---

[30] "Los neuroderechos laborales: la neurotecnología llega al lugar de trabajo", *Trabajo y Derecho*, 2024, núm. 117 (septiembre 2024), en colaboración con Ramos Quintana, M. I.

venir a constituir una categoría diferenciada y cualificada de los datos biométricos en tanto que datos que pertenecen únicamente al dominio del cerebro. En 2019, la OCDE en el primer instrumento jurídico internacional sobre neurotecnología definió los datos cerebrales personales como "*datos relacionados con el funcionamiento o la estructura del cerebro humano de un individuo identificado o identificable que incluye información única sobre su fisiología, salud o estados mentales*".

La ingente recolección de datos llevada a cabo por las neurotecnologías, junto con su creciente difusión, anticipa la creación de bases de datos masivas de neurodatos. No sorprende por ello que alguna de las primeras respuestas para afrontar este nuevo reto se centre en el control y limitación del tratamiento de esta categoría especial de datos. Así en Brasil, el Projeto de Lei 522/2022 que modifica a Lei núm. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), se dirige a regular los límites de este tipo particular de datos biológicos. El proyecto normativo parte de la definición de dato neuronal como "*cualquier información obtenida, directa o indirectamente, de la actividad del sistema nervioso central y cuyo acceso se realiza a través de interfaces cerebro-computadora, o cualquier otra tecnología, invasiva o no invasiva*". En Estados Unidos esta senda es seguida por la enmienda a la California Consumer Privacy Act, actualmente en tramitación, que incorpora el concepto de "*datos neuronales", entendiendo por tales: "la información generada por la medición de la actividad de los sistemas nerviosos centrales o periféricos de un individuo*". De igual modo, el 17 de abril de 2024, la Cámara de Representantes y el Senado de Colorado aprobaron un proyecto de ley para proteger la privacidad de los datos biológicos y neuronales de las personas. La futura modificación de la "Colorado Privacy Act" amplía la definición de "datos sensibles" para incluir los datos biológicos, que son "*datos que proporcionan una caracterización de las propiedades, composiciones o actividades biológicas, genéticas, bioquímicas o fisiológicas del cuerpo o las funciones corporales de una persona*". Los datos biológicos incluyen los datos neuronales, definidos como la "*información relativa a la actividad del sistema nervioso central o de los sistemas nerviosos periféricos de una persona, incluidos el cerebro y la médula espinal, y que pueden procesarse mediante un dispositivo o con su ayuda*".

En el ámbito europeo todavía no nos hemos enfrentado frontalmente con esta cuestión, pero alguno de los fundamentos sobre los que se asienta nuestra normativa en materia de protección de datos marca el rumbo sobre la necesidad de introducir importantes precauciones y limitaciones en el uso de los datos neuronales.

4. INTELIGENCIA ARTIFICIAL Y SEGURIDAD Y SALUD EN EL TRABAJO

No obstante, no todo es negativo en este escenario que parece anunciar la definitiva muerte de la privacidad. Los algoritmos también pueden ayudarnos. Como en su reciente informe ha señalado la Agencia Europea para la Seguridad y Salud en el Trabajo, "*Estudio prospectivo sobre riesgos nuevos y emergentes para la seguridad y salud en el trabajo asociados a la digitalización en 2025*", estos nuevos sistemas pueden facilitar la comprensión de los problemas relativos a la seguridad y salud en el trabajo, la toma de mejores decisiones y la predicción de los problemas en materia preventiva antes de que ocurran, así como pueden favorecer intervenciones más oportunas y eficaces. La IA ha facilitado la aparición de nuevas formas de seguimiento y gestión de los trabajadores. Estas tecnologías digitales permiten formas nuevas, generalizadas, continuas y de menor costo de control y gestión de los trabajadores basadas en la recopilación de grandes cantidades de datos en tiempo real sobre los trabajadores.

De este modo, algunas compañías han empezado a trabajar en la creación de programas destinados a analizar los datos y predecir probabilidades con el fin de reducir la cifra de accidentes laborales. Por ejemplo, Suffolk, una empresa constructora estadounidense está creando un algoritmo que analiza fotografías de los lugares de trabajo y las analiza para localizar los riesgos potenciales de seguridad. Además, también busca infracciones por parte de los trabajadores tales como la falta de uso de equipo protección y el incumplimiento de protocolos de seguridad. Una vez que el algoritmo posee esta información, la relacionará con los accidentes y será capaz de prevenirlos[31]. Suffolk también está escribiendo un algoritmo que analizará información de una variedad de fuentes, incluyendo 10 años de datos de sus archivos, y pronosticará retrasos en el proyecto, información que podría ser comunicada a los propietarios de edificios y subcontratistas. El consorcio también está explorando formas de utilizar datos de sensores automáticos conectados a internet para aumentar la eficiencia. Una idea es rastrear la ubicación de los camiones de sus proveedores en concreto para que los trabajadores estén listos para verter el hormigón tan pronto como lleguen los camiones y así ahorrar tiempos en los procesos.

---

[31] https://www.lr21.com.uy/tecnologia/1371181-inteligencia-artificial-construccion-industria-evitar-accidentes

No obstante, el control permanente plantea también dudas legales. Así se ha cuestionado si resulta viable laboralmente el establecimiento de un sistema de geolocalización que favorezca la prevención de riesgos laborales del trabajador (evitar que, ante la dificultad de desarrollar con normalidad la actividad de vigilancia y control en materia de prevención de riesgos laborales, algún trabajador sufra un accidente de trabajo). Ejemplo de ello es el sistema Lone Worker Connect, por medio del cual la empresa instalaría una app en el teléfono del empleado que convierte su móvil en un dispositivo de alerta y detección de caídas. Dicho sistema es capaz de detectar accidentes por tres vías redundantes: aceleración, inclinación y no-movimiento. Además, su sistema de geofencing permite establecer barreras virtuales y perimetrar zonas de acceso restringido o determinar áreas donde deben encontrarse los trabajadores sin salir de ellas. La aplicación la puede desconectar el mismo empleado al terminar su turno, dejando de esta manera de estar geolocalizado.

Una medida como la propuesta no resulta en sí misma invasiva ni afecta a los derechos de dignidad e intimidad, siempre que se articule su uso de forma proporcionada lo que exigiría que la misma se proyecte, exclusivamente, sobre aquellos trabajadores que realicen actividades en un contexto que impida un contacto inmediato y directo con otras personas caso de concurrir un evento dañoso para su seguridad o su salud y siempre que la información obtenida no produzca otros efectos que los estrictamente vinculados a la tutela y prevención de riesgos profesionales. El establecimiento de la app en el teléfono personal del trabajador debería derivar del voluntario y expreso consentimiento del trabajador. Para su adecuada implantación, la empresa debería informar previamente a los trabajadores sobre su establecimiento, así como sobre las condiciones o reglas de funcionamiento y las medidas que se adoptarán para garantizar su efectiva aplicación en línea con lo previsto en el art. 90.1 LOPD. En todo caso, la AEPD ha recomendado evitar el diseño de sistemas con la orientación "palanca del hombre muerto" y dar siempre la opción de que un operador humano pueda ignorar el algoritmo en un momento dado, procedimentalizando aquellas situaciones en las que debe optarse por este modo de actuar[32].

---

[32] AEPD (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, Madrid, p. 44.

A su vez, los algoritmos permiten estudiar también datos recabados a través de ropa inteligente y otros accesorios (*wearables*). La tecnología wearable es habitualmente referenciada en la jerga tecnológica como WT (*Wearable Technology*), y los dispositivos asociados como WD (*Wearable Devices*) o, simplemente, wearables. En castellano, es habitual acompañar a estos dispositivos con los adjetivos "tecnológico" o "inteligente": chaqueta tecnológica, reloj inteligente, etc.[33] Señala el GT29, en el citado WP 249, en relación con los *Wearable* devices, que los empleadores están cada vez más tentados de proporcionar dispositivos portátiles a sus empleados con el fin de rastrear y registrar su salud y actividad dentro, y algunas veces incluso fuera del lugar de trabajo. Lo cierto es que, a través de estos sistemas, los empresarios podrían además fomentar el uso de estos dispositivos durante el tiempo de ocio, para medir los patrones de sueño y los niveles de ejercicio, basándose en su posible vinculación con la productividad y con comportamientos ligados a la idea de empresa saludable. El riesgo está en el acceso y control a datos especialmente sensibles: los relativos a la salud de los trabajadores. Datos en relación con los cuales el RGPD establece como principio general la prohibición de tratamiento.

La IA también incorpora nuevas amenazas y nuevas formas de acoso tecnológico[34]. Como acertadamente se ha dicho, "la IA pueden generar nuevos riesgos de carácter psicológico o de estrés mental en tanto que, como hemos ya señalado, una de las formas de actuación de los dispositivos inteligentes es la capacidad de analizar constantemente (24 horas/7 días a la semana) la conducta del trabajador. Esta capacidad, más allá de problemas de estrés mental, puede incluso generar el riesgo de que los trabajadores adapten su conducta según la actuación del dispositivo, apareciendo comportamientos de dependencia o alienación tecnológica que afecten al trabajador de manera profesional y personal. La mayor intensidad del trabajo y el trabajar con una máquina que progresivamente va siendo más inteligente –generando para el empleado una especie de desafío constante– puede derivar en patologías de carácter psicosocial"[35]. Y es que la

---

[33] Al respecto, J. Baz Rodríguez, en su excelente estudio, *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid, Bosch, 2019.

[34] Ampliamente analizadas por Molina Navarrete, C. (2019). *El ciberacoso en el trabajo. Cómo identificarlo, prevenirlo y erradicarlo de las empresas*, Madrid, Wolters Kluwer.

[35] Del Rey Guanter, S. "Inteligencia artificial y relaciones laborales: algunas implicaciones jurídicas", AA. VV. (2021), *Los desafíos del Derecho del Trabajo ante el cambio económico y social. Libro en Homenaje a Federico Durán*, Madrid, Iustel, pp. 195-196.

hiperconectividad que conllevan estos sistemas obliga a realizar una reflexión muy profunda sobre el tiempo de trabajo en la era de la digitalización máximo cuando la desconexión es una idea que, lentamente, está cobrando forma.

5. ¿PUEDEN DESPEDIR LOS ALGORITMOS?

Los algoritmos están aterrizando también en el ámbito de los despidos y la realidad lo pone de manifiesto. Xsolla, la filial rusa de una empresa de *software* y servicios interactivos con sede en Los Ángeles, ejecutó una vanguardista reestructuración de su plantilla siguiendo únicamente el dictamen de un algoritmo de rendimiento laboral que los consideraba "improductivos" y "poco comprometidos" con los objetivos de la empresa[36]. Jeff Bezos afirmaba que las únicas decisiones empresariales que es imprescindible dejar en manos de seres humanos son "las estratégicas". El resto, las decisiones "cotidianas", por trascendentes que resulten, es preferible que las tomen algoritmos de IA, porque actúan "teniendo en cuenta toda la información relevante y sin interferencias emocionales".

Aun tratándose de realidades normativas distantes y con difícil acomodo en la nuestra, lo cierto es que algoritmos se están ganando espacios, por ejemplo, en el ámbito de la selección de los trabajadores afectados por un despido colectivo. Ejemplo de ello es la STS de 25 de septiembre de 2018[37], en la que la selección se realizó aplicando la Skill Competence Matrix, un programa evaluativo dirigido a garantizar que las personas que permanezcan en la plantilla de la empresa son las que tienen mejor valoración y un más elevado índice de polivalencia, cuyo funcionamiento se describe del siguiente modo: herramienta informática, en forma de tabla donde se valoran las capacidades técnicas de la plantilla, considerando solamente la mano de obra directa. El recurso a sistemas de objetivización en la identificación de los trabajadores afectados por el despido puede resultar, por supuesto, una fórmula útil y eficiente pero su tratamiento, como se ha advertido respecto de otros usos laborales de los algoritmos, "debe someterse a las debidas cautelas para evitar que la identificación de los trabajadores afectados por el

---

[36] https://elpais.com/icon/2021-10-10/150-despidos-en-un-segundo-asi-funcionan-los-algoritmos-que-deciden-a-quien-echar-del-trabajo.html. Véase también el caso de Amazon, Klecher, C. 'How Amazon automatically tracks and fires warehouse workers for 'productivity', https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivityfiring-terminations

[37] ECLI: ES:TS:2018:3463.

despido genere riesgos de discriminación o, sin llegar tan lejos, seleccione trabajadores sin atender a las razones que originan la medida de reestructuración". Es preciso," si estos sistemas se utilizan para seleccionar a los trabajadores afectados por el despido, que el algoritmo forme parte de período de consultas, de modo que se asegure la transparencia en su diseño e incluso la participación de los trabajadores para definir la lógica aplicada en el sistema"[38].

¿Calcularán las indemnizaciones los algoritmos? No hace falta recordar que estamos en un tiempo en que el modelo de indemnizaciones tasadas se observa con desconfianza. Dicho modelo indemnizatorio es rígido y no graduable en relación a diversos parámetros (como la antigüedad en el empleo). Se niega, además, cualquier posibilidad al juzgador de tomar en cuenta las circunstancias concretas de cada caso, algo que para el Tribunal italiano es necesario para poder "personalizar" el daño sufrido por la parte trabajadora y adoptar la decisión que se estime más adecuada sobre la cuantía resarcitoria. La cuestión está en saber si en el "Estatuto de los Trabajadores del siglo XXI" la indemnización por despido terminará estando definida en función de una pluralidad de factores integrados algorítmicamente.

6. HACIA UNA ADMINISTRACIÓN SOCIAL ALGORÍTMICA

La racionalidad de la Administración, en la clásica expresión de Max Weber, inevitable y progresivamente burocrática, es la piedra de toque no solo del Estado moderno, sino también de la economía moderna que necesita de una administración permanente, rigurosa y calculable. Un alto grado de eficacia cuasimecánica, una racionalidad técnico formal basada sobre relaciones institucionales fijas, divisiones funcionales claras, procedimientos regulares que requiere que la Administración funcione con una eficacia "maquinal"[39] de modo que los

---

[38] De La Puebla Pinilla, A. (2021). *El despido por causas empresariales*, XXXI Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social. Reestructuraciones empresariales, Madrid, MTES, p. 206.

[39] Weber, M. utilizó con frecuencia el ejemplo de las máquinas para analizar la naturaleza de la organización burocrática. Como una máquina, la burocracia es el sistema más racional de acumular energías para el cumplimiento de determinadas tareas. El miembro de la burocracia es solo un engranaje más en el mecanismo del movimiento perpetuo que le asigna una ruta esencialmente fija". Al igual que una máquina puede ponerse al servicio de muchos amos distintos, como pone de relieve Giddens, A. (1997). *Política y sociología en Max Weber*, Madrid, Alianza Editorial, p. 75. Sobre la idea de la eficacia "maquinal" de la Administración, González García, J. M. (1989). *La máquina burocrática (Afinidades electivas entre Max Weber y Kafka)*, Madrid, Visor.

funcionarios dirijan metódicamente su conducta hacia el recto cumplimiento de las atribuciones oficiales fijadas por las normas. Pero hay algo más. La burocracia debe proceder según "criterios objetivos", reglas generales previsibles, sin odio y sin pasión, sin amor y sin entusiasmo. "Su finalidad la desarrolla en su mayor grado cuanto más se "deshumaniza", cuanto más completamente alcanza las peculiaridades específicas que le son contadas como virtudes: la eliminación del amor, del odio y de todos los elementos puramente personales, de todos los elementos irracionales que se retraen al cálculo"[40].

La digitalización y la Administración electrónica han servido hasta el momento para favorecer la comunicación entre la Administración y los ciudadanos sobre todo a la hora de presentar solicitudes y escritos, recibir notificaciones y facilitar la firma electrónica. Su objetivo es agilizar los procedimientos administrativos y reducir los tiempos de tramitación, en definitiva, mejorar la eficiencia administrativa. Ahora estamos comenzando a andar también el camino de la Administración algorítmica, una Administración basada en el uso de la inteligencia artificial que permita prevenir y combatir el fraude y las ilegalidades[41].

Para el eficaz funcionamiento de estos sistemas en el ámbito público es esencial la colaboración entre las distintas administraciones. En España, las normas legales habilitan esta comunicación y son múltiples los Convenios entre entidades públicas que están sirviendo para construir un Big data público que nutra los sistemas algorítmicos y de IA que se están implantando. El Derecho español vigente incorpora diversas normas que establecen controles y cautelas respecto al uso de algoritmos, el art. 41.1 Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público entiende por decisión administrativa automatizada "*cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público*", de modo que dicha regulación no se aplicará a los casos en que esta intervención sea auxiliar, complementaria o previa a la decisión final. No faltan razones a quienes han afirmado que "esta regulación ha nacido vieja, porque está pensada para algo que

---

[40] Weber, M. (1984). *Economía y Derecho (Sociología del Derecho)*, en *Economía y Sociedad*, México, FCE, p. 732.

[41] De este tema se ocupa más ampliamente en Mercader Uguina, J. R. *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., pp. 111-156.

era muy novedoso hace décadas, pero no tiene en cuenta que ahora los verdaderos riesgos están en el contenido de las decisiones y no sólo en la forma en que ven la luz" ([42]). Igualmente, el art. 23 de la Ley 15/2022 establece que las administraciones públicas "*priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos*", y "*abordarán su potencial impacto discriminatorio*".

Las Administraciones públicas deben promover el uso de una inteligencia artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea. La implantación de sistemas de IA debe realizarse, por ello, a la luz de la normativa europea en materia de protección de datos personales que se encuentra integrada por el Reglamento General de Protección de Datos Personales, el Reglamento de Libre Circulación de Datos no Personales, Reglamento de Gobernanza de Datos y la Directiva relativa a los datos abiertos y la reutilización de la información del sector público. Papel esencial tendrá también el RIA, cuyo objetivo declarado es promover la adopción de una inteligencia artificial centrada en el ser humano y fiable y garantizar un elevado nivel de protección de la salud, la seguridad, los derechos fundamentales, la democracia y el Estado de Derecho frente a los efectos nocivos de los sistemas de inteligencia artificial en la Unión, apoyando al mismo tiempo la innovación.

La IA está cada vez más presente como instrumento de predicción en las actuaciones de la Administración Social española. Los ejemplos son múltiples. La Tesorería General de la Seguridad Social lleva desarrollando desde hace años un sistema que permite evaluar el riesgo de que una empresa sea ficticia, de que pueda producir altas fraudulentas, que permite detectar el fraude organizado, o la tendencia hacia la morosidad y probabilidad de insolvencia de determinadas empresas. Los sistemas de IA se han puesto también al servicio de la gestión y control de las prestaciones de incapacidad temporal por el Instituto Nacional de Seguridad Social y no se descarta su uso futuro para la calificación de las situaciones de Incapacidad permanente. El Servicio Público Estatal de Empleo utiliza un sistema de perfilado estadístico de desempleados para una más eficaz búsqueda de empleo.

---

[42] Huergo, A. (2021). *Administraciones Públicas e inteligencia artificial: ¿más o menos discrecionalidad?*, El Cronista del Estado Social y Democrático de Derecho, núms. 96-97, pp. 78-95.

El uso de la IA puede producir importantes beneficios en el ámbito de la potestad sancionadora de la Administración. Por un lado, permite un uso más eficiente de los recursos públicos en la medida de que cada día se aprueban más las normas que establecen infracciones y sanciones y los medios personales y materiales de los que dispone la Administración no crecen en la misma proporción. La IA facilita un Derecho también granular, esto es, de un Derecho adaptado a las concretas circunstancias de cada caso. Y, en fin, a través de la reutilización y aprovechamiento de los datos permite definir planes de lucha contra el fraude cada vez más precisos.

El uso de la IA en el ámbito público puede articularse a través de distintos niveles que llevan consigo respuestas jurídicas diferenciadas, aunque su proximidad es evidente. Por un lado, actuaciones automatizadas sin inteligencia artificial. En este caso, existe actuación automatizada porque el acto se dicta sin intervención humana, pero no hay inteligencia artificial o predicción algorítmica porque el contenido del acto resulta de unos hechos establecidos en la norma y de la regla legal prevista en ella. En segundo término, la predicción algorítmica sin actuación automatizada o modelos semiautomatizados. En estos casos los sistemas de IA se utilizan como instrumento predictivo, si bien la predicción no se aplica por sí sola, automáticamente, sino que se limita a ser un elemento que tenga a su alcance el titular del órgano que deba dictar la decisión como un informe más. Y, en último término, la vigilancia predictiva que consiste en utilizar los sistemas de IA para tratar de determinar el riesgo de que determinadas personas cometan infracciones o reincidan en su comisión, o para predecir su comisión o reiteración. Los riesgos de esta policía predictiva al estilo del programa Pre Crimen de la conocida película "Minority Report" son evidentes.

Sobre esta base se hace necesario reflexionar si es viable y conveniente la utilización de sistemas automatizados en todas las infracciones laborales o solo en relación con algunas de ellas y si los mismos deben operar en relación con todas las fases del procedimiento sancionador o solo en relación con algunas de ellas[43].

---

[43] Para un análisis integral de estas cuestiones me remito a Goerlich Peset, J. M., *Decisiones administrativas automatizadas en materia social: algoritmos en la gestión de la Seguridad Social y en el procedimiento sancionador*, Labos, 2021, Vol. 2, núm. 2, pp. 22-42.

En principio, es posible considerar que no todas las infracciones administrativas son susceptibles de automatización. Por lo que cabría entender que tales procesos deberían quedar reservados a aquellas en las que su valoración jurídica no requiere de una intervención caso por caso del Inspector; especialmente todo cuanto afecta al cumplimiento de datos documentales o formales y de cumplimiento dentro de determinados plazos. Tales infracciones se podrían automatizar sin mayor reparo, por cuanto que la valoración jurídica es un resultado automático de hechos formales constatados. Mayores matices requiere su concreción en las distintas fases del procedimiento sancionador:

En la fase de iniciación es donde tiene mayor impacto y eficacia la utilización de los *big data* a disposición de la Administración, incluso el cruce de datos entre diversas Administraciones Públicas. En esta fase ha de admitirse la capacidad de la Administración de sacarle todo el partido posible a los datos de los que dispone sea a través de fórmulas automatizadas con y sin sistemas de IA asociados[44].

En la fase de instrucción la Inspección despliega labores diversas en las que el tratamiento masivo de datos es una vía cada vez más relevante y, como tal, puede desembocar en tratamientos automatizados. Pero es necesario introducir matices. Allí donde la valoración jurídica requiera un razonamiento humano o incorpore elementos de discrecionalidad será necesario reflexionar sobre cuál deben ser los límites que deben imponerse al uso de la IA. A título de ejemplo, en Alemania. la Ley Federal de Procedimiento Administrativo establece que: "*La producción automatizada de actos administrativos es admisible siempre que lo haya autorizado una norma jurídica (legal o reglamentaria) y no exista discrecionalidad ni margen de apreciación*". Conviene advertir también que el uso de sistemas predictivos de IA puede abrir nuevos usos como, por ejemplo, permitir una más precisa aplicación de las reglas de graduación de las sanciones administrativas adaptadas a las particulares circunstancias de cada caso. Igualmente, el derecho de defensa del administrado debe ser tutelado y la facultad de presentar alegaciones en el procedimiento deberá seguir siendo respetado aun cuando nos encontremos ante sistemas plenamente automatizados.

Por lo que se refiere a la fase de resolución, es muy difícil que en estos supuestos se pueda producir una decisión del órgano competente por medio de una

---

[44] Cruz Villalón, J. *Algoritmo, digitalización y sanciones laborales "automatizadas"*. http://jesuscruzvillalon.blogspot.com/2021/03/algoritmo-digitaliacion-y-sanciones.html

actuación plenamente automatizada. No obstante, sí sería posible una resolución de este tipo en aquellos casos en los que no se hubiesen formulado alegaciones por el interesado o bien las mismas se hubiesen presentado fuera de plazo. En todo caso, la exigencia de motivación y transparencia resulta imprescindible cuando se utilizan sistemas de IA o algorítmicos. Su falta fue una de las causas en las que se sustentó la importante Sentencia del Tribunal de Distrito de La Haya de 5 de febrero de 2020, que declaró contrario al art. 8 CEDH, el uso del algoritmo SyRI utilizado por autoridades públicas holandesas para predecir la probabilidad de fraude a la Seguridad Social por parte de los solicitantes de beneficios estatales.

Naturalmente la implantación de estos sistemas requerirá de un elevado nivel de cautelas y garantías que permitan a los ciudadanos entender y comprender, cómo y porqué se han adoptado las decisiones que les afectan. En suma, se trata de evitar que la IA al servicio de lo público resulte para las personas una "caja negra". Como puso de relieve una importante sentencia del Consejo de Estado italiano (8 de abril de 2019) la regla técnica que gobierna cualquier algoritmo "no deja de ser una regla administrativa general", que es elaborada por un ser humano, aunque se aplique por una máquina. De modo que "la regla, aun definida de forma matemática, posee pleno valor jurídico y administrativo. Y está sometida a los principios generales de la actividad administrativa: publicidad, transparencia, razonabilidad y proporcionalidad".

Es cierto por ello que debe valorarse el alcance y los efectos que su utilización puede producir sobre instituciones clave del procedimiento sancionador: comprobación directa por el funcionario actuante; valor del principio de presunción de certeza de las actas; afectación al principio de contradicción y defensa y, en fin, los riesgos que entraña la "discriminación algorítmica de la Administración". La exigencia de garantías reforzadas para el uso de los sistemas automatizados viene requerida por el Reglamento General de Protección de Datos en particular de su artículo 22 (relativo a las decisiones individuales automatizadas) y por los pronunciamientos del Tribunal de Justicia de la Unión Europea que están ayudando a definir su alcance. Particularmente importante es la reciente STJUE de 7 de diciembre de 2023, Asunto Schufa, en la que consideró que el pronóstico sobre la probabilidad de un comportamiento futuro de una persona para el reembolso de un préstamo constituye una decisión automatizada a efectos del RGPD.

La IA está llamada a convertirse en una herramienta esencial para el desarrollo de la actividad de la Inspección de Trabajo. Su uso requerirá, en línea con las

exigencias y garantías impuestas por la normativa comunitaria, de un desarrollo legal preciso y detallado, que garantice los derechos de los ciudadanos, especialmente en el campo de la protección de datos personales, la transparencia, y la igualdad de trato y no discriminación. Creo, por todo ello, que, frente a las muchas reticencias frente al uso público de la IA, hay que tener una disposición favorable y no obstaculizadora, pero firmemente garantista.

7. REGULANDO LOS ALGORITMOS: DIMENSIONES LABORALES DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

Después de un largo período de tramitación y tras sortear variados obstáculos, el Parlamento Europeo ha dado luz verde al RIA. Una norma cuyo objetivo declarado en su primer artículo es promover la adopción de una IA centrada en el ser humano y fiable y garantizar un elevado nivel de protección de la salud, la seguridad, los derechos fundamentales, la democracia y el Estado de Derecho frente a los efectos nocivos de los sistemas de inteligencia artificial en la Unión, apoyando al mismo tiempo la innovación. Su escalonada entrada en vigor (art. 113 RIA) permitirá su adecuada comprensión, pero, a su vez, esta vigencia diferida tendrá que luchar contra el acelerado cambio que vive esta materia donde el futuro se convierte en pasado a enorme velocidad[45].

El RIA otorga carácter de principio a lo que denomina "*alfabetización en materia de inteligencia artificial*" que enuncia en su art. 4 y conceptúa en el art. 3.56 del siguiente modo: "*Los proveedores y responsables del despliegue de sistemas de IA* (en el caso laboral, los empleadores) *adoptarán medidas para garantizar que, en la mayor medida posible, su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los grupos de personas en que se utilizarán dichos sistemas*". Como precisa el Considerando 20, "*la alfabetización en*

[45] Mercader Uguina, J. R. "El Reglamento de Inteligencia Artificial: frecuentemos el futuro", Brief AEDTSS 42/2024. También me he ocupado de este tema en relación con las fases finales del RIA, en concreto, en "El Reglamento de Inteligencia Artificial entra en la recta final, una primera lectura en clave laboral", Revista General de Derecho del Trabajo y de la Seguridad Social, 2024, núm. 67.

materia de inteligencia artificial debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución. Además, la puesta en práctica general de medidas de alfabetización en materia de inteligencia artificial y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo y, en última instancia, sostener la consolidación y la senda de innovación de una IA fiable en la Unión".

Definido su ámbito de aplicación, el RIA, como precisa su Considerando 9, conforma un conjunto de normas armonizadas que "*deben aplicarse en todos los sectores y, en consonancia con el nuevo marco legislativo, deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, (...), derechos fundamentales, empleo, protección de los trabajadores (...)*". Una regla de salvaguardia con expresa proyección en lo laboral que queda materializada en su art. 2.11: "*El presente Reglamento no impedirá que los Estados miembros o la Unión mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores o fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores*". Y es que, como viene a aclarar de nuevo el Considerando 9, esta norma "*tampoco debe afectar en modo alguno al ejercicio de los derechos fundamentales reconocidos en los Estados miembros y a escala de la Unión, incluidos el derecho o la libertad de huelga o de emprender otras acciones contempladas en los sistemas de relaciones laborales específicos de los Estados miembros y el derecho a negociar, concluir y hacer cumplir convenios colectivos o a llevar a cabo acciones colectivas conforme a la legislación nacional*". De igual modo, se añade, "*el presente Reglamento no debe afectar a las disposiciones destinadas a mejorar las condiciones laborales en el trabajo en plataformas digitales*", en los términos que defina la recientemente aprobada Directiva en esta materia.

Sobre las anteriores bases, el RIA asienta su actuación sobre lo que podríamos calificar su "triángulo de oro": aproximación desde el riesgo, garantías y responsabilidades.

El riesgo está asociado, de manera inescindible, a los cambios que lleva consigo la incorporación de los nuevos sistemas de IA. Así lo pone de manifiesto la RIA que articula su regulación, precisamente, sobre una aproximación desde la idea de "riesgo", definida como "*la combinación de la probabilidad de que se produzca un*

daño y la gravedad de dicho daño". El Reglamento establece una jerarquía de riesgos en función del uso de la IA y sobre las categorías detectadas, establece una serie de obligaciones cuyas proyecciones sobre lo laboral resultan más que evidentes.

En este ámbito quedan directamente proscritos los sistemas de reconocimiento de emociones. El RIA expresamente prohíbe "*la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para inferir las emociones de una persona física en los ámbitos de la aplicación de la ley (...) en lugares de trabajo (...)*" (art. 5.1 f) RIA). Igualmente se encuentra prohibida "*la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual (...)*" (art. 5.1 g) RIA).

Pero la pieza esencial del sistema que construye el RIA se asienta en el establecimiento de límites al uso de los sistemas que califica de "alto riesgo" (art. 6.1 y 2 por relación con lo establecido en el Anexo III del RIA). Una noción que, como precisa el Considerando 46, se diseña tomando en cuenta sus efectos, por cuanto incluye entre tales sistemas aquellos que "*tengan consecuencias perjudiciales importantes para la salud, la seguridad y los derechos fundamentales de las personas de la Unión, y dicha limitación reduce al mínimo cualquier posible restricción del comercio internacional, si la hubiera*". Lo laboral ocupa, también aquí, un papel protagonista. Y es que, como viene a subrayar el Considerando 48, "*la magnitud de las consecuencias adversas de un sistema de IA para los derechos fundamentales protegidos por la Carta es especialmente importante a la hora de clasificar un sistema de IA como de alto riesgo. Entre dichos derechos se incluyen el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, (y) los derechos de los trabajadores (...)*".

La lectura del art. 6.2 en relación con el Anexo III de RIA ratifica de modo concluyente la referida proyección a nuestro campo. Dicho Anexo III incorpora entre los sistemas de IA de alto riesgo los que afecten al "*empleo, gestión de los trabajadores y acceso al autoempleo*" y, en concreto, a) "*Sistemas de IA destinados a ser utilizados para la contratación o la selección de personas físicas, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos*"; y "b) *sistemas de IA destinados a utilizarse para*

tomar decisiones o influir sustancialmente en ellas que afecten a la iniciación, promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas basada en la conducta individual o en rasgos o características personales, o al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones". El Considerando 57 justifica dicha inclusión sobre la base de que los mismos: "*pueden perpetuar patrones históricos de discriminación, por ejemplo, contra las mujeres*[46]*, ciertos grupos de edad, las personas con discapacidad o las personas de orígenes raciales o étnicos concretos o con una orientación sexual determinada, durante todo el proceso de contratación y en la evaluación, promoción o retención de personas en las relaciones contractuales de índole laboral. Los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad*".

El RIA incorpora un importante sistema de garantías que se anudan a los requisitos generales que deberán cumplir los sistemas de IA de alto riesgo "*teniendo en cuenta sus finalidades previstas, así como el estado actual de la técnica generalmente reconocido en materia de IA*" (art. 8). Ello lleva consigo el establecimiento, implantación, documentación y mantenimiento de un sistema de gestión de riesgos entendido como "*un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida de un sistema de IA de alto riesgo, que requerirá revisiones y actualizaciones sistemáticas periódicas*" (art. 9). A ello se une la necesaria "*gobernanza de los datos*" (art. 10), las exigencias de un precisa documentación técnica (art. 11) y la necesidad de garantizar un nivel de trazabilidad del funcionamiento del sistema (art. 12). La transparencia suficiente para que los responsables del despliegue interpreten y usen correctamente la información de salida que incorporen los sistemas de IA, constituye un principio maestro (art. 13) al que se une la necesidad de que su diseño y desarrollo permita cumplir con el principio de humano al mando (art. 14). En fin, unos sistemas que se diseñarán y desarrollarán

---

[46] Como señala M. E. CASAS BAAMONDE, "Trabajo de las mujeres y digitalización", Revista de Derecho Laboral vLex (RDLV), 2021, núm. 4, pp. 67-88, "estando lejos de cerrarse las distintas brechas estructurales de género, parece confirmarse que la digitalización, la robotización y la inteligencia artificial amplían la desigualdad de género por causa de las brechas digitales y la intensificación de las brechas tradicionales existentes, particularmente de la ocupacional y retributiva". Son, por ello, "necesarias políticas de igualdad real, de apoyo económico en las transiciones de empleo, de conciliación corresponsable e igualitaria de la vida laboral y familiar, y de empoderamiento de las mujeres en el trabajo transformado en la era digital".

de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme durante todo su ciclo de vida (art. 15).

Los responsables del despliegue de los sistemas de IA que incorporen estas técnicas se encuentran, además, obligados a cumplir con un ineludible presupuesto (art. 26.7 RIA y Considerando 92): "*Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo. Esta información se facilitará, cuando proceda, con arreglo a las normas y procedimientos establecidos en el Derecho nacional y de la Unión y conforme a las prácticas en materia de información a los trabajadores y sus representantes*". Una exigencia esencial si atendemos a los términos del Considerando 92 que considera que "*este derecho de información es accesorio y necesario para el objetivo de protección de los derechos fundamentales que subyace al presente Reglamento (...)*" y, además, se impone "*incluso aunque no se cumplan las condiciones de las citadas obligaciones de información o de información y consulta previstas en otros instrumentos jurídicos* (la referencia se hace a la Directiva 2002/14/CE)".

El último vértice del triángulo de oro del RIA se cierra con un potente régimen de responsabilidades y sanciones asociadas. Como expresa el Considerando 168 del RIA, "*se debe poder exigir el cumplimiento del presente Reglamento mediante la imposición de sanciones y otras medidas de ejecución*". Sus efectos parecen, a priori, demoledores. A título de ejemplo, el art. 99.3 RIA establece que: "*El no respeto de la prohibición de las prácticas de IA a que se refiere el artículo 5 estará sujeto a multas administrativas de hasta 35.000.000 euros o, si el infractor es una empresa, de hasta el 7% de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior*". Por su parte, el art. 99.4 establece que: "*El incumplimiento por parte de un sistema de IA de cualquiera de las disposiciones que figuran a continuación en relación con los operadores o los organismos notificados, distintas de los mencionados en el artículo 5, estará sujeto a multas administrativas de hasta 15.000.000 euros o, si el infractor es una empresa, de hasta el 3% de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior*", resultando a nuestros efectos relevante el apartado e) que proyecta los anteriores efectos sobre "*las obligaciones de los responsables del despliegue con arreglo al artículo 26*".

8. EL IMPACTO EN EL MERCADO DE TRABAJO: ¿HACIA UNA CUOTA DE RESERVA PARA EL TRABAJO HUMANO?

Y, para concluir, una breve reflexión sobre el futuro de un trabajo que camina entre los algoritmos y la IA. En el momento actual, las características de la sociedad postindustrial con la intensificación de los procesos de automatización, incorporación de nuevas tecnologías, etc., ejercen en sí mismas –como factor de base objetiva de aumento del desempleo– una fuerza de expulsión de mano de obra y una reducción de la fuerza de trabajo necesaria en la producción. A medida que la economía lentamente se reactiva, este componente de desempleo tecnológico puede pesar en unos mercados de trabajo debilitados: muchos puestos de trabajo que se destruyeron ya no volverán jamás, serán sustituidos por máquinas más eficientes. La mayor parte del trabajo táctico, algorítmico y estructurado será automatizado por las máquinas a lo largo del tiempo[47].

Desde hace tiempo en numerosos trabajos vengo hablando de una idea que me parece importante: la empresa tecnológicamente responsable (o, si se prefiere, algorítmicamente responsable). Creo que el gran objetivo de poner diques de contención al irrefrenable cambio tecnológico pasa por la plena concienciación de todos los agentes sociales, económicos y políticos sobre los devastadores efectos del "tsunami tecnológico" que se atisba en el horizonte. Podemos hablar también de una "transición justa" como lo hace la OIT, pero, en todo caso, el reto consiste en que la transición entre empleos que se crean y se destruyan en este proceso sea los más eficiente y equitativa posible, el objetivo es proteger a las personas y no los puestos de trabajo. En todo caso lo que es evidente es que "la IA posee tanto riesgos como oportunidades en términos de creación y mantenimiento de un modelo de trabajo decente"[48].

---

[47] Extensamente, Mercader Uguina, J. R. "Reflexiones sobre la simultánea creación, destrucción y transformación del empleo en la era digital", en Molina Navarrete, C. (dir.) (2022). *De la economía digital a la sociedad del E-work decente: condiciones sociolaborales para una industria 4.0 justa e inclusiva*, Pamplona, Aranzadi/Thomson Reuters, pp. 93-115.

[48] Deshpande, A. et al. (2021). *Improving working conditions using Artificial Intelligence, Publication for the Special Committee on Artificial Intelligence in a Digital Age*, Policy Department for Economic, Scientific and Quality of Life Policies, Parlamento Europeo, Luxembourg, p. 16. Disponible en: http://www.europarl.europa.eu/supporting-analyses

BIBLIOGRAFÍA

AEPD (2020). *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*, Madrid.

Alba Rico, S. (2017). *Ser o no ser (un cuerpo)*, Barcelona, Seix Barral.

Baz Rodríguez, J. (2019). *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid, Bosch.

Bernhardt, A., Kresge, L. y Suleiman, R. (2021). *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Labor Center.

Byung-Cul Han (2021). *No cosas. Quiebras del mundo de hoy*, Barcelona, Taurus.

Casas Baamonde, M. E. (2020). "El Derecho del Trabajo, la digitalización del trabajo y el trabajo a distancia", *Derecho de las relaciones laborales*, núm. 11, pp. 1413-1437.

Casas Baamonde, M. E. (2021). "Trabajo de las mujeres y digitalización", Revista de Derecho Laboral vLex (RDLV), núm. 4, pp. 67-88.

Cruz Villalón, J. *Algoritmo, digitalización y sanciones laborales "automatizadas"*. http://jesuscruzvillalon.blogspot.com/2021/03/algoritmo-digitaliacion-y-sanciones.html

Dastin, J. *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*. https://perma.cc/T6NZ-T4ZW

Deshpande, A. et al. (2021). *Improving working conditions using Artificial Intelligence, Publication for the Special Committee on Artificial Intelligence in a Digital Age*, Policy Department for Economic, Scientific and Quality of Life Policies, Parlamento Europeo, Luxembourg. Disponible en http://www.europarl.europa.eu/supporting-analyses

Fernández Ramírez, M. (2021). *El derecho del trabajador a la autodeterminación informativa en el marco de la actual empresa "neopanóptica"*, Pamplona, Aranzadi.

Fernández Sánchez, S. (2020). *Relaciones laborales y derechos fundamentales en la era digital. Una visión desde el derecho italiano*, Temas Laborales, núm. 155, pp. 177-189.

Giddens, A. (1997). *Política y sociología en Max Weber*, Madrid, Alianza Editorial.

Ginés I Fabrellas, A. (2021). *El trabajo en plataformas digitales. Nuevas formas de precariedad laboral*, Pamplona, Aranzadi.

Goerlich Peset, J. M. (2021). *Decisiones administrativas automatizadas en materia social: algoritmos en la gestión de la Seguridad Social y en el procedimiento sancionador*, Labos, Vol. 2, núm. 2, pp. 22-42.

González García, J. M. (1989). *La máquina burocrática (Afinidades electivas entre Max Weber y Kafka)*, Madrid, Visor.

Huergo, A. (2021). "Administraciones Públicas e inteligencia artificial: ¿más o menos discrecionalidad?", *El Cronista del Estado Social y Democrático de Derecho*, núms. 96-97, pp. 78-95.

Huergo, A. (2021). "Una aproximación a los algoritmos desde el Derecho Administrativo", AA. VV., *La regulación de los algoritmos*, Pamplona, Aranzadi, pp. 23-87.

Kim, P. T. y Bodie, M. T. (2021). *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, Journal of Labor and Employment Law, Vol. 35, núm. 2, pp. 294-296.

Klecher, C. 'How Amazon automatically tracks and fires warehouse workers for 'productivity'. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivityfiring-terminations

Kyung Lee, M., Kusbit, D., Metsky, E. y Dabbish, L. *Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers*. http://www.cs.cmu.edu

Mayer-Schónberger, V. y Cukier, K. (2013). *Big data. La revolución de los datos masivos*, Turner, Madrid.

Mercader Uguina, J. R. (2001) "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones Laborales*, núm. 10, pp. 11-31.

Mercader Uguina, J. R. (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Valencia, Tirant lo Blanch.

Mercader Uguina, J. R. (2022). "Reflexiones sobre la simultánea creación, destrucción y transformación del empleo en la era digital", en C. Molina Navarrete (dir.), *De la economía digital a la sociedad del E-work decente: condiciones sociolaborales para una industria 4.0 justa e inclusiva*, Pamplona, Aranzadi/ Thomson Reuters, pp. 93-115.

Mercader Uguina, J. R. (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Valencia, Tirant lo Blanch.

Mercader Uguina J. R. (2022). "En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo", *El Cronista del Estado Social y Democrático de Derecho*, núm. 100 (ejemplar dedicado a: Inteligencia artificial y derecho), pp. 136-145.

Mercader Uguina, J. R. "El Reglamento de Inteligencia Artificial: frecuentemos el futuro", Brief AEDTSS 42/2024.

Mercader Uguina, J. R. (2024). "El Reglamento de Inteligencia Artificial entra en la recta final, una primera lectura en clave laboral, Revista General de Derecho del Trabajo y de la Seguridad Social, núm. 67.

Mercader Uguina, J. R. (2024). "*Los usos de alto riesgo en el ámbito laboral de la IA y la autocertificación*", Foro de Labos, 9 de mayo de 2024.

Mercader Uguina, J. R. (2024). "*El "big bang" de la biometría laboral. De la huella dactilar a los neurodatos*", Labos, Vol. 5, núm. 2, pp. 4-23.

Molina Navarrete, C. (2019). *El ciberacoso en el trabajo. Cómo identificarlo, prevenirlo y erradicarlo de las empresas*, Madrid, Wolters Kluwer.

Muñoz Pérez, A. F. (2020). *La "inteligencia artificial (IA) autónoma" en el órgano de administración*, Revista de Derecho de Sociedades, núm. 60. BIB 2020\36730.

Muñoz Ruiz, A. (2019). *¿Se deben regular los algoritmos? Un breve análisis a la propuesta normativa alemana: la pirámide de criticidad basada en el riesgo*, Foro de Labos, 11 de diciembre de 2019.

Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídico-Laborales*, Valencia, Tirant lo Blanch.

Nathan, N. R., Once, D. S. y Klieger, D. M. *In Hiring, Algorithms Beat Instinct* https://hbr.org/2014/05/in-hiring-algorithms-beat-instinct

Oliva León, R. *¿Es discriminatorio el algoritmo de Deliveroo que «rankea» a sus riders?* https://www.algoritmolegal.com/tecnologias-disruptivas/es-discriminatorio-el-algoritmo-de-deliveroo-que-rankea-a-sus-riders/.

Pasquale, F. A. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. http://www.jstor.org/stable/j.ctt13x0hch .

Peña, D. (2022). *Observación y cálculo en estadística con datos masivos*, Madrid, Real Academia de Ciencias Exactas, Físicas y Naturales de España.

Pérez del Prado, D. (2021). *El debate europeo sobre el trabajo de plataformas. Propuestas para una Directiva, Trabajo y Derecho*, núm. 77.

Pérez del Prado, D. (2023). *Derecho, Economía y digitalización*, Valencia, Tirant lo Blanch.

Pérez Hernández, A. (2019). *Algoritmos y derecho de la competencia: un estudio sobre la alineación automática de precios*, Revista de Derecho Mercantil, núm. 311.

Puebla Pinilla, A., de la (2021). *El despido por causas empresariales*, XXXI Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social. Reestructuraciones empresariales, Madrid, MTES.

Ramos Quintana, M. I. y Mercader Uguina, J. R. (2024). *Los neuroderechos laborales: la neurotecnología llega al lugar de trabajo*, Trabajo y Derecho, núm. 117 (septiembre 2024).

Rey Guanter, S., del (2021). "Inteligencia Artificial y relaciones laborales: algunas implicaciones jurídicas" en AA. VV., *Los desafíos del Derecho del Trabajo ante el cambio económico y social. Libro en Homenaje a Federico Durán*, Madrid, Iustel.

Srnicek, N. (2017). *Platform capitalism*, Cambridge, Polity Press.

Todolí Signes, A. (2020). *The evaluation of workers by customers as a method of control and monitoring in firms: Digital reputation and the European Union's regulation on data protection*, International Labour Review.

Weber, M. (1984). *Economía y Derecho (Sociología del Derecho), en Economía y Sociedad*, México, FCE.

Zuboff, S. (2020). *La era del capitalismo de la vigilancia*, Barcelona, Paidós.

Capítulo 9
BIG DATA Y ALGORITMOS: SU IMPACTO EN EL DERECHO DE LA PROPIEDAD INTELECTUAL, INDUSTRIAL Y COMPETENCIA

Jaume Martí Miravalls
Profesor Titular (acreditado a Catedrático) de Derecho Mercantil
Universidad de Valencia
https://orcid.org/0000-0002-2377-627X

1. INTRODUCCIÓN

En la era de la economía digital[1] puede parecer desfasado recordar la célebre frase del matemático británico Humby formulada en 2006: "los datos son el nuevo petróleo". Pero no es así, porque mientras que la frase obtuvo reconocimiento mundial, su contextualización ha pasado algo más desapercibida e incide directamente en el objeto de nuestro estudio. Tras está impactante afirmación, se añadía que: "(los datos) son valiosos, pero si no se refinan realmente no se pueden utilizar. Tienen que transformarse en gasóleo, plástico, productos químicos, etc., para crear una entidad valiosa que impulse una actividad rentable"; concluyendo que: "por lo tanto, los datos deben desglosarse y analizarse para que tengan valor".

En este contexto, se comprende que los métodos para recopilar, analizar y procesar el "Big data", fundamentalmente a través de algoritmos, así como el conocimiento adquirido en dicho proceso, han adquirido la condición de activo empresarial "especialmente valioso". En efecto, el tratamiento y estudio de los

[1] También llamada "cuarta revolución industrial" por el profesor Gómez-Segade, J. A. (2020). "La protección de los macrodatos (big data) mediante las normas sobre secretos empresariales", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, García Vidal (dir.), Tirant, p. 119; quién la califica como: "la revolución de los datos y la interconexión".

datos obtenido en la red ofrece a quien los posee una posición relevante en el mercado, puesto que le permite tener un mayor conocimiento de elementos clave de su negocio y, por supuesto, del propio mercado: como, por ejemplo, patrones de consumo y/o necesidades de los clientes, ayudando a generar nuevas ideas o soluciones, así como a predecir los acontecimientos futuros con mayor precisión. Ello, obviamente, incide en su proceso de toma de decisiones, ofreciendo una ventaja competitiva que debe protegerse; y, por extensión, cuando dicho activo está en manos de una empresa con poder de mercado, constituye un elemento a valorar y supervisar en el proceso competitivo[2].

Por ello, en el presente trabajo –de ambicioso título– se pretende ofrecer un conjunto de pinceladas[3] sobre los principales problemas que el "Big data" y/o los algoritmos plantean en el mercado, tanto desde la perspectiva del Derecho de la propiedad intelectual e industrial, como desde la perspectiva del Derecho de la competencia, en su doble vertiente de Defensa de la competencia y Competencia desleal. Así, en la primera parte, analizaremos, dada la importancia que estos activos están adquiriendo, cómo pueden protegerse en atención a las distintas instituciones que ofrece el Derecho de la propiedad intelectual e industrial;

---

[2] Téngase en cuenta que, en la económica actual, los servicios digitales y, particularmente, las plataformas en línea ocupan una posición cada vez más relevante en el mercado mundial, posibilitando que los empresarios lleguen a clientes en todo el mundo, mejorando la transparencia, facilitando el comercio transfronterizo y ofreciendo oportunidades de negocio completamente nuevas a un gran número de empresarios. Esta economía de plataformas, cada vez más consolidada y basada en mercados de "dos lados" o "two-sided-markets" (así, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: "Las plataformas en línea y el mercado único digital. Retos y oportunidades para Europa", 2016, COM/2016/0288), se caracterizan por una fuerte presencia de efectos de red, tanto directos (el valor del bien aumenta a medida que aumenta el número de usuarios del mismo lado de la plataforma) como, sobre todo, indirectos (el valor aumenta cuando aumentan los usuarios del otro lado de la plataforma). En consecuencia, las plataformas –esto es, muy pocos operadores– tienen la capacidad de conectar a muchos usuarios profesionales con muchos usuarios finales a través de sus servicios, lo que, a su vez, les permite trasladar sus ventajas, como su acceso a grandes cantidades de datos, de un ámbito de actividad a otro. Y ello, sin duda, afecta al proceso competitivo, pudiendo llegar a alterar el correcto funcionamiento del mercado.

[3] Obviamente, en un trabajo de esta naturaleza no es posible profundizar en todos y cada uno de los problemas que esta poliédrica materia presenta, por ello se va a proceder a realizar una recopilación de los principales asuntos que se plantean en las diferentes ramas del ordenamiento jurídico que se analizan. Para un análisis más detenido de cada una de las cuestiones que se plantean, la obra de referencia en nuestro país es AA. VV., *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, García Vidal (dir.), Tirant, 2020.

y, en la segunda parte, analizaremos algunas de las cuestiones relacionadas con su explotación, particularmente los problemas concurrenciales que ya se han planteado desde la óptica de los acuerdos colusorios y el abuso de posición de dominio; así como desde la óptica de la competencia desleal.

2. CUESTIONES CONCEPTUALES Y TERMINOLÓGICAS

Con carácter previo a entrar en cada una de las cuestiones que son objeto de estudio en este trabajo conviene realizar unas breves referencias conceptuales y terminológicas respecto a qué se entiende por "Big data" y por algoritmo, como conceptos básicos de lo que se ha venido a denominar el "Derecho digital"[4].

En primer lugar, el término "dato" según la RAE hace referencia, en su primera acepción, a "información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho"; y, en su tercera acepción, a "información dispuesta de manera adecuada para su tratamiento por una computadora"; aunque en el ámbito normativo –europeo– el término "dato" es definido como "toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual", diferenciándose entre "datos personales" (que son los datos que se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679[5]) y "datos no personales" (que son el resto de datos que no sean datos personales). Así se definen en los artículos segundo del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos); y del Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas

---

[4] Ver, Valpuesta Gastaminza, E. (2023). "El Derecho digital como categoría transversal en el ordenamiento jurídico y su relación con el Derecho Mercantil", *De Iure Mercatus. Libro Homenaje al Prof. Dr. Dr.h.c. Alberto Bercovitz Rodríguez-Cano*, Tirant lo Blanch, pp. 203 y ss.

[5] Esto es: "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

(UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). Ahora bien, como apunta la doctrina[6], lo verdaderamente importante en la cuarta revolución industrial no son los datos individuales, que siempre tuvieron interés y fueron recogidos frecuentemente en ficheros manuales, sino los "datos masivos" o "macrodatos", popularizados bajo la denominación de "Big data". Y aunque este término no cuenta con carta de naturaleza jurídica, sí ha sido definido en la Comunicación de la Comisión «Hacia una economía de los datos próspera» –COM (2014) 442 final, de 2 de julio de 2014– como: "una gran cantidad de diferentes tipos de datos producidos a alta velocidad a partir de un gran número de diversos tipos de fuentes" –es lo que se conoce como las tres "V": volumen, variedad y veracidad"; a las que últimamente se han añadido dos más: valor y visibilidad–.

Ahora bien, para tratar[7] y manejar en tiempo real el "Big data", es decir, el conjunto de datos muy variables y de naturaleza heterogénea, se necesitan nuevas herramientas y métodos, como software, algoritmos y procesadores de gran potencia. En este sentido, se ha afirmado con precisión que "el extraordinario volumen de datos manejados, así como los sofisticados programas y algoritmos que se utilizan para su análisis, permite que los datos sean examinados no solo con fines descriptivos o de constatación de lo que ha sucedido, sino también con finalidad predictiva, lo que da lugar a un conocimiento difícilmente obtenible por otras vías. Se abandona el estudio tradicional de los datos, basado en la formulación de una hipótesis del tipo causa-efecto que después se verifica, para pasar a obtener un conocimiento de las relaciones de los hechos y datos, sin conocer en muchas ocasiones la relación causa-efecto, dado el extraordinario número de variables existentes. Se trata, pues, de encontrar en los datos masivos patrones repetitivos que puedan ser empleados posteriormente para crear

---

[6] Gómez-Segade, J.A. *La protección de los macrodatos...*, op. cit., pp. 122 y 123.

[7] Respecto al término "tratamiento" se ha generalizado la definición recogida también en artículo 4, punto 1, del Reglamento (UE) 2016/679, y que se refiere a "cualquier operación o conjunto de operaciones" realizadas sobre datos o conjuntos de datos, "ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

modelos predictivos y para la toma de decisiones de todo tipo, o para un mejor conocimiento de relaciones que permanecían ocultas en un análisis tradicional"[8].

Aquí es donde entra en juego el otro gran término: algoritmos. Y, como puede observarse, su relación es muy estrecha. Utilizando el símil culinario: los datos son la materia prima y, por tanto, cuanto mejor sea su calidad, mejor será el resultado; mientras que el algoritmo primero fue la receta y, actualmente, con el "Machine Learning" y aparición de la "inteligencia artificial", ya puede considerarse directamente el cocinero. Y ello porque ahora el algoritmo puede ser quién decide cómo tratar la materia prima y exprimir todo su potencial en un producto final. En efecto, el "Machine Learning" es una disciplina del campo de la Inteligencia Artificial que, a través de algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo). Este aprendizaje permite a los ordenadores realizar tareas específicas de forma autónoma, es decir, sin necesidad de ser programados. En este sentido, un sistema de inteligencia artificial no es más que es un software que se desarrolla empleando una o varias de técnicas y/o estrategias[9] y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

Pues bien, a día de hoy seguimos sin un concepto legal de algoritmo. Varios textos legales hacen referencia al algoritmo, pero ninguno de ellos los ha definido. En ausencia de definición legal, utilizaremos el concepto y clasificación realiza por la OCDE en 2023, en su documento "Algorithmic Competition" –en adelante, informe de la OCDE 2023[10]–. Simplificando mucho, es común considerar que un algoritmo es, sencillamente, una secuencia finita de pasos que

---

[8] García Vidal, A. (2020). "Big data e internet de las cosas: su impacto en el Derecho de la competencia y de la Propiedad industrial e intelectual", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch, p. 26.

[9] Por ejemplo: a) estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo; b) estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico); y c) estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización.

[10] Elaborado por Antonio Capobianco y Daniel Westrik, ambos de la División de Competencia de la OCDE.

deben ser seguidos para cumplir una tarea y que normalmente están representados a través de diagramas de flujo. Se trata de una secuencia que permite transitar desde un estado inicial (input) a un estado final (output). De hecho, según el Diccionario de la RAE, algoritmo se define, en su primera acepción, como "Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema"; y, en su segunda, como "Método y notación en las distintas formas del cálculo". Pues bien, para que este algoritmo sea procesado y ejecutado por un ordenador –"hardware"–, debe ser convertido a un "lenguaje de máquina", también llamado "código objeto". Y este último es una representación binaria del programa computacional, consistente en patrones de 1s y 0s (bits), que a su vez son procesados por el computador como señales electrónicas que hacen operar sus circuitos y switchs.

Con independencia de su definición, lo cierto es que en una economía digital los algoritmos son un instrumento esencial para el progreso tecnológico y, por ende, para el desarrollo industrial[11]. Es una realidad que actualmente se utilizan cada vez más algoritmos para diversos fines, ya sea para crear nuevos productos, mejorar los existentes o parametrizar su funcionamiento. En este sentido, los algoritmos son la fuente de todo mercado online y, sin duda, están revolucionando sectores que se resistían a entrar en el mercado online. Si el algoritmo puede utilizarse en cualquier sector y para prácticamente cualquier actuación, su clasificación es –por esencia– heterogénea. Así, el informe de la OCDE 2023 clasifica los algoritmos de la siguiente manera: En primer lugar, los algoritmos se pueden clasificar en atención a su función: a) búsqueda (p. ej., Google Search); b) recomendación (p. ej., playlists automáticas de Spotify); c) alocación de demanda con oferta (p. ej., Uber); d) monitoreo de conductas (p. ej., Webwatcher); y e) de fijación de precios (p. ej., Rainmaker Group); y, en segundo lugar, otra manera de clasificar algoritmos, más centrada en la tecnología que en la función, es la que distingue entre algoritmos basados en inteligencia artificial, "machine learning" y "deep learning"[12].

---

[11] Botana Agra, J. M. (2020). "Protección jurídica de algoritmos y programas de ordenador", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch, p. 157.

[12] El "deep learning" es un tipo de "machine learning" que entrena a un ordenador para que realice tareas como las hacemos los seres humanos, como el reconocimiento del habla, la

En definitiva, como resume perfectamente el profesor Gómez-Segade[13]: "hay que tener en cuenta que, al hablar de datos y de economía datificada, deben distinguirse tres categorías fundamentales de datos: los datos individuales, las series de datos (estructurados o desestructurados) y los metadatos. Sólo estas dos últimas categorías son las que podemos calificar como macrodatos. Por lo demás, conviene tener presente que el proceso de obtención de macrodatos se descompone en tres fases que se desarrollan sucesivamente. En primer lugar, una fase de obtención de los datos, generados automáticamente por máquinas o procedentes de personas, o bien recogidos de fuentes libremente accesibles. Esta recolección de datos puede ser voluntaria, por ejemplo, porque se proporcione la información como contrapartida por el uso de una aplicación o un servicio en el caso de tiendas en línea o plataformas sociales; pero también puede ser automática por el uso de sensores conectados del IoT o por el empleo de cookies, técnicas de rastreo, o cualquier otro método de captura de datos mediante motores de búsqueda o máquinas. El dato aislado y singular adquiere contenido informativo cuando se contextualiza mediante metadatos; estos metadatos ordenan los datos aislados y hacen surgir series de datos que pueden ser filtradas por un algoritmo generado automáticamente, que da lugar a múltiples datos que se denominan series de datos desestructurados. En la segunda fase, cada serie de datos es objeto de tratamiento por un algoritmo de aprendizaje automático y se transforma en una serie de datos estructurada, de la que surgen nuevamente metadatos. Estos metadatos ya no describen las notas características de cada dato individual, sino la relación en que se encuentran entre sí las distintas series de datos; y de esta serie de datos estructurados, de nuevo con la ayuda de algoritmos de aprendizaje automático pueden deducirse nuevos conocimientos que ni se podían imaginar a la vista de los datos singulares. Finalmente, en la tercera fase, los conocimientos adquiridos en la segunda fase permiten concretar nuevas series de datos estructuradas (por ejemplo, los hábitos alimenticios de un sector de los consumidores) de las que pueden deducirse informaciones que pueden ser decisivas para la adopción de una medida empresarial".

---

identificación de imágenes o hacer predicciones. Obsérvese, por tanto, que el "deep learning" es una subcategoría de "machine learning" que, a su vez, es una subcategoría de inteligencia artificial.

[13] Gómez-Segade, J. A. *La protección de los macrodatos*..., op. cit., pp. 135-136.

3. EL BIG DATA Y LOS ALGORITMOS COMO OBJETO DE PROTECCIÓN EN EL DERECHO DE LA PROPIEDAD INTELECTUAL E INDUSTRIAL

Como es sabido, el sistema clásico de clasificación de las creaciones, que se corresponde con la segunda mitad del siglo XIX, establece un esquema normativo dual: por un lado, la propiedad industrial, más vinculado con creaciones industriales o empresariales utilitarias, como son las patentes, el diseño, las marcas, etcétera; y, por otro, la propiedad intelectual, vinculada a los derechos de autor para la protección de las creaciones con una utilidad más intelectual o estética, sin perjuicio de ciertos aspectos o destinos prácticos[14]. Si bien, esta dualidad, con el tiempo, se ha ido suavizando, dando lugar a la doctrina de los bienes inmateriales[15]. En este apartado analizaremos de manera gradual los principales problemas que el "Big data" y los algoritmos presentan a los efectos de su calificación como bien objeto de protección jurídica. Y ello es relevante porque, de todo cuanto se ha dicho hasta el momento, se comprende el valor empresarial que tanto el "Big data" como los algoritmos están llamados a tener en una economía digital.

En relación con el "Big data" lo primero que analizar es si es posible su protección "en bruto"[16], en la medida en que los datos, tanto si son recopilados por humanos o por máquinas, son la materia prima desde la que se parte y ello en sí mismo puede tener valor empresarial. Téngase en cuenta que en el "Big data" la recopilación de los datos no se hace con una única finalidad porque en realidad es posible recopilar los datos sin saber muy bien la información que se quiere extraer de ellos. Y ello porque, aunque algunos datos puedan ser inicialmente irrelevantes, con la aplicación de algoritmos y su interconexión con otros datos estos datos irrelevantes pueden convertirse en sustanciales[17].

---

[14] Buena prueba de lo que se dice es el tratamiento internacional inicial en sendos Convenios separados, el Convenio de París de 1883 para la propiedad industrial y el Convenio de Berna de 1886 para el derecho de autor (obras artísticas y literarias).

[15] Véase, por todos, Gómez-Segade, J. A. (2015). "Los bienes inmateriales en el Anteproyecto de Ley del Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, Universidad Carlos III de Madrid, pp. 115-135.

[16] García Vidal, A. *Big data e internet de las cosas*..., op. cit., p. 29.

[17] Así, García Vidal, A. *Big data e internet de las cosas*..., op. cit., p. 28.

Pues bien, actualmente no existe un derecho específico o "sui generis" sobre macrodatos como objeto de protección, pese a que ya se ha propuesto su creación[18]. Por ello, en este momento la protección de los macrodatos debe llevarse a cabo utilizando algunos de los instrumentos legales existentes en el ordenamiento jurídico. Así, en primer lugar, analizaremos la protección jurídica que ofrece el derecho "sui generis" sobre las bases de datos.

La protección jurídica de las bases de datos no es algo nuevo para el Derecho de la propiedad intelectual[19]. Ya en el ámbito internacional el artículo 10.2 del Acuerdo sobre los ADPIC (Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio) establecía que: "Las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, serán protegidas como tales. Esa protección, que no abarcará los datos o materiales en sí mismos, se entenderá sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos" –precepto que se reproduce en el artículo 5 del Tratado de la OMPI sobre Derecho de Autor–.

En Europa, por su parte, la protección de las bases de datos se proclama en la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, definidas en su artículo 1.2 como: "las recopilaciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma"; y en cuyo artículo 3.1 proclama que: "...las bases de datos que por la selección o la disposición de su contenido constituyan

---

[18] Sobre el debate acerca de la creación de un Derecho para los macrodatos, Gómez-Segade, J.A., *La protección de los macrodatos*..., op. cit., pp. 127-128, donde se indica que: "aunque parezca sorprendente a primera vista, también la industria se mostró contraria a la creación de un nuevo derecho de propiedad industrial sobre los datos por diversas razones. En primer lugar, muchas empresas trabajan con macrodatos y no están seguras de si ese nuevo derecho producirá más beneficios que perjuicios; y, en segundo término, no existe acuerdo sobre quién sería el titular de esos datos, teniendo en cuenta la complejidad del tema, pues los interesados pueden ser muchos y variados".

[19] En la doctrina, sobre las bases de datos, por todos, Minero Alejandre, G. (2014). *La protección jurídica de las bases de datos en el ordenamiento europeo*, Tecnos; en especial relación con los macrodatos; García Vidal, A. (2020). "La protección de los macrodatos: exclusividad versus libre acceso", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch, pp. 38-58.

una creación intelectual de su autor estarán protegidas, como tal creación, por los derechos de autor". Esta normativa, a efectos internos, se traduce en los artículos 12, 34, 40 ter, 133 a 137 y 203 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia –LPI–, que a efectos conceptuales declara en el artículo 12.2 que: "...se consideran bases de datos las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma".

Pues bien, en atención a este régimen jurídico, la recopilación de macrodatos puede, en principio, si cumple los requisitos para calificarse como base de datos, obtener la protección que ofrece la normativa como derecho de autor, si consigue la calificación jurídica de obra[20]; y/o, principalmente, a través del derecho "sui generis" sobre las bases de datos de los artículos 133 a 137 LPI. Y, en este segundo caso, el artículo 133.1 LPI, declara nítidamente que: "El derecho «sui generis» sobre una base de datos protege la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido"; y que su contenido permite

---

[20] Aunque, como señala García Vidal, A., *La protección de los macrodatos*..., op. cit., pp. 45-46: "En las bases de datos electrónicas no es frecuente que se realice una selección creativa, siendo más factible que la creatividad se manifieste en el criterio de presentación de los datos a los usuarios de la base. No obstante, la recopilación de macrodatos es muy improbable que alcance el grado requerido de originalidad y creatividad en el criterio de selección o clasificación. Ello es debido a que la recopilación de los datos masivos no suele sujetarse a criterios de clasificación en el momento de recoger los datos y, si lo hace, estos no suelen ser especialmente elaborados. Y, del mismo modo, tampoco es frecuente que los distintos datos sean presentados de un modo original, fundamentalmente porque el usuario de la base de datos compuesta por macrodatos no tiene interés en acceder a los datos aislados, porque estos solo son útiles para aplicar sobre ellos el correspondiente algoritmo y para ello no es preciso que estén presentados u organizados conforme a criterios de creatividad y originalidad. En todo caso, en el muy improbable supuesto de que la base con los macrodatos cumpliese el requisito de originalidad exigido, el autor de una base de datos tendrá el derecho exclusivo de realizar determinados actos enumerados en el artículo 5 de la directiva y en el artículo 133 de la LPI, respecto de la forma de expresión de dicha base susceptible de la protección de los derechos de autor, esto es, la estructura resultante de la selección o disposición de sus contenidos. Es decir, la exclusiva no se extiende al contenido de la base (artículos 1.2 de la directiva y 12.1 de la LPI), por lo que no se extendería en modo alguno a los datos incluidos en el conjunto de macrodatos, sino solo a los criterios de clasificación o presentación de dichos datos".

al fabricante de una base de datos "prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de esta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo"; derecho que nace –artículo 16 LPI– "en el mismo momento en que se dé por finalizado el proceso de fabricación de la base de datos, y expirará quince años después del 1 de enero del año siguiente a la fecha en que haya terminado dicho proceso".

En sede del derecho "sui generis" sobre bases de datos interesa destacar dos sentencias del TJUE. La primera de ellas, de 15 de enero de 2025, asunto C-30/14, caso "Ryanair", en la que se declaró que: "La Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, debe interpretarse en el sentido de que no es aplicable a una base de datos que no está protegida por los derechos de autor ni por el derecho sui generis en virtud de la propia Directiva, por lo que los artículos 6, apartado 1, 8 y 15 de esta no se oponen a que el creador de dicha base de datos establezca limitaciones contractuales a su utilización por terceros, sin perjuicio del Derecho nacional aplicable"; y la segunda de ellas, de 3 de junio de 2021, asunto C-762/19, caso "CV-Online Latvia", en la que primero se recuerda que es doctrina del TJUE que la finalidad del derecho previsto en el artículo 7 de la Directiva 96/9 es garantizar a la persona que tomó la iniciativa y asumió el riesgo de realizar una inversión sustancial –en términos de medios humanos, técnicos o financieros– en la constitución y el funcionamiento de una base de datos que obtenga la remuneración de su inversión, protegiéndola frente a la apropiación no autorizada de los resultados obtenidos gracias a dicha inversión; de modo que el objetivo perseguido por el legislador de la Unión mediante el establecimiento de un derecho sui generis es, por tanto, fomentar la implantación de sistemas de almacenamiento y tratamiento de datos que contribuyan al desarrollo del mercado de la información en un contexto marcado por un aumento exponencial de la cantidad de información generada y procesada anualmente en todos los sectores de actividad (Sentencia de 19 de diciembre de 2013, Innoweb, C-202/12, EU:C:2013:850); y, en después se concluye, en el caso concreto, que: "el artículo 7, apartados 1 y 2, de la Directiva 96/9/CE... debe interpretarse en el sentido de que un motor de búsqueda en Internet especializado en la búsqueda del contenido de las bases de datos, que copia o indexa la totalidad o una parte sustancial de una base de datos accesible libremente en Internet y a continuación permite

a sus usuarios efectuar búsquedas en esa base de datos en su propio sitio de Internet según criterios pertinentes desde el punto de vista de su contenido, realiza una «extracción» y una «reutilización» de dicho contenido, en el sentido de esta disposición, que el fabricante de dicha base de datos puede prohibir en la medida en que tales actos ocasionen un perjuicio a su inversión en la obtención, verificación o presentación de dicho contenido, es decir, siempre que constituyan un riesgo para las posibilidades de amortización de esa inversión mediante la explotación normal de la base de datos en cuestión, extremo este que corresponde comprobar al órgano jurisdiccional remitente".

Ahora bien, téngase en cuenta que, como se ha dicho, el nacimiento de la protección "sui generis" sobre las bases de datos se produce "en el mismo momento en que se dé por finalizado el proceso de fabricación de la base de datos", lo cual, obviamente, casa mal con el "Big data", donde el flujo de incorporación de datos es constante –recuérdese la que una de las tres "v" es la de velocidad con la que se generan los datos–. Y, como ha señalado la doctrina, aunque el Tribunal de Justicia (Sentencia de 5 de marzo de 2009, Apis-Hristovich EOOD) ha reconocido que es posible que un conjunto global de datos esté formado por subgrupos separados que pueden constituir, por sí mismos, una base de datos que responde a los requisitos de concesión de la protección por medio del derecho sui generis, lo cierto es que: "la existencia de subgrupos en los macrodatos, que sean a su vez bases de datos en sí mismas, no solventa automáticamente el problema, si esos subgrupos son objeto de actualización constante"[21].

En este sentido, cabe concluir que la protección jurídica que otorga al "Big data" la normativa sobre propiedad intelectual, principalmente por la vía de la protección jurídica de las bases de datos, presenta más complicaciones que soluciones. Y ello explica el recurso a otras vías de protección, como el secreto empresarial, en la medida en que en esta sede no es necesario acreditar requisito alguno de originalidad en la compilación ni acreditación de inversión sustancial[22]. Lo que nos sitúa directamente en el ámbito de la propiedad industrial.

En este punto conviene precisar que la tutela sobre el secreto empresarial se recoge en la Ley 1/2019, de 20 de febrero, de Secretos Empresariales –LSE–,

---

[21] García Vidal, A. *La protección de los macrodatos*..., op. cit., p. 54.
[22] García Vidal, A. *La protección de los macrodatos*..., op. cit., p. 59.

que transpone la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas; y, residualmente, en el artículo 13 de la Ley 3/1991, de 10 de enero, de Competencia Desleal –LCD– que declara que: "se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales".

Pues bien, el artículo 1.1 LSE proclama que se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto; y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto. En este sentido, como ahora veremos, los macrodatos pueden encajar en el concepto jurídico de secreto empresarial[23].

No hay duda de que los macrodatos son "información" en el sentido de la LSE, por lo que debe analizarse si cumple el resto de requisito, esto es, el ontológico (carácter secreto), el objetivo (valor comercial) y el subjetivo (medidas de protección). Desde una perspectiva ontológica, los macrodatos pueden tener la condición de secreto, incluso aunque estén configurados por un datos públicos o accesibles por terceros, en la medida en que el carácter secreto no debe predicarse respecto de los datos en concreto, sino respecto de su conjunto o configuración. Además, como apunta la mejor doctrina[24]: "la LSC no establece umbrales cuantitativos o cualitativos para determinar el carácter secreto de un macrodato, y por lo tanto es irrelevante el grado de estructuración o contextualización de la serie de datos, o el número de datos singulares contenidos en cada serie de datos. Por ello, hay que considerar que incluso tienen carácter secreto las masas de datos desestructurados originados en la primera fase de elaboración de los

---

[23] Así, entre nosotros, Gómez-Segade, J. A., *La protección de los macrodatos*..., op. cit., pp. 134 y 145; y García Vidal, A., *La protección de los macrodatos*..., op. cit., p. 59.

[24] Gómez-Segade, J.A. *La protección de los macrodatos*..., op. cit., p. 139.

macrodatos antes mencionada; es lo que sucedería, por ejemplo, con las series de datos en bruto procedentes de los sensores integrados en el internet de las cosas".

Por su parte, respecto del requisito objetivo, esto es, el valor comercial, tampoco hay duda de que los macrodatos, si se mantienen en secreto, ostentan está cualidad, pues no sólo permite su explotación directa, sino también la indirecta a través de su comercialización a terceros. En este sentido, el conjunto ingente de datos, mantenidos en secreto, incluso de información trivial –que en principio– no ostentaría la condición de secreto empresarial, puede ser objeto de protección precisamente por ese elemento cuantitativo[25]. Recuérdese que en el "Big data" la recopilación de los datos no se hace con una única finalidad, porque en realidad es posible recopilar los datos sin saber muy bien la información que se quiere extraer de ellos, de modo que, aunque algunos datos puedan parecer inicialmente irrelevantes, con la aplicación de algoritmos y su interconexión con otros datos pueden convertirse en relevantes, por ello los macrodatos tienen valor comercial en sí mismos. Y que el valor empresarial a efectos de la LSE puede ser real "o potencial".

Finalmente, en cuanto al requisito subjetivo (la adopción de medidas razonables de protección de los macrodatos, hay que tener en cuenta dos cuestiones: la primera, que no basta con la mera voluntad de mantener secreto, sino que es necesaria la adopción y acreditación de medidas concretas, enjuiciadas desde una perspectiva de estándares de conducta objetivos; y la segunda, que ello conlleva que determinar si se trata de medidas razonables no es una tarea fácil y requiere necesariamente estar al caso concreto[26].

En consecuencia, hay que concluir que, pese a que se ha levantado alguna opinión en contra[27], los macrodatos, incluso en bruto, pueden encajar en el concepto jurídico de secreto empresarial. Si bien, la protección jurídica que ofrece esta normativa no atribuye un "derecho de exclusiva", sino que su régimen se recoge en los artículos 2 y 3 LSE, que regulan los actos lícitos e ilícitos de terceros. En este sentido, se declara –básicamente– que la obtención de la información constitutiva del secreto empresarial se considera lícita cuando se realice

---

[25] En este sentido, García Vidal, A., *La protección de los macrodatos*..., op. cit., p. 63.

[26] Así, Gómez-Segade, J. A., *La protección de los macrodatos*..., op. cit., pp. 141-142.

[27] Drexl, J. (2017). "Designing Competitive Markets for Industrial Data", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 8, núm. 4, pp. 257 y ss.

por alguno de los medios siguientes: a) El descubrimiento o la creación independientes; b) La observación, estudio, desmontaje o ensayo de un producto u objeto que se haya puesto a disposición del público o esté lícitamente en posesión de quien realiza estas actuaciones, sin estar sujeto a ninguna obligación que válidamente le impida obtener de este modo la información constitutiva del secreto empresarial; c) El ejercicio del derecho de los trabajadores y los representantes de los trabajadores a ser informados y consultados, de conformidad con el Derecho europeo o español y las prácticas vigentes; así como, d) Cualquier otra actuación que, según las circunstancias del caso, resulte conforme con las prácticas comerciales leales, incluidas la transferencia o cesión y la licencia contractual del secreto empresarial. En cambio, la obtención de secretos empresariales sin consentimiento de su titular se considera ilícita cuando se lleve a cabo mediante: a) El acceso, apropiación o copia no autorizadas de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes, que contengan el secreto empresarial o a partir de los cuales se pueda deducir; y b) Cualquier otra actuación que, en las circunstancias del caso, se considere contraria a las prácticas comerciales leales. Así, la utilización o revelación de un secreto empresarial se consideran ilícitas cuando, sin el consentimiento de su titular, las realice quien haya obtenido el secreto empresarial de forma ilícita, quien haya incumplido un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto empresarial, o quien haya incumplido una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial. Así como cuando la persona que las realice, en el momento de hacerlo, sepa o, en las circunstancias del caso, debiera haber sabido que obtenía el secreto empresarial directa o indirectamente de quien lo utilizaba o revelaba de forma ilícita según lo dispuesto en el apartado anterior. Y la producción, oferta o comercialización de mercancías infractoras o su importación, exportación o almacenamiento con tales fines también constituyen utilizaciones ilícitas de un secreto empresarial cuando la persona que las realice sepa o, en las circunstancias del caso, debiera haber sabido que el secreto empresarial que incorporan se había utilizado de forma ilícita[28].

Lo singular de este régimen, desde la perspectiva de la tutela, es que, en sede de acciones en defensa del secreto, se establece un régimen mucho más moderno

[28] Ver, Gómez-Segade, J. A. (2019-2020). "La nueva ley de secretos empresariales", *Actas de derecho industrial y derecho de autor*, Tomo 40, pp. 141-164.

y próximo al de los derechos exclusivos de la propiedad industrial que al tradicional de la competencia desleal, no sólo en materia de acción de daños y perjuicios, sino también en prescripción. Así, por ejemplo, el artículo 10.1 LSE, en sede de cálculo de la indemnización, declara que: "Al fijarse la indemnización de daños y perjuicios se tendrán en cuenta todos los factores pertinentes, como son los perjuicios económicos, incluido el lucro cesante, que haya sufrido el titular del secreto empresarial, el enriquecimiento injusto obtenido por el infractor y, cuando proceda, otros elementos que no sean de orden económico, como el perjuicio moral causado al titular del secreto empresarial por su obtención, utilización o revelación ilícitas. También podrán incluirse, en su caso, los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial. Con carácter alternativo, se podrá fijar, según los casos, una cantidad a tanto alzado en concepto de indemnización de daños y perjuicios, atendiendo, al menos y entre otros aspectos, al importe que la parte demandada habría tenido que pagar al titular del secreto empresarial por la concesión de una licencia que le hubiera permitido utilizarlo durante el período en el que su utilización podría haberse prohibido"; y, en materia de prescripción, establece que: "Las acciones de defensa de los secretos empresariales prescriben por el transcurso de tres años desde el momento en que el legitimado tuvo conocimiento de la persona que realizó la violación del secreto empresarial. Su prescripción se interrumpirá por las causas previstas con carácter general en el Código Civil"[29].

Por su parte, los algoritmos presentan una protección jurídica relativamente similar, en cuanto a su régimen idóneo y problemática que genera. Los algoritmos, entendidos como una secuencia finita de pasos que deben ser seguidos para cumplir una tarea, pueden gozar en sede de Propiedad intelectual de la protección del Derecho de autor y, de forma indirecta, cuando se integra en un "programa de ordenador", de la protección que se otorga a esta figura[30].

En efecto, aunque desde la perspectiva de la Propiedad intelectual lo que se protege es la expresión de la obra y no la lógica subyacente, lo que podría plantear algún problema, lo cierto es que, a nuestro juicio, los signos y diagramas que

---

[29] Sobre las acciones en defensa del secreto empresarial, por todos, Girona Domingo, R. (2022), *Las acciones civiles en defensa del secreto empresarial*, Atelier.

[30] En este sentido, Botana Agra, J. M., *Protección jurídica de algoritmos*..., op. cit., p. 157.

describen el algoritmo podrían ser objeto de protección mediante el derecho de autor como obra, en la medida en que cumpla los requisitos de originalidad y expresión. Así, el concepto de "obra", tal como resulta de una reiterada jurisprudencia del Tribunal de Justicia, es una noción autónoma del Derecho de la Unión que debe ser interpretada y aplicada de manera uniforme y que supone la concurrencia de dos elementos acumulativos: por una parte, este concepto implica que existe un objeto original, en el sentido de que el mismo constituye una creación intelectual propia de su autor; por otra parte, la calificación como obra se reserva a los elementos que expresan dicha creación intelectual (véanse, en este sentido, las Sentencias de 16 de julio de 2009, Infopaq International, C-5/08, EU:C:2009:465, apartados 37 y 39, y de 13 de noviembre de 2018, Levola Hengelo, C-310/17, EU:C:2018:899, apartados 33 y 35 a 37, y la jurisprudencia citada). En lo que se refiere al primer elemento, el TJUE tiene consolidado que, para que un objeto pueda considerarse original, resulta al mismo tiempo necesario y suficiente que refleje la personalidad de su autor, manifestando las decisiones libres y creativas del mismo (véanse, en este sentido, las Sentencias de 1 de diciembre de 2011, Painer, C-145/10, EU:C:2011:798, apartados 88, 89 y 94, y de 7 de agosto de 2018, Renckhoff, C-161/17, EU:C:2018:634, apartado 14)[31]; por su parte, respecto al segundo elemento, el TJUE ha declarado que ello implica necesariamente una expresión del objeto de la protección del derecho de autor que la identifique con suficiente precisión y objetividad, aun cuando esta expresión no sea necesariamente permanente (véase, en este sentido, la Sentencia de 13 de noviembre de 2018, Levola Hengelo, C-310/17, EU:C:2018:899, apartado 40).

Además, el algoritmo, como componente integrado en un programa de ordenador –que no en sí mismo–, puede acogerse a la protección jurídica que la Propiedad intelectual dispensa a esta figura[32]. Así, el artículo 96 LPI entiende por programa de ordenador "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático

---

[31] En cambio, cuando la realización de un objeto ha venido determinada por consideraciones técnicas, reglas u otras exigencias que no han dejado espacio al ejercicio de la libertad creativa, no puede considerarse que dicho objeto tenga la originalidad necesaria para constituir una obra (véase, en este sentido, la Sentencia de 1 de marzo de 2012, Football Dataco y otros, C-604/10, EU:C:2012:115, apartado 39 y jurisprudencia citada).

[32] En el ámbito europeo, véase la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador.

para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación", lo que comprende también su documentación preparatoria. Y documentación técnica, así como los manuales de uso de un programa gozarán de la misma protección. Eso sí, el programa de ordenador es protegido únicamente si es original, en el sentido de ser una creación intelectual propia de su autor[33].

Ahora bien, como proclaman los Considerandos 10 y 11 de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador: "(10) La función de un programa de ordenador es comunicarse y trabajar con otros componentes del sistema de ordenador y con sus usuarios y, a tal fin, se exige contar con un sistema lógico y, cuando sea conveniente, físico de interconexión e interacción para permitir a los elementos de los soportes físicos y lógicos trabajar con otros soportes físicos y lógicos y con usuarios, en la forma prevista. Las partes del programa que establecen dicha interconexión e interacción entre los elementos de software y hardware suelen denominarse «interfaces». La interconexión e interacción funcional suele conocerse como «interoperabilidad»; dicha interoperabilidad puede ser definida como la capacidad de los programas de ordenador para intercambiar información y utilizar mutuamente la información así intercambiada. (11) Para evitar cualquier duda, debe establecerse claramente que solo se protege la expresión del programa de ordenador y que las ideas y principios implícitos en los elementos del programa, incluidas las de sus interfaces, no pueden acogerse a la protección de los derechos de autor con arreglo a la presente Directiva. De acuerdo con este principio de derechos de autor, en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están protegidos con arreglo a la presente Directiva. De acuerdo con la legislación y jurisprudencia de los Estados miembros y los convenios internacionales en la materia, la expresión de dichas ideas y principios debe protegerse mediante derechos de autor".

---

[33] La duración del derecho sobre el programa de ordenador se establece en el artículo 98 LPI: "1. Cuando el autor sea una persona natural la duración de los derechos de explotación de un programa de ordenador será, según los distintos supuestos que pueden plantearse, la prevista en el capítulo I del Título III de este Libro. 2. Cuando el autor sea una persona jurídica la duración de los derechos a que se refiere el párrafo anterior será de setenta años, computados desde el día 1 de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado".

En consecuencia, en materia de programas de ordenador, como ha declarado el TJUE, en Sentencia de 2 de mayo de 2012, asunto C-310/17, caso "SAS Institute", el objeto de la protección de engloba las formas de expresión de un programa de ordenador, así como los trabajos preparatorios de concepción que pueden llevar respectivamente a la reproducción o a la creación ulterior de tal programa. De ello concluyó el Tribunal de Justicia que el código fuente y el código objeto de un programa de ordenador son formas de expresión de este que, por tanto, merecen la protección del derecho de autor sobre los programas de ordenador. En cambio, por lo que respecta a la interfaz gráfica de usuario, el Tribunal de Justicia declaró que tal interfaz no permite reproducir el programa de ordenador, sino que sólo constituye un elemento de dicho programa por medio del cual los usuarios utilizan las funcionalidades de este. Y, sobre la base de estas consideraciones, declaró que ni la funcionalidad de un programa de ordenador ni el lenguaje de programación o el formato de los archivos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones constituyen una forma de expresión de tal programa; recordando, como había apuntado el Abogado General, que admitir que el derecho de autor pudiera proteger la funcionalidad de un programa de ordenador supondría ofrecer la posibilidad de monopolizar las ideas, en perjuicio del progreso técnico y del desarrollo industrial.

Por su parte, en el ámbito de la propiedad industrial, desde una perspectiva de delimitación negativa, el algoritmo en sí mismo, como ocurre con los programas de ordenador, no puede ser objeto de protección vía patente. Como expresamente establece el artículo 4.4 de la Ley 24/2015, de 24 de julio, de Patentes –LP–: "No se considerarán invenciones en el sentido de los apartados anteriores, en particular: a) Los descubrimientos, las teorías científicas y los métodos matemáticos; b) Las obras literarias, artísticas o cualquier otra creación estética, así como las obras científicas; c) Los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, así como los programas de ordenadores; y d) Las formas de presentar informaciones". De manera que el algoritmo como tal no entra dentro de las invenciones protegibles por patente; si bien, como en el caso del programa de ordenador, ello no le impide gozar de una protección indirecta cuando este constituya un elemento integrante de la invención patentable.

En consecuencia, como ya ocurría con la protección jurídica de los macrodatos, en el ámbito de la propiedad industrial la figura que mejor encaje otorga

al algoritmo como objeto de protección es el secreto empresarial. Ahora bien, recuérdese que deben cumplirse tres requisitos: el ontológico –ser secreto–, objetivo –tener valor comercial– y, sobre todo, subjetivo –adoptar medidas razonables de protección–; y que, en todo caso, se trata de una protección de baja intensidad[34], puesto que no ofrece un derecho de exclusiva, sino que su ámbito de protección queda limitado al artículo 3 LSE. Aunque, tampoco se olvide, el algoritmo como secreto empresarial gozará de una naturaleza patrimonial, será objeto de derecho de propiedad por parte de su titular, que podrá transmitirlo o licenciarlo, y toda apropiación, revelación o utilización realizada sin su consentimiento o incumpliendo los pactos por los que se permitió su uso o acceso, se considerará una violación de secreto empresarial ilícita.

Y, en todo caso, tanto para los algoritmos como para los macrodatos, la protección jurídica de los mismos que ofrecen las distintas figuras del Derecho de la Propiedad intelectual e industrial, puede verse complementada y reforzada por la tutela que ofrece el Derecho contractual, principalmente a través de acuerdos de confidencialidad –todo ello sin perjuicio de que, como proclama la célebre frase de La Celestina: "A quien dices tu secreto, das tu libertad"–.

4. EL BIG DATA Y LOS ALGORITMOS ANTE EL DERECHO DE LA COMPETENCIA

Analizados los mecanismos de protección jurídica de los macrodatos y de los algoritmos ahora procede adentrarse en el proceloso mundo de su relación con el Derecho de la competencia, en su doble vertiente, Defensa de la competencia y Competencia desleal. En relación con la Defensa de la competencia, el perfecto maridaje entre macrodatos, algoritmos e inteligencia artificial está generando nuevos y complejos problemas en materia de acuerdos colusorios y abuso de posición dominante. Por su parte, en el ámbito del Derecho represor de la competencia desleal la cuestión se centra en el análisis de la aplicación del principio de complementariedad relativa y de la jurisprudencia relativa al principio de aprovechamiento indebido del esfuerzo ajeno.

En efecto, en materia de acuerdos colusorios el artículo 101.1 TFUE, al igual que el artículo 1.1 de la Ley 15/2007, de 3 de julio, de Defensa de la

---

[34] Así, Botana Agra, J. M., *Protección jurídica de algoritmos*..., op. cit., p. 158.

Competencia –LDC–, establece que: "Serán incompatibles con el mercado interior y quedarán prohibidos todos los acuerdos entre empresas[35], las decisiones de asociaciones de empresas y las prácticas concertadas que puedan afectar al comercio entre los Estados miembros y que tengan por objeto o efecto impedir, restringir o falsear el juego de la competencia dentro del mercado interior y, en particular, los que consistan en: a) fijar directa o indirectamente los precios de compra o de venta u otras condiciones de transacción; b) limitar o controlar la producción, el mercado, el desarrollo técnico o las inversiones; c) repartirse los mercados o las fuentes de abastecimiento; y d) aplicar a terceros contratantes condiciones desiguales para prestaciones equivalentes, que ocasionen a estos una desventaja competitiva". Por tanto, como es sabido, se prohíben los acuerdos

[35] Téngase en cuenta que el concepto de "empresa" en Derecho de la competencia tiene autonomía conceptual. Es doctrina consolidada por el TJUE que el "concepto de empresa" en el sentido de los artículos 101 y 102 TFUE comprende cualquier entidad que ejerza una actividad económica, con independencia de la naturaleza jurídica de dicha entidad y de su modo de financiación –por todas, STJUE de 10 de septiembre de 2009, asunto C-97/08 P, caso "Akzo Nobel", apartados 54 y 55–. A este respecto, el Tribunal de Justicia ha precisado, por un lado, que en este mismo contexto debe entenderse que el concepto de empresa designa una unidad económica aunque, desde el punto de vista jurídico, dicha unidad económica esté constituida por varias personas físicas o jurídicas; y, por otro lado, que, cuando una entidad económica de este tipo infringe las normas sobre competencia, le incumbe, conforme al principio de "responsabilidad personal", responder por esa infracción –así, entre otras, Sentencias del TJUE de 27 de abril de 2017, caso Akzo Nobel y otros/Comisión, C 516/15 P, apartado 48; de 20 de enero de 2011, caso General Química y otros/Comisión, C 90/09 P, apartados 34 a 36; y de 11 de diciembre de 2007, caso ETI y otros, C 280/06, apartado 38–. La identificación de las entidades que están comprendidas en el perímetro de la empresa depende del objeto de la infracción –así, STJUE de 6 de octubre de 2021, asunto C-882/19, caso "Sumal": "el concepto de "empresa" empleado en el artículo 101 TFUE es un concepto funcional, y la unidad económica constitutiva de dicha empresa debe identificarse desde la perspectiva del objeto del acuerdo de que se trate"–. En ese sistema la responsabilidad recae sobre los activos económicos, en lugar de sobre una determinada personalidad jurídica. La construcción de la personalidad jurídica tradicional del Derecho privado, fundada en los patrimonios separados, también se diluye en el ámbito del Derecho de la competencia. Desde un punto de vista económico, por tanto, la misma empresa que cometió la infracción es considerada responsable tanto de las sanciones públicas como de los daños conforme al Derecho privado.

colusorios entre empresas, tanto en el plano horizontal –cuyo mayor exponente es el cártel[36]– como vertical[37].

Pues bien, como ya hemos dicho, los algoritmos, con la información que ofrecen los macrodatos –"Big data"–, pueden realizar análisis predictivos en materia de precios, preferencias de consumidores, demanda estimada, etcétera, lo que, sin duda, puede tener efectos procompetitivos, en el sentido de que el análisis en tiempo real de los macrodatos permite tomar decisiones empresariales tendentes a optimizar los precios, reducir los costes de producción y transacción, segmentar por grupos y ofrecer precios más ajustados a las características de cada uno de ellos, e, incluso, ofrecer más y mejores servicios y/o productos. Y ello, evidentemente, aumenta la competencia y la eficiencia de los mercados, así como el bienestar de los consumidores[38]. Pero como en una moneda, esta cara (positiva) tiene irremediablemente otra (negativa). Puesto que la conjunción de algoritmos y macrodatos para adaptar precios de forma automatizada y constante puede facilitar nuevas formas de colusión, provocando una reducción del bienestar del consumidor y un funcionamiento ineficiente del mercado, tanto en relaciones horizontales como verticales. La coordinación en el

---

[36] Como establece la Disposición adicional cuarta LDC, punto segundo: "...se entiende por cártel todo acuerdo o práctica concertada entre dos o más competidores cuyo objetivo consista en coordinar su comportamiento competitivo en el mercado o influir en los parámetros de la competencia mediante prácticas tales como, entre otras, la fijación o la coordinación de precios de compra o de venta u otras condiciones comerciales, incluso en relación con los derechos de la propiedad intelectual e industrial; la asignación de cuotas de producción o de venta; el reparto de mercados y clientes, incluidas las colusiones en licitaciones, las restricciones de las importaciones o exportaciones o las medidas contra otros competidores contrarias a la competencia".

[37] Por acuerdos verticales se entienden los acuerdos o prácticas concertadas suscritos entre dos o más empresas que operen, a efectos del acuerdo o de la práctica concertada, en planos distintos de la cadena de producción o distribución y que se refieran a las condiciones en las que las partes pueden adquirir, vender o revender determinados bienes o servicios. En Europa, la aplicación de la prohibición de acuerdos colusorios a los acuerdos verticales está consolidada desde la Sentencia del Tribunal de Justicia de las Comunidades Europeas en los asuntos acumulados 56/64 y 58/64 Grundig-Consten contra Comisión, Rec. 1966, p. 299, y en el asunto 56/65 Technique Minière contra Maschinenbau Ulm GmbH, Rec. 1966, p. 235. En la actualidad, su régimen está en el Reglamento (UE) 2022/720 de la Comisión de 10 de mayo de 2022 relativo a la aplicación del artículo 101, apartado 3, del Tratado de Funcionamiento de la Unión Europea a determinadas categorías de acuerdos verticales y prácticas concertadas.

[38] Véase, Olmedo Peralta, E. (2023). "Colaboración en la generación, intercambio y procesamiento de datos (big data): entre la cooperación lícita y las conductas antitrust", *Cooperación y mercados digitales*, Atelier.

ámbito horizontal y la monitorización en el vertical se han demostrado como los grandes problemas de la relación de los algoritmos con la prohibición de acuerdos colusorios.

En efecto, el desarrollo de los mercados digitales y la inteligencia artificial permite buscar, recolectar, almacenar y analizar, por medio de algoritmos, una inmensa cantidad de datos, lo que contribuye a reforzar la transparencia de dichos mercados –y, en determinadas circunstancias, a reducir o eliminar las barreras de entrada existentes–, y permite que los proveedores, las plataformas digitales e, incluso, los consumidores, puedan adoptar decisiones automatizadas basadas en dicho análisis (efectos procompetitivos). Siendo ello cierto, y una ventaja incontestable, al mismo tiempo es una realidad que este proceso facilita nuevas formas de colusión entre proveedores y entre proveedores y distribuidores (horizontales y verticales). En los mercados digitales los algoritmos de precios pueden ser empleados para monitorizar los precios de los competidores o, en su caso, de los distribuidores, con el objeto de detectar instantáneamente las posibles desviaciones de las condiciones previamente concertadas y, en su caso, poder adoptar las correspondientes medidas disuasorias con una elevadísima frecuencia y de manera automática. Por ello, la coordinación algorítmica en materia de precios facilita conductas que dan lugar a sobreprecios.

Como señala el informe de la OCDE 2023, en términos generales, existen tres formas en las que los algoritmos pueden facilitar la colusión: a) algoritmos que facilitan acuerdos colusorios explícitos: los sistemas automatizados de fijación de precios basados en datos de precios, que pueden detectar y responder a las desviaciones de precios, haciendo más estable la colusión explícita entre empresas (por ejemplo, para implementar el mantenimiento de precios de reventa o un acuerdo de fijación de precios); b) algoritmos en entornos radiales: en las que varias empresas utilizan el mismo software de fijación de precios de terceros que determina sus decisiones de fijación de precios, lo que da como resultado un entorno radial que puede facilitar el intercambio colusorio de información; y c) la colusión algorítmica tácita y autónoma: donde los algoritmos de autoaprendizaje pueden decidir coludir (o al menos evitar alcanzar un resultado competitivo) sin compartir información ni coordinación explícita[39].

---

[39] Sobre la colusión algorítmica, por todos, Framiñan Santas, J. (2020). "La colusión tácita mediante algoritmos de precios", *Big data e internet de las cosas. Nuevos retos para el Derecho de la*

Como ejemplo de colusión algorítmica horizontal, dos empresas acordaron que ninguna de ellas fijaría un precio de venta al público inferior al de la otra para productos vendidos en el Reino Unido a través de Amazon, siempre que no hubiera un tercero vendiendo a un precio inferior. Después de tratar de aplicar el acuerdo de manera manual, las partes llegaron a la conclusión de que su ejecución sería mucho más precisa mediante el uso de algoritmos de precios. Se trataba de programas de inteligencia artificial de precios suministrados por proveedores independientes que fueron configurados para establecer automáticamente un precio más bajo que el de los competidores, con dos excepciones: a) si el precio más barato del mercado era el de una de ellas, el de la otra no sería más bajo en ningún caso, sino –como mucho– igual; y b) se establecía además un precio mínimo, por debajo del cual no se podía establecer, aunque hubiera competidores más baratos. Una vez configurado el algoritmo conforme a tales reglas, el programa ajustaba los precios automáticamente cada 15 minutos, con el resultado de que ambos competidores terminaron fijando precios idénticos para el 99% de los productos.

Por su parte, como ejemplo de monitorización algorítmica de precios y comportamientos prohibidos en acuerdos verticales resulta clásica la cita a las cuatro Decisiones de la Comisión de 24 de julio de 2018[40], en la que se sancionaron

---

competencia y de los bienes inmateriales, Tirant lo Blanch; Robles Martín-Laborda, A., "Cuando el cartelista es un robot: colusión en mercados digitales mediante algoritmos de precios", *Actas de derecho industrial y derecho de autor*, Tomo 38, 2017-2018; y Díez Estella, F. (2023). "La colusión algorítmica: dificultades y retos de su regulación antitrust", *Comunicaciones en propiedad industrial y derecho de la competencia*, núm. 100.

[40] El origen de estas Decisiones hay que situarlo en la investigación sectorial sobre el comercio electrónico realizada por la Comisión, iniciada en mayo de 2015 en el contexto de su estrategia para el mercado único digital. Durante la investigación, la Comisión recabó datos de casi 1.900 empresas que operan en el comercio electrónico y analizó alrededor de 8.000 contratos de distribución y licencia, publicándose el 10 de mayo de 2017 el Informe final. Según decía el informe, a día de hoy, la mayoría de las empresas realizan un seguimiento de los precios en línea de sus competidores, incluidos sus distribuidores. Según la Comisión, las dos terceras partes de los casos analizados utilizan programas informáticos automáticos que ajustan sus propios precios en función de los precios que han observado en sus competidores. Con los programas de monitorización de precios, detectar las desviaciones con respecto a los precios de venta al público «recomendados» es cuestión de segundos, por lo que cada vez más los fabricantes pueden controlar e influir en la fijación de precios de los minoristas. Y la posibilidad de obtener información sobre los precios en tiempo real también puede fomentar la coordinación de precios automatizada entre competidores. Estas tendencias de mercado influyen de forma significativa en las estrategias de distribución y fijación de precios, tanto de los fabricantes como de los minoristas. De hecho, un 42% de los participantes en

diferentes conductas por "fijación de precios de reventa"[41], en asuntos AT.40465, Asus; AT.40469, Denon y Marantz; AT.40181, Philips; y AT.40182, Pioneer, con una multa conjunta total de 111 millones de euros. Es común a todos los casos que la conducta de los fabricantes afectaba principalmente a los distribuidores online que vendían sus productos a un precio más bajo que el recomendado por el fabricante[42]. Según explican las Decisiones, los distribuidores que no aplicaban los precios de reventa recomendados por los fabricantes recibían amenazas o sanciones, como la denegación de suministro. Según la Comisión, los fabricantes utilizaron mecanismos muy sofisticados, basado en algoritmos, para monitorizar los precios de reventa, con lo que podían intervenir rápidamente ante una reducción del precio.

En efecto, en el asunto Asus la monitorización de estos precios de reventa se realizaba a través de varios mecanismos: la observación de webs de comparación de precios, la utilización de un software interno con herramientas de monitorización que permitía identificar a los distribuidores que vendían los productos de Asus por debajo del precio que deseaba la marca, o a través de quejas de sus distribuidores, que informaban a Asus del incumplimiento de precios por parte de otros distribuidores. Asus requirió y exigió, a aquellos distribuidores que vendían por debajo de los precios recomendados, subidas de precios. La conducta se realizó en Alemania y Francia entre 2011 y 2014; y por ello fue sancionada con 63,5 millones de euros.

---

el Informe afirmaron estar afectados por restricciones de precios, si bien este dato incluye prácticas lícitas, como los recomendados y los máximos.

[41] Téngase en cuenta que, el artículo 4 del Reglamento UE 330/2010 –vigente en ese momento–, como el del actual Reglamento UE 720/2022, establecen que: "La exención prevista en el artículo 2 no se aplicará a los acuerdos verticales que, directa o indirectamente, por sí solos o en combinación con otros factores bajo control de las partes, tengan por objeto: a) la restricción de la facultad del comprador de determinar el precio de venta, sin perjuicio de que el proveedor pueda imponer precios de venta máximos o recomendar un precio de venta, siempre y cuando estos no equivalgan a establecer un precio de venta fijo o mínimo como resultado de presiones o incentivos procedentes de cualquiera de las partes".

[42] Del análisis de estos casos podemos extraer una conclusión hermenéutica, que no es nueva: la información es poder y su gestión genera responsabilidad. En las redes de distribución debe interiorizarse la competencia intramarca, tanto por parte de los proveedores como por parte de los propios distribuidores. Recomendar, según la RAE significa, en su tercera acepción, "aconsejar algo a alguien para bien suyo", lo que supone que, cuando un proveedor instaura una política de precios recomendados, sus distribuidores son tan libres de fijar el precio de reventa como si no existiera la recomendación.

Por su parte, Denon monitorizaba los precios de reventa de sus distribuidores a través de webs de comparación de precios, y sus agentes de venta se ponían en contacto con los distribuidores que no seguían el precio recomendado para que ajustaran el precio, con la consiguiente amenaza de denegarles las existencias en caso de no cumplir con el precio recomendado. Por dicha conducta, producida en Alemania y los Países Bajos entre 2011 y 2015, para productos de audio y vídeo, Denon fue sancionada con 7,7 millones de euros.

Philips, por su parte, monitorizaba y contactaba directamente a los distribuidores que no cumplían con el precio recomendado o actuaba tras recibir quejas de otros distribuidores que sí aplicaban y seguían los precios recomendados, amenazando con dar por concluidas las relaciones comerciales con ellos si no reajustaban sus precios. La conducta de Philips se realizó en Francia respecto de varios productos de electrónica entre 2011 y 2013, por lo que recibió una multa de 29,8 millones de euros.

Y, finalmente, Pioneer, además de monitorizar e intervenir en el precio de los distribuidores, trataba de impedir las importaciones paralelas, tomando medidas para desincentivar las ventas transfronterizas y, de este modo, evitar que los distribuidores con precios más bajos vendieran fuera de su territorio y generaran así un mercado de precios inestable en los territorios objetivo. Estas conductas afectaron a los distribuidores de un total de 12 Estados Miembros, incluida España, entre el 2011 y el 2013. Y la sanción impuesta a Pioneer por estas conductas fue de 10,2 millones de euros.

Ahora bien, la propia Comisión tiene claro que la monitorización de precios en acuerdos verticales no está prohibida "per se" y en la Comunicación de la Comisión, 30 de junio de 2022, sobre "Directrices relativas a las restricciones verticales" se avala expresamente la monitorización y la notificación de precios, siempre que no vengan acompañadas de medidas tendentes a fijar el precio de reventa. Así, se proclama que: "El control de precios se utiliza cada vez más en el comercio electrónico, donde tanto los proveedores como los minoristas suelen utilizar programas informáticos de control de precios. Este programa informático aumenta la transparencia de los precios en el mercado, lo cual permite que los fabricantes hagan un seguimiento eficaz de los precios de reventa en su red de distribución. También permite a los minoristas seguir los precios de sus competidores. Sin embargo, por sí mismos, el seguimiento y la notificación de los precios no constituyen una imposición del precio de reventa". Y, en nuestra

opinión, esta posición es correcta, porque monitorizar es una cosa (efecto procompetitivo) y exigir el cumplimiento a los distribuidores de una concreta política de precios otra (efecto restrictivo). Y, en las cuatro Decisiones Comisión de 2018 ocurría lo segundo, no lo primero.

Por su parte, en el ámbito de las conductas unilaterales, el uso de los macrodatos y algoritmos por parte de empresas en posición de dominio puede conllevar a conductas constitutivas un abuso. Recuérdese que el artículo 102 TFUE, al igual que el artículo 2 LDC, establece que: "Será incompatible con el mercado interior y quedará prohibida, en la medida en que pueda afectar al comercio entre los Estados miembros, la explotación abusiva, por parte de una o más empresas, de una posición dominante en el mercado interior o en una parte sustancial del mismo. Tales prácticas abusivas podrán consistir, particularmente, en: a) imponer directa o indirectamente precios de compra, de venta u otras condiciones de transacción no equitativas; b) limitar la producción, el mercado o el desarrollo técnico en perjuicio de los consumidores; c) aplicar a terceros contratantes condiciones desiguales para prestaciones equivalentes, que ocasionen a estos una desventaja competitiva; y d) subordinar la celebración de contratos a la aceptación, por los otros contratantes, de prestaciones suplementarias que, por su naturaleza o según los usos mercantiles, no guarden relación alguna con el objeto de dichos contratos".

En este sentido, la empresa en posición de dominio, independientemente de las causas que expliquen dicha posición, tiene una "responsabilidad especial" de no impedir, con su comportamiento, el desarrollo de una competencia efectiva y no falseada en el mercado común[43]. Por ello se prohíbe su abuso[44]. Si bien,

---

[43] Como ha declarado la STJUE de 30 de septiembre de 2003, asunto T-203/01, caso "Michelin": "Por consiguiente, aunque la acreditación de la existencia de una posición dominante no implica, en sí misma, ningún reproche a la empresa de que se trate, sí supone que incumbe a esta, independientemente de las causas que expliquen dicha posición, una responsabilidad especial de no impedir, con su comportamiento, el desarrollo de una competencia efectiva y no falseada en el mercado común... Del mismo modo, si bien la existencia de una posición dominante no priva a una empresa que se encuentra en dicha posición del derecho a proteger sus propios intereses comerciales cuando estos se ven amenazados, y si bien dicha empresa puede, en una medida razonable, realizar los actos que considere adecuados para proteger sus intereses, no cabe admitir tales comportamientos cuando su objeto es precisamente reforzar dicha posición dominante y abusar de ella".

[44] Según reiterada jurisprudencia, el concepto de explotación abusiva es un concepto objetivo que se refiere a las actividades de una empresa en situación de posición dominante que pueden influir en la estructura de un mercado en el que, debido justamente a la presencia de la empresa

no existe una lista exhaustiva de prácticas que constituyan abuso, ni tampoco una definición omnicomprensiva del concepto. De modo que, con carácter general, es posible identificar tres tipos de abusos: explotativos, exclusionarios y mixtos. Los primeros, son aquellos que persiguen explotar las oportunidades que entrega la posición de dominio para afectar directamente a consumidores, como ejemplo, la modificación unilateral de condiciones comerciales, la imposición de precios excesivos, la discriminación arbitraria de precios o la vulneración de la privacidad. Los segundos, están encaminados a excluir a determinados agentes económicos o generan una desventaja artificial con respecto a los rivales. Se trata de conductas que razonablemente son capaces de crear, aumentar, o prolongar el poder monopólico de una empresa al limitar las oportunidades de sus competidores; y, al mismo tiempo, restringen el bienestar de los consumidores de manera indirecta, ya que se ven impedidos de los beneficios del proceso competitivo, aunque en el corto plazo pueda conllevar una rebaja de precios o mejores condiciones comerciales. Estas conductas pueden consistir en precio predatorios –lo que consiste en competir agresivamente, soportando pérdidas o renunciando a beneficios en el corto plazo, con el objeto de inducir la salida de un competidor o entrante y así obtener una posición dominante en el futuro, perjudicando a los consumidores–; negativa de venta –lo que ocurre, por ejemplo, cuando una empresa dominante goza de una instalación o insumo esencial aguas arriba, que le entrega una posición dominante en el mercado vertical aguas abajo; y un competidor en el mercado aguas abajo busca acceder a dicha instalación, lo que le es denegado por la empresa dominante de manera directa o indirecta, mediante dilaciones en la negociación o el establecimiento de precios excesivamente altos (estrangulamiento de márgenes)–; y/o acuerdos de exclusividad –obviamente, una empresa dominante puede intentar excluir a sus competidores impidiéndoles que vendan a clientes mediante obligaciones

---

de que se trata, la intensidad de la competencia se encuentra ya debilitada y que obstaculizan, recurriendo a medios diferentes de los que rigen una competencia normal de productos o servicios basada en las prestaciones de los agentes económicos, el mantenimiento del grado de competencia que aún exista en el mercado o el desarrollo de dicha competencia (Sentencias del Tribunal de Justicia de 13 de febrero de 1979, Hoffmann-La Roche/Comisión, 85/76, Rec. p. 461, apartado 91; de 9 de noviembre de 1983, Michelin/Comisión, 322/81, Rec. p. 3461, apartado 70, y de 3 de julio de 1991, AKZO/Comisión, C-62/86, Rec. p. I-3359, apartado 69; Sentencia del Tribunal de Primera Instancia de 7 de octubre de 1999, Irish Sugar/Comisión, T-228/97, Rec. p. II-2969, apartado 111).

de compra exclusiva o descuentos, denominados conjuntamente acuerdos exclusivos–. Y, finalmente, los abusos mixtos, se corresponden a aquellos abusos que tienen un componente exclusionario y uno explotativo, como es el caso de las ventas vinculadas –esta conducta consiste en la venta de dos productos o servicios que son diferentes entre sí (vinculante y vinculado), de manera condicionada, por una empresa con poder de mercado sobre uno de los productos– y discriminación arbitraria de precio –que, en términos generales, consiste en cobrar precios diferentes por productos similares que tienen el mismo costo marginal–.

Pues bien, según el informe de la OCDE 2023, una conducta algorítmica unilateral realizada por una empresa en posición de dominio puede replicar el modelo de abuso de exclusión y/o de explotación. Así, podemos encontrarnos ante una conducta excluyente algorítmica como: a) la autopreferencia; b) los precios predatorios; c) los descuentos; y d) la vinculación y agrupación; o bien, antes una conducta de explotación algorítmica la identifica como: i) la fijación de precios excesivos[45]; ii) las condiciones comerciales desleales; y iii) la discriminación de precios. La evidencia de esta realidad, unida a la convicción de que el Derecho de Defensa de la competencia por sí solo no sería suficiente para reprimir y/o acabar con este tipo de conductas, particularmente en el ámbito de las plataformas digitales, es lo que ha dado origen al Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)[46]. Como establece en su Considerando Tercero: "Un reducido número de grandes empresas prestadoras de servicios básicos de plataforma han acumulado un gran poder económico, lo que podría cualificarlas para que se las designe como guardianes de acceso de conformidad con el presente Reglamento[47]. Por lo general, tienen

---

[45] Sobre ello, Rodilla Martí, C. (2018). *Los precios excesivos por explotación como ilícito del derecho de la competencia*, Thomson-Aranzadi.

[46] Por todos, Ruiz Peris, J. I. (2023). "El Reglamento de mercados digitales (Reglamento (UE) 2022/1925) y la acción de las Autoridades nacionales de competencia (ANCs) de los Estados miembros", *Revista de derecho de la competencia y la distribución*, núm. 33; ídem., "La nueva digital market act, una respuesta híbrida de la Unión Europea a los "gatekeepers" GAFA", *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 57, 2021.

[47] Con fecha de 6 de septiembre de 2023, la Comisión Europea designó seis guardianes de acceso en virtud del Reglamento de mercados digitales. Se trata de Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft. Se supone que las empresas que prestan al menos uno de los diez

la capacidad de conectar a muchos usuarios profesionales con muchos usuarios finales a través de sus servicios, lo que, a su vez, les permite trasladar sus ventajas, como su acceso a grandes cantidades de datos, de un ámbito de actividad a otro. Algunas de estas empresas controlan ecosistemas completos de plataformas en la economía digital y a los operadores de mercado existentes o nuevos, con independencia de lo innovadores y eficientes que puedan ser, les resulta sumamente difícil, por motivos estructurales, competir con ellos o disputarles el mercado. La disputabilidad se reduce en particular debido a la existencia de enormes obstáculos a la entrada o la salida del mercado, como unos altos costes de inversión, que no pueden recuperarse, o al menos no fácilmente, en caso de salida, y la ausencia de algunos insumos clave en la economía digital, como los datos, o un acceso reducido a estos. Como consecuencia de ello, aumenta la probabilidad de que los mercados subyacentes no funcionen bien o de que pronto dejen de funcionar bien"; afirmando en su Considerando Quinto que: "De ello se deduce que la dinámica del mercado a menudo es incapaz de garantizar resultados económicos justos con respecto a los servicios básicos de plataforma. Aunque los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea (TFUE) se aplican a la conducta de los guardianes de acceso, el ámbito de aplicación de dichas disposiciones se limita a determinados casos de poder de mercado (por ejemplo, dominio en mercados específicos) y de comportamiento contrario a la competencia, y el control del cumplimiento se produce ex post y requiere una investigación extensa caso por caso de hechos a menudo muy complejos. Además, el Derecho de la Unión vigente no aborda, o al menos no de manera eficaz, los retos para el funcionamiento eficaz del mercado interior que plantea la conducta

---

servicios básicos de plataforma enumerados en el Reglamento son guardianes de acceso si cumplen los criterios enumerados a continuación. Estos servicios básicos de plataforma son los siguientes: servicios de intermediación en línea, tales como tiendas de aplicaciones, motores de búsqueda en línea, servicios de redes sociales, determinados servicios de mensajería, servicios de plataformas de intercambio de vídeos, asistentes virtuales, navegadores web, servicios de computación en nube, sistemas operativos, mercados en línea y servicios de publicidad. Una misma empresa puede ser designada como guardián de acceso en lo que respecta a varios servicios básicos de plataforma. Por su parte, existen tres criterios cuantitativos principales que originan la presunción de que una empresa es un guardián de acceso a tenor del Reglamento: a) cuando la empresa alcance un determinado volumen de negocios anual en el Espacio Económico Europeo y preste un servicio básico de plataforma en al menos tres Estados miembros de la UE; b) cuando la empresa preste un servicio básico de plataforma a más de 45 millones de usuarios finales activos mensuales establecidos o situados en la UE y a más de diez mil usuarios profesionales activos anuales establecidos en la UE; y c) cuando la empresa haya cumplido el segundo criterio durante los tres últimos años.

de los guardianes de acceso que no son necesariamente dominantes en términos de derecho de la competencia"[48].

Pues bien, volviendo al ámbito de la competencia y la conducta unilateral algorítmica constitutiva de abuso de posición de dominio, en esta sede resulta obligada la cita al asunto T-612/17, caso "Google Shopping". La Comisión Europea impuso a Google una multa de 2.400 millones de euros por abuso de posición dominante como motor de búsqueda por dar una ventaja ilegal a su propio servicio de compras comparativas, es decir, por un comportamiento de autopreferencia[49] –resolución que el 10 de noviembre de 2021 fue ratificada por el Tribunal General de la Unión Europea–.

En 2004, Google entró en el mercado de los servicios de compras comparativas en Europa, con un producto que se llamó inicialmente «Froogle» y que desde 2013 se llama «Google Shopping». Este producto permite a los consumidores comparar productos y precios en internet, así como encontrar ofertas de minoristas en línea de todo tipo, como tiendas virtuales de fabricantes, plataformas (Amazon, eBay, etc.) y otros revendedores. En 2008, Google inició en los mercados europeos un cambio fundamental de estrategia para impulsar su servicio de compras comparativas. Esta estrategia se basaba, según la Comisión, en la posición dominante de Google en las búsquedas de carácter general en internet, y no en la competencia según los méritos en los mercados de las compras comparativas: a) Google colocaba sistemáticamente en un lugar destacado su propio servicio de compras comparativas: cuando un consumidor hacía una consulta en el motor de búsqueda de Google sobre la cual el servicio de compras comparativas de Google desea mostrar resultados, estos aparecían en la parte superior de la lista de resultados de búsqueda, o cerca de ella; y b) Google colocaba en peor lugar los servicios de compras comparativas rivales en los resultados de búsqueda que ofrecía: los servicios de compras comparativas rivales aparecían en la lista de

---

[48] Véase, Estevan de Quesada, C. (2023). "Los gigantes tecnológicos: regulación y Derecho de la competencia", *De Iure Mercatus. Libro Homenaje al Profesor Dr. Dr.h.c. Alberto Bercovitz Rodríguez-Cano*, Tirant lo Blanch.

[49] Sobre ello, Ruiz Peris, J. I. (2021). "Gatekeepers, discriminación autopreferente exclusionaria y reforzamiento de la posición de dominio: la nueva propuesta europea de Digital Market Act", *Competencia en mercados digitales y sectores regulados*, Tirant lo Blanch; y Diez Estella, F. (2021). "El abuso de dominio por las plataformas digitales: Google en el banquillo", *Competencia en mercados digitales y sectores regulados*, Tirant lo Blanch.

resultados de búsqueda de Google según los algoritmos de búsqueda genérica de esta compañía. Google incluía diversos criterios en estos algoritmos, con el resultado de que los servicios de compras comparativas rivales aparecieran en peor posición –puede comprobarse que, incluso el servicio rival mejor situado, aparecía por término medio solo en la cuarta página de resultados de búsqueda de Google, y otros figuran incluso más abajo–. Mientras que el propio servicio de compras comparativas de Google no estaba sometido a los algoritmos de búsqueda genérica de aquel, incluida la colocación en posiciones menos favorables. La consecuencia de todo ello fue, para la Comisión, que el servicio de compras comparativas de Google les aparecía a los consumidores de forma mucho más visible en los resultados de las búsquedas, mientras que la visibilidad de los servicios rivales era mucho menor[50].

Finalmente, en el ámbito del Derecho de la Competencia desleal, el punto de partida debe situarse en la doctrina consolidada por el Tribunal Supremo sobre el "principio de complementariedad relativa", proclamado, entre otras, en la Sentencia 450/2015, de 2 de septiembre: "Partiendo de la distinta función que cumplen las normas de competencia desleal y las de marcas, el criterio de la complementariedad relativa sitúa la solución entre dos puntos: de una parte, la mera infracción de estos derechos marcarios no puede constituir un acto de competencia desleal; y de otra, tampoco cabe guiarse por un principio simplista de especialidad legislativa, que niega la aplicación de la Ley de Competencia Desleal cuando existe un derecho exclusivo reconocido en virtud de los registros marcarios a favor de sus titulares y estos pueden activar los mecanismos de defensa de su exclusiva (Sentencia 586/2012, de 17 de octubre)".

En este sentido, como acertadamente ha declarado la doctrina[51], con este presupuesto hay que concluir que la mera infracción del derecho sui generis del productor de una base de datos constituida por macrodatos, o del derecho sobre el secreto empresarial, no debe dar lugar, sin más, al ejercicio de las acciones por competencia desleal. Cosa distinta es que, además de la infracción del derecho,

---

[50] Google implantó esta práctica en todos los países del EEE donde utiliza este producto de compras comparativas, comenzando en enero de 2008 en Alemania y el Reino Unido. Posteriormente la hizo extensiva a Francia en octubre de 2010, a Italia, Países Bajos y España en mayo de 2011, a Chequia en febrero de 2013 y a Austria, Bélgica, Dinamarca, Noruega, Polonia y Suecia en noviembre de 2013.

[51] García Vidal, A. *La protección de los macrodatos*..., op. cit., pp. 65-66.

exista un acto de confusión o asociación o algún otro acto de deslealtad en el mercado como, por ejemplo, el aprovechamiento indebido del esfuerzo ajeno. En estos casos no se estaría duplicando protección, sino que se estaría aplicando la LCD a conductas que, en realidad, han quedado al margen de la valoración realizada por las normas de propiedad industrial o intelectual. Aunque, en realidad, la jurisprudencia ha reducido significativamente el margen de apreciación de deslealtad en este ámbito. Así, en la clásica Sentencia 827/2011 del Tribunal Supremo, de 22 de noviembre, en relación con el volcado de una base de datos, se afirmó que: "El aprovechamiento de esfuerzo ajeno, en el que se sustenta la pretensión actora, no constituye por sí solo un ilícito concurrencial, con independencia de su cita como ejemplo genérico de comportamiento desleal en algunas sentencias de esta Sala. De haber sido como la recurrente pretende resultaría inexplicable que para el ilícito del art. 11.2 LCD se exija la existencia, como presupuesto, de la imitación de un producto, y esta Sala tiene reiterado que no cabe la degradación de los tipos por reducción de elementos, lo que ocurriría de estimar aplicable sin más la cláusula general ex art. 5º a dicha actuación. Para que el aprovechamiento del esfuerzo ajeno pueda constituir el ilícito pretendido, además de su propia consustancialidad en relación con los términos de la expresión, y una cierta entidad, se requiere que concurra el reproche de desleal, es decir, que integre una actuación incorrecta o irregular en la perspectiva de la buena fe objetiva, de modo que afecte –suprima, restrinja o falsee– la estructura competitiva o el normal funcionamiento del mercado.

En el caso no cabe desconocer que relaciones de profesionales y centros sanitarios, y su localización, similares a la en conflicto, figuran en los Catálogos de Servicios de las entidades prestacionales sanitarias, de fácil acceso para el público, y que cualquier interesado puede aprovechar su contenido para ponerse en contacto con los relacionados para contratarlos y ofrecerles formar parte de un Cuadro Asistencial sin ninguna traba legal que lo impida. Que la inclusión en el Cuadro una vez obtenida la aceptación sea sin copia de la relación que facilitó la información o por el procedimiento del "volcado", en la terminología al uso, no resulta relevante en la perspectiva de la competencia desleal. Es claro que, al copiar los datos, se facilita la labor al respecto de quien carece de datos de investigación propia o trata de completar estos, pero a salvo traba contractual o derecho de exclusiva, que no constan, no cabe negar la accesibilidad y utilización de la información ajena, por mucho que lograr esta hubiera supuesto, para el que la obtuvo, empleo de tiempo, dinero y energías. Continuamente sucede en el

mercado que las empresas aprovechan las informaciones y experiencias de otras, lo que facilita el desarrollo y el progreso social y económico, y con ello no se resiente el buen orden de dicho mercado, a cuya protección responde la Ley de Competencia Desleal. No ha habido un comportamiento irregular concurrencial y no hay ningún imperativo ético o de honradez que conculque el estándar de comportamiento justo y honrado reconocido en el tráfico, tal y como viene exigiendo la reiterada doctrina jurisprudencial. No basta que exista una práctica molesta para que se pueda aplicar la cláusula general de comportamiento contrario a la buena fe objetiva del art. 5º LCD, y menos habría sido admisible que el mero aprovechamiento del esfuerzo ajeno pudiera haber servido de soporte para el singular efecto pretendido de eliminar del mercado a un competidor".

5. CONCLUSIONES

Como apuntábamos al principio de este trabajo, en la era de la economía digital los métodos para recopilar, analizar y procesar el "Big data", fundamentalmente a través de algoritmos, así como el conocimiento adquirido en dicho proceso, han adquirido la condición activos especialmente valiosos y, por tanto, dignos de tutela. En el trabajo se han analizado los diferentes mecanismos que el Derecho de la Propiedad intelectual e industrial ofrecen para una mejor tutela de los macrodatos y de los algoritmos, concluyendo, en ambos casos, que –probablemente– la mejor vía –por sus requisitos y singularidades– sea el "secreto empresarial".

Por su parte, la asociación entre macrodatos, algoritmos e inteligencia artificial está generando nuevos y complejos problemas en materia de acuerdos colusorios y abuso de posición dominante. Cuestiones como la colusión algorítmica de precios o la monitorización de precios, tanto en acuerdos horizontales como verticales, así como la conducta unilateral algorítmica por parte de empresas en posición de dominio son algunos de los grandes retos de Derecho de Defensa de la Competencia. Y ya han sido objeto, por una parte, de importantes resoluciones –como se ha visto–; y, por otra, de medidas más drásticas, de naturaleza regulatoria, como el Reglamento de mercados digitales para los "guardianes de acceso".

En conclusión, parafraseando al maestro Garrigues, "Derecho vivo" en su máxima esencia. Derecho que todavía está configurándose a nivel global y en el que muchos intereses hay en juego. Y Derecho del que todos nosotros tenemos en estos momentos el privilegio y la responsabilidad de trabajar por que sea "un mejor Derecho", como nos alentaba Von Ihering en su conocida obra "La lucha por el Derecho".

BIBLIOGRAFÍA

AA. VV. (2020). *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, García Vidal (dir.), Tirant lo Blanch.

Botana Agra, J. M. (2020). "Protección jurídica de algoritmos y programas de ordenador", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch.

Díez Estella, F. (2021). "El abuso de dominio por las plataformas digitales: Google en el banquillo", *Competencia en mercados digitales y sectores regulados*, Tirant lo Blanch.

Díez Estella, F. (2023). "La colusión algorítmica: dificultades y retos de su regulación antitrust", *Comunicaciones en propiedad industrial y derecho de la competencia*, núm. 100.

Drexl, J. (2017). "Designing Competitive Markets for Industrial Data", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 8, núm. 4.

Estevan de Quesada, C. (2023). "Los gigantes tecnológicos: regulación y Derecho de la competencia", *De Iure Mercatus. Libro Homenaje al Profesor Dr. Dr.h.c. Alberto Bercovitz Rodríguez-Cano*, Tirant lo Blanch.

Framiñan Santas, J. (2020). "La colusión tácita mediante algoritmos de precios", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch.

García Vidal, A. (2020). "Big data e internet de las cosas: su impacto en el Derecho de la competencia y de la Propiedad industrial e intelectual", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch.

García Vidal, A. (2020). "La protección de los macrodatos: exclusividad versus libre acceso", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, Tirant lo Blanch.

Girona Domingo, R. (2022). *Las acciones civiles en defensa del secreto empresarial*, Atelier.

Gómez-Segade, J. A. "La nueva ley de secretos empresariales", *Actas de derecho industrial y derecho de autor*, Tomo 40, 2019-2020.

Gómez-Segade, J. A. (2020). "La protección de los macrodatos (big data) mediante las normas sobre secretos empresariales", *Big data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*, García Vidal (dir.), Tirant lo Blanch.

Gómez-Segade, J. A. (2015). "Los bienes inmateriales en el Anteproyecto de Ley del Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, Universidad Carlos III de Madrid.

Minero Alejandre, G. (2014). *La protección jurídica de las bases de datos en el ordenamiento europeo*, Tecnos.

Olmedo Peralta, E. "Colaboración en la generación, intercambio y procesamiento de datos (big data): entre la cooperación lícita y las conductas antitrust", *Cooperación y mercados digitales*, Atelier.

Robles Martín-Laborda, A. "Cuando el cartelista es un robot: colusión en mercados digitales mediante algoritmos de precios", *Actas de derecho industrial y derecho de autor*, Tomo 38, 2017-2018.

Rodilla Martí, C. (2018). *Los precios excesivos por explotación como ilícito del derecho de la competencia*, Thomson-Aranzadi.

Ruiz Peris, J. I. (2023). "El Reglamento de mercados digitales (Reglamento (UE) 2022/1925) y la acción de las Autoridades nacionales de competencia (ANCs) de los Estados miembros", *Revista de derecho de la competencia y la distribución*, núm. 33.

Ruiz Peris, J. I. (2021). "Gatekeepers, discriminación autopreferente exclusionaria y reforzamiento de la posición de dominio: la nueva propuesta europea de Digital Market Act", *Competencia en mercados digitales y sectores regulados*, Tirant lo Blanch.

Ruiz Peris, J. I. (2021). "La nueva digital market act, una respuesta híbrida de la Unión Europea a los "gatekeepers" GAFA", *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 57.

Valpuesta Gastaminza, E. (2023). "El Derecho digital como categoría transversal en el ordenamiento jurídico y su relación con el Derecho Mercantil", *De Iure Mercatus. Libro Homenaje al Profesor Dr. Dr.h.c. Alberto Bercovitz Rodríguez-Cano*, Tirant lo Blanch.

Capítulo 10
DISCRIMINACIÓN ALGORÍTMICA[1]

Ana Garriga Domínguez
Profesora Titular de Filosofía del Derecho[2]
Universidad de Vigo
https://orcid.org/0000-0003-2846-3448

1. INTRODUCCIÓN

El desarrollo de las tecnologías digitales ha supuesto un considerable impacto social, político e individual. Las sucesivas etapas de este proceso han posibilitado importantes avances en nuestro progreso económico o científico, si bien, la evolución de la informática, de las tecnologías de la Información y la Comunicación (TIC) y, especialmente en la actualidad, de la inteligencia artificial (IA) han suscitado serias y justificadas inquietudes al posibilitar nuevas formas de agresión a la dignidad y autonomía de las personas, a su identidad y a la capacidad de pensar libremente[3] y, en general, al conjunto de los derechos fundamentales. Esta preocupación por la "*erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías*"[4] no es nueva, sino que surge a medida que el desarrollo del software y del hardware posibilitan el tratamiento

[1] Este trabajo se ha realizado en el marco del proyecto de investigación DATATRANSCO con referencia núm. PID2021-128309NB-I00.

[2] Acreditada para el acceso a concursos de catedráticas/os de universidad.

[3] *Vid*. De Asís Roig, R. (2022). "Sobre la propuesta de los neuroderechos", *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 47, pp. 51-70; Yuste, R. (2022). "Los neuroderechos: un abordaje de derechos humanos para la neurotecnología", RECHE Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*, Aranzadi, Cizur Menor, pp. 29-34.

[4] Pérez Luño, A. E. (1992). "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data", García San Miguel, L. (ed.), *Estudios sobre el derecho a la intimidad,* Tecnos, Madrid, p. 37.

automatizado de la información personal y cuando las sucesivas generaciones de computadores posibilitaron una mayor rapidez y eficiencia en estas tareas.

Tradicionalmente se ha venido identificando el derecho a la vida privada como aquel más amenazado por el desarrollo tecnológico, aunque el desarrollo de las tecnologías digitales tiene el potencial de afectar casi a cualquier derecho fundamental y como ha señalado Rafael de Asís, "*una sola aplicación de Inteligencia Artificial puede impactar en una gran cantidad de derechos*"[5]. En el propio preámbulo del Reglamento General de Protección de Datos (RGPD) se indican varios derechos objeto de protección, así como los riesgos de discriminación y usurpación de la identidad (Considerandos 4 y 75). La relación entre el tratamiento de datos personales sin las debidas garantías y las posibilidades de discriminación ha sido señalada constantemente por la doctrina especializada[6], ya que las normas sobre protección de datos personales se proyectan sobre la elaboración de perfiles y la adopción de decisiones automatizadas[7] y, en ese sentido, ha venido siendo interpretado el art. 18.4 de nuestra Constitución (CE) por el Tribunal Constitucional (TC)[8]. La razón de esta proyección como habrá de señalar el Tribunal Europeo de Derechos humanos (TEDH) se encuentra en la intensa relación de este derecho fundamental con el valor de la dignidad humana[9], que se proyecta en sus dos dimensiones: la noción de autodisponibilidad y autodeterminación y que podemos definirla como "*un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás*"[10]

---

[5] De Asís Roig, R. (2022). *Derechos y tecnologías*, Madrid, Dykinson, p. 102.

[6] Me remito a lo expuesto en mi trabajo *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2015. Particularmente, pp. 62-73.

[7] Las decisiones administrativas o privadas que se basen, como único fundamento, en un tratamiento automático de información personal se regulan por primera vez en la ley francesa de *Informátique, aux fichiers et aux libertés*, de 1978. También se recogió en el ámbito del Derecho español en el art. 12 sobre *Impugnación de valoraciones basadas exclusivamente en datos automatizados,* en la pionera Ley Orgánica 5/1992, de 29 de octubre, LORTAD y, asimismo, en el art. 15 de la Directiva 95/46/CE.

[8] Entre otras, SSTC 11/1998, de 13 de enero; 292/2000, de 30 de noviembre y 76/2019, de 22 de mayo.

[9] Entre otras, STEDH de 20 diciembre 2005, asunto Wisse c. Francia.

[10] STC 53/1984, de abril. También, SSTC 115/2010, de 24 de noviembre y 23/2010, de 27 de abril, entre otras.

y, la segunda dimensión, que hace referencia al igual valor que como ser humano tiene cada persona, directamente relacionada con la prohibición de discriminación, pues se niega a quien se discrimina su condición plena como ser humano.

La preocupación por la discriminación algorítmica ha estado presente en muchas de las recomendaciones que ha ido adoptando el Consejo de Europa[11]. En su Recomendación CM/Rec(2020)1 sobre *el impacto de los sistemas algorítmicos en los derechos humanos*, se subraya la necesidad de garantizar que los desequilibrios raciales, de género y otros desequilibrios sociales y laborales que aún no se han eliminado de nuestras sociedades no se perpetúen deliberada o accidentalmente a través de sistemas algorítmicos, así como la conveniencia de abordar estos desequilibrios mediante el uso de tecnologías adecuadas. Esta misma idea se recoge en *Recomendación sobre la ética de la inteligencia artificial* de la UNESCO, en relación con los sesgos que la IA puede "*incorporar y exacerbar, lo que puede llegar a provocar discriminación, desigualdad, brechas digitales y exclusión y suponer una amenaza para la diversidad cultural, social y biológica, así como generar divisiones sociales o económicas*" e, igualmente, en las Directrices éticas para una IA fiable del Grupo de expertos de alto nivel sobre inteligencia artificial de la Comisión Europea. En definitiva, puede afirmarse que existe un consenso generalizado acerca del impacto, en ocasiones grave o muy grave, en el principio de igualdad y no discriminación de determinados diseños, aplicaciones, sistemas y usos de las tecnologías de IA. No obstante, y si bien esto es cierto, también es posible utilizar la IA para descubrir y señalar discriminaciones sociales ocultas, por ejemplo, mediante la búsqueda de patrones discriminatorios ocultos al ojo humano[12].

Para comprender en fenómeno de la discriminación algorítmica debemos detenernos en las características de la presente revolución tecnológica, cuyo centro son las tecnologías del ámbito de la IA, que se sirven de grandes conjuntos de datos (Big Data) y que se basan en aprendizaje automático. El desarrollo de la IA

---

[11] Así se recogía en su Recomendación (2010)13 del 23 de noviembre de 2010, sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles en el ámbito del Big Data, que ha sido actualizada por la Recomendación CM/Rec (2021)8 del Comité de Ministros del Consejo de Europa en materia de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la elaboración de perfiles.

[12] Zuiderveen Borgesius, F. (2018). *Discrimination, artificial intelligence, and algorithmic decision-making,* Consejo de Europa, p. 16.

ha estado facilitada y condicionada por la cantidad de información disponible, pero también por el desarrollo de un conjunto de tecnologías, que se conocen como minería de datos, que empleando complejos algoritmos y estadística realizan predicciones, extraen información oculta o correlaciones imprevistas y, en último término, favorecen la toma de decisiones. Su potencial discriminatorio se aborda en la Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)), en donde se señalan ya los principales aspectos que deben ser tenidos cuenta en el desarrollo de los sistemas de IA para garantizar la seguridad y los derechos de las personas[13].

2. SISTEMAS DE INTELIGENCIA ARTIFICIAL Y SESGOS

En el ámbito de las ciencias computacionales se ha perseguido con ahínco el objetivo de *"lograr que una máquina tenga una inteligencia de tipo general similar a la humana"*[14]. En este sentido, los dos modelos computacionales más importantes plantean las dos visiones principales de IA: la débil y la fuerte. Los avances que se han producido en el ámbito de la IA se corresponderían con la IA débil, pues la *"Inteligencia Artificial actual no es inteligencia en el sentido que los seres humanos otorgamos a esa palabra"*[15]. Su evolución, desde la IA simbólica[16], que se basaba en reglas predefinidas ejecutadas por una máquina, a la IA que se basa en el aprendizaje

---

[13] En este sentido se indica la necesidad de distinguir *"entre cantidad y calidad de los datos a fin de facilitar la utilización eficaz de los macrodatos (algoritmos y otras herramientas analíticas)"* porque, tanto los datos como los procedimientos de baja calidad *"podrían dar lugar a algoritmos sesgados, correlaciones falsas, errores, una subestimación de las repercusiones éticas, sociales y legales, el riesgo de utilización de los datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos, lo que puede traducirse en procedimientos deficientes de toma de decisiones con repercusiones negativas en las vidas y oportunidades de los ciudadanos, en particular los grupos marginalizados"* (Considerando N).

[14] Meseguer González, P. y López De Mántaras Badia, R. (2017). *Inteligencia artificial,* Madrid, Editorial CSIC Consejo Superior de Investigaciones Científicas, p. 7.

[15] Zlotnik, A. (2019). "Inteligencia Artificial en las Administraciones Públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación", *Boletic*, núm. 84, julio, p. 26.

[16] La IA simbólica "opera con representaciones abstractas del mundo real que se modelan mediante lenguajes de representación basados principalmente en la lógica matemática y sus extensiones", Meseguer González, P. y López De Mántaras Badia, R., *Inteligencia artificial*, ob. cit., p. 11.

automático, ha tenido como consecuencia el incremento de su número de aplicaciones y de su capacidad para resolver problemas. Estas técnicas de IA parten de un conjunto de variables de entrada y salida y la relación entre estas variables "*se establece mediante un proceso de "entrenamiento" o "aprendizaje" realizado por algoritmos, generalmente guiados por grandes cantidades de datos*"[17]. La capacidad de emular en máquinas la capacidad de aprender se denomina *Machine Learning* (ML) o aprendizaje automático y esta área de estudio puede ser definida como "*el conjunto de algoritmos*[18] *que son capaces de aprender a partir de conjuntos de datos*"[19]. Por lo tanto, se trata de sistemas que aprenden de forma autónoma a partir de los datos que se les aportan. Dentro del ML se distinguen los métodos que emplean aprendizaje guiado o supervisado, entrenados "*con conjuntos de datos y salida previamente etiquetados*"[20], de aquellos otros no supervisados en los que los datos no son previamente etiquetados y el algoritmo agrupa los datos en función de las características semejantes que presenten tratando "*de descubrir patrones y correlaciones presentes en el conjunto de datos*"[21]. También existen métodos de aprendizaje semi-supervisado, cuando sólo una parte de los datos de entrenamiento están etiquetados, y aprendizaje reforzado, "*en el que el sistema es un simulador o "agente" y aprende en base a ensayo-error*"[22]. A través del uso de las diferentes técnicas aplicadas a los conjuntos de datos se pretende obtener un nuevo conocimiento y a este "*proceso global de*

---

[17] Zlotnik, A. "Inteligencia Artificial en las Administraciones Públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación", ob. cit., p. 26.

[18] Un algoritmo es una fórmula o conjunto de reglas (o procedimiento, procesos, instrucciones o pasos) para resolver un problema o realizar una tarea. En Inteligencia Artificial, el algoritmo indica a la máquina cómo encontrar respuestas a una pregunta o soluciones a un problema. En el aprendizaje automático, los sistemas utilizan muchos tipos diferentes de algoritmos. Algunos ejemplos comunes son los árboles de decisión, los algoritmos de agrupación, los algoritmos de clasificación o los algoritmos de regresión. Es decir, se trata de conjuntos finitos y ordenados de pasos, dirigidos a resolver un problema o a tomar una decisión. En AA. VV. (2022). *Glossary of human-centric artificial intelligence*, EUR 31113, Publications Office of the European Union, Luxembourg, p. 10.

[19] González Cabanes, F. y Díaz Díaz, N. (2023). "¿Qué es la Inteligencia Artificial?", Gamaero Cadasado, E. y Pérez Guerrero, F. L., *Inteligencia Artificial y sector público*, Tirant lo Blanch, Valencia, p. 40.

[20] Palma Ortigosa, A. (2022). "El ciclo de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", Cotino Hueso, L. (dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor, p. 33.

[21] Ibidem.

[22] González Cabanes, F. y Díaz Díaz, N. "¿Qué es la Inteligencia Artificial?", ob. cit., p. 49.

búsqueda de nuevo conocimiento a partir de un conjunto de datos se denomina KDD (*Knowledge Discovery in Data bases*)"[23].

Son varias y diferentes las tecnologías de IA y, en el ámbito de los textos deontológicos y legales, no se maneja una única definición. En el art. 3.1 del recientemente aprobado Reglamento sobre Inteligencia Artificial[24] (RIA), se define al sistema de IA como aquel "*sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales*". La IA incluye un variado conjunto de técnicas que tienen capacidad para generar determinados resultados como contenidos, recomendaciones, clasificaciones o decisiones que influyen en los entornos en los que interactúan, pero también pueden utilizarse para realizar predicciones sobre eventos futuros[25]. Respecto de su funcionamiento y capacidades, destaca que suelen funcionar mediante la detección de patrones en grandes conjuntos de datos, ofrecen la posibilidad de mejorar el rendimiento de los servicios (sobre todo gracias a una mayor precisión, orientación y coherencia), aportando nuevas soluciones y mejorando la eficiencia y eficacia de las tareas y el rendimiento del sistema[26].

Estas tecnologías se aplican en muchos ámbitos y sectores para decidir o ayudar en la adopción de decisiones que pueden afectar a los derechos de las personas, a su acceso a bienes o servicios, prestaciones o empleos, en el ámbito financiero y de los seguros, al diagnóstico médico, etc. Por ello, la existencia de sesgos en esos procesos tecnológicos pueden tener efectos graves y perjudiciales para las personas, con independencia de que exista o no una intencionalidad discriminatoria. La referencia a los sesgos en los sistemas de IA se suele emplear en

---

[23] Ibidem, p. 47.

[24] Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión.

[25] NIST (National Institute of Standars and Technology. U. S. Departament of Commerce). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, p. 3/77. https://doi.org/10.6028/NIST.SP.1270

[26] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, p. 5.

un sentido negativo, que es la que recoge la RAE al definirlo en el ámbito de la estadística como el "*error sistemático en el que se puede incurrir cuando al hacer muestreos o ensayos se seleccionan o favorecen unas respuestas frente a otras*". El sesgo es definido también como una anomalía en el resultado de los sistemas de IA, debida a los prejuicios y/o suposiciones erróneas realizadas durante el proceso de desarrollo del sistema o a prejuicios en los datos de entrenamiento, por lo que los resultados del sistema de IA no pueden generalizarse ampliamente[27]. La IA tiene una amplia capacidad para para reproducir y reforzar los sesgos, "*puede exacerbar las formas ya existentes de discriminación, los prejuicios y los estereotipos*"[28]. En consecuencia, resulta importante "*controlar las fases en las que surgen los sesgos, que después se replicarán y acabarán arrojando un resultado discriminatorio*"[29] para determinados colectivos o personas. A ese resultado discriminatorio que se produce a través de sistemas automatizados y que contribuye a un trato diferente injustificado o que desfavorece a las personas en función de determinadas "*circunstancias específicas especialmente sospechosas de discriminación*"[30] es a lo que se denomina "discriminación algorítmica".

Existe una gran variedad de sesgos en la IA ya que se desarrolla en un contexto social y cultural determinado, que la condiciona. Por ello, "*la existencia de un sistema de discriminación estructural es una premisa clave*"[31] para comprender la discriminación algorítmica por lo que se requiere, "*no solo el análisis de los productos de software, sino también de las ideologías sociales y las prescripciones normativas de la sociedad que utiliza dichos sistemas*"[32]. En este sentido, la UNESCO ha

---

[27] AA. VV.: *Glossary of human-centric artificial intelligence*, ob. cit., p. 20.

[28] Recomendación sobre Ética de la Inteligencia Artificial de la UNESCO, adoptada el 23 de noviembre de 2021, p. 10.

[29] Belloso Martín, N. (2022). "La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un Derecho a la protección contra los sesgos?", Llano Alonso, F. H. (dir.), *Inteligencia Artificial y Filosofía del Derecho,* Editorial Laborun, Murcia, p. 48.

[30] Cotino Hueso, L. "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", Gamaero Cadasado, E. y Pérez Guerrero, F. L., *Inteligencia Artificial y sector público*, ob. cit., p. 260.

[31] Soriano Arnaz, A. "Discriminación algorítmica: garantías y protección jurídica", Cotino Hueso, L. (dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas,* ob. cit., p. 140.

[32] Jaume-Palasí, L. "Justicia: inteligencia artificial y discriminación - una arqueología", Reche Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*, ob. cit., p. 72.

afirmado que la IA corre el riesgo de reproducir estructuras sociales discriminatorias si quienes la desarrollan e implantan no se cuestionan críticamente las prácticas actuales. También en el ámbito del Consejo de Europa se pone énfasis en el carácter humano de los sistemas automatizados de toma de decisiones, siendo las personas que los diseñan o intervienen en su funcionamiento *"los responsables en última instancia de cómo un sistema recibe sus entradas (por ejemplo, quién recoge los datos que se alimentan a un sistema), cómo se utiliza y cómo se interpretan sus resultados y se actúa en consecuencia"*[33]. Por lo tanto, como respecto de cualquier otro producto humano, se debe exigir un correcto funcionamiento y la ausencia de errores y sesgos, intencionados o involuntarios y, *"en cualquier caso, no se puede atribuir a la IA sin más "se equivoca" y que, por ello, produce los denominados "sesgos algorítmicos""*[34]. El sesgo sistemático puede surgir como fruto de los datos utilizados para entrenar los sistemas, pero también como resultado de los valores que poseen los desarrolladores y usuarios finales de los mismos y, si bien, se produce con más frecuencia cuando las aplicaciones de aprendizaje automático se entrenan con datos que sólo reflejan ciertos grupos demográficos o que reflejan prejuicios sociales, también se ocasionan por errores y sesgos sociales no intencionados pero que después han sido reproducidos o reforzados automáticamente por los sistemas de IA[35]. Este resultado se origina cuando se utilizan alguno de los rasgos sospechosos o variables que pueden correlacionarse en mayor medida con alguno de los grupos tradicionalmente discriminados (*proxies*)[36]; pero también porque "muchas de las características seleccionadas para entrenar el sistema "*tienden a mimetizar o reproducir la forma en la que funcionan de hecho las sociedades y las estructuras que sitúan al as personas y los grupos en posiciones y estatus desiguales, asumiendo como criterios neutrales aquellos que en realidad, constituyen un reflejo*

---

[33] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on *the protection of individuals with regard to automatic processing of personal data in the context of profiling*, apartado 2.4, p. 4.

[34] Belloso Martín, N. *La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un Derecho a la protección contra los sesgos?,* ob. cit., p. 49.

[35] STOA (Panel for the Future of Science and Technology): *The ethics of artificial intelligence: Issues and initiatives*, European Parliamentary Research Service Scientific Foresight Unit (STOA), PE 634.452, March 2020, p. 15.

[36] Barocas, S. y Selbst, A. D. (2016). *Big Data's Disparate Impact,* California Law Review, Vol. 104, p. 691.

de estas posiciones de desigualdad, de subordinación y desventaja"[37]. Por lo tanto, pueden deberse a diversos factores: a que se hayan utilizados conjuntos de datos incorrectamente seleccionados, no representativos o insuficientes, por un incorrecto diseño del programa o "*porque la interpretación de los resultados ha sido equivocada*"[38]. Es importante insistir en la idea de que el problema de los sesgos no proviene exclusivamente de los datos de entrenamiento del sistema, sino que es igualmente relevante la elección de las características que se van a seleccionar durante su diseño y el valor o puntuación que se le otorgue a los datos o a las características seleccionadas, pues, tales opciones, pueden tener un impacto adverso mayor o menor en los grupos de personas tradicionalmente discriminadas[39].

En ocasiones el sesgo no está en el sistema propiamente dicho, sino que puede deberse a la forma en la que se interpreta la información de salida que facilita el sistema de IA, es el denominado sesgo de automatización o confirmación. Ello se debe al exceso de confianza en la IA ante la creencia de que nos encontramos ante algoritmos matemáticos abstractos, que pueden revelar verdades puras objetivas y universales[40]; pero, también porque quien interprete los datos de salida identifique *probabilidad* con *causalidad*[41], otorgándole a esa predicción un valor absoluto. En su *Special Publication* 1270, el NIST señala como las personas y equipos que diseñan y desarrollan los sistemas de IA incorporan al proceso sus propios prejuicios cognitivos, tanto individuales como de grupo, y estos prejuicios prevalecen en las suposiciones sobre qué datos deben utilizarse, qué modelos de IA deben desarrollarse, dónde debe ubicarse el sistema de IA o si la IA es necesaria en absoluto[42]. Por lo tanto, la causa de los sesgos y la discriminación *"puede ser el erróneo diseño y elección de algoritmos, del peso que atribuyen a unos u otros factores*

---

[37] Añón Roig, M. J. (2022). "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", *Derechos y Libertades*, núm. 47, época II, junio, 34.

[38] Belloso Martín, N. *La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un Derecho a la protección contra los sesgos?,* ob. cit., 48.

[39] Barocas, S. y Selbst, A. D. *Big Data's Disparate Impact,* ob. cit., p. 680.

[40] UNESCO (2020). *Artificial Intelligence and Gender Equality*, p. 9. Asimismo, Boyd, D. y Crawford, K. (2012). "Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon", *Information, Communication & Society*, Vol. 15, núm. 5, junio, en especial pp. 662-663.

[41] En el mismo sentido, Cotino Hueso, L., *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público*, ob. cit., p. 270.

[42] *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, ob. cit., p. 6.

o a los errores en el desarrollo de los sistemas de aprendizaje automático"[43]. Otro factor importante en el reforzamiento de los prejuicios sociales, que se incorporara a los sistemas que se basas en modelos estadísticos, son los derivados de los bucles de retroalimentación que mantienen, replican y refuerzan sesgos, errores y suposiciones preexistentes[44].

El NIST distingue tres categorías principales de sesgo: sistémico, estadístico y humano[45]. La primera de estas categorías se denomina también sesgo *histórico o institucional* y es resultado de procedimientos y prácticas institucionales concretas y que, aunque no tienen que ser resultado de un prejuicio o discriminación consciente, tienen como consecuencia que determinados grupos sociales se vean favorecidos o perjudicados. Los más comunes son el racismo y el sexismo y pueden estar presentes en los conjuntos de datos utilizados en la IA, en las normas prácticas y procesos institucionales a lo largo del ciclo de la vida del sistema y en la cultura y en la sociedad en general[46]. Los sesgos *estadísticos y computacionales* se producen cuando se utilizan muestras que no son representativas de la población[47]; por ejemplo, cuando los miembros de grupos vulnerables se encuentren supra o infra-representados[48]. Están presentes en los conjuntos de datos y en los procesos algorítmicos utilizados en el desarrollo de las aplicaciones de IA. Finalmente, los sesgos *humanos* reflejan los errores sistemáticos en el pensamiento humano. Se trata de sesgos con frecuencia implícitos y que tienen que ver con la forma en la que las personas percibimos la información para tomar una decisión o para completar la información que falta o que se desconoce[49].

Con independencia de cuál sea la clase o el origen de los sesgos, el actual grado de infiltración de las decisiones tecnológicas de variada intensidad, que se

---

[43] Cotino Hueso, L. *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público*, ob. cit., pp. 270-271.

[44] *Vid*. Recommendation CM/Rec(2020)1, cit.

[45] Ibidem, p. ii. En el mismo sentido, Cotino Hueso, L., *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público,* ob. cit., pp. 261-262.

[46] NIST: *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, ob. cit., p. 6.

[47] Cotino Hueso, L. *Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público,* ob. cit., p. 261.

[48] Soriano Arnaz, A. *Discriminación algorítmica: garantías y protección jurídica,* ob. cit., p. 140.

[49] NIST. *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* ob. cit., p. 9.

manifiesta la gran cantidad de sectores, públicos y privados de todos los ámbitos (económicos, sociales, científicos, de servicios, etc.) en los que se emplean y en el elevado número de personas afectadas, determina que el número de errores (en forma de falsos positivos y falsos negativos) y sesgos intrínsecos, producirá un impacto considerable en los derechos fundamentales y en particular en el derecho a la igualdad de trato y a no ser discriminado, si no se adoptan las medidas y garantías adecuadas para evitarlo. Las dificultades para enfrentar la discriminación algorítmica derivan de sus tres características definitorias: su invisibilidad, su intensidad y su complejidad técnica[50]. Este último aspecto, la complejidad y opacidad de los sistemas implicará obstáculos para su comprensión por la sociedad, pero también su validación independiente para auditar su seguridad.

Por otra parte, en este ámbito la noción de impacto es fundamental y es diferente de la tasa de error, que aún respecto de aquellas herramientas más afinadas y con tasas bajas, puede suponer una afectación relevante en la vida y en los derechos de las personas perjudicadas. La valoración del impacto tiene que ver con el número real de personas concernidas y también con el contexto y el daño efectivo que se ocasiona en los derechos fundamentales afectados[51], en ocasiones con consecuencias difícilmente reparables. Esta evidencia requiere que el Ordenamiento jurídico proporcione una respuesta adecuada a la altura del problema. Existe un amplio conjunto normativo con el que se debe hacer frente a estos riesgos, desde el conjunto de normas que forman el Derecho antidiscriminatorio, la legislación sobre protección de datos personales y las normas reguladoras de la IA, en especial, el Reglamento de Inteligencia Artificial. Desde su primera versión se han recogido las preocupaciones derivadas de las posibilidades de discriminación

---

[50] Sáenz Lara, C. (2020). "El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 155, p. 45.

[51] Sirva de ejemplo de daño en un derecho fundamental concreto el examen que realiza el Tribunal Supremo en su sentencia 1307/2022 de 14 octubre, en la que reprocha que *"el mero análisis estadístico o algorítmico sobre medias del sector, no sometido a contraste y no explicado por la Agencia promotora, sea suficiente para justificar una entrada en el domicilio constitucionalmente protegido de un contribuyente". (...) Con mayor razón es esto así cuando el origen y naturaleza de las ratios y fuentes estadísticas empleadas no se conoce, no es homogénea y no ha podido ser sometida a debate o controversia por el titular del domicilio y no ha sido objeto de un razonamiento judicial propio que no se limitase al asentimiento acrítico a lo que la Administración -a quien no se puede negar la condición de parte interesada en la obtención del auto- propone* (basándose en) *"la observancia de medias aritméticas o a algoritmos de ignoto origen"*.

a través de sistemas de IA. En su redacción final, recuerda la importancia de los principios de diversidad, no discriminación y equidad, que implica que los sistemas de IA se desarrollarán y utilizarán *"de manera que incluyan a diversos actores y promuevan la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los impactos discriminatorios y los sesgos injustos prohibidos por el Derecho de la Unión o nacional"* (Considerando 14).

3. EL PRINCIPIO DE IGUALDAD ANTE LA DISCRIMINACIÓN ALGORÍTMICA

La utilización de la IA puede dar lugar a decisiones injustas por error o porque se utilice para adoptar decisiones que pueden producir discriminaciones, aunque un error algorítmico no habrá de implicar necesariamente un resultado discriminatorio. Han sido ampliamente tratadas las dificultades de la aplicación del Derecho antidiscriminatorio a las decisiones de los sistemas algorítmicos, por el difícil encaje en los conceptos de discriminación directa o indirecta[52] y, en especial, por la problemática que plantean, tanto la complejidad de los sistemas, como su opacidad. Los propios rasgos de la discriminación algorítmica derivados de su presunta *"objetividad (y autoridad matemática) y el ahorro de costes y tiempo en el ámbito de cualquier decisión (...), conllevarán problemas de prueba, tanto bajo del test de la discriminación directa como indirecta"*[53]. En todo caso, que las decisiones algorítmicas están sometidas la mandato constitucional de igualdad de trato está fuera de toda duda y, específicamente, a la Ley 15/2022, integral para

---

[52] Vantin, S. (2021). "Inteligencia artificial y derecho antidiscriminatorio", Llano Alonso, F. H. y Garrido Martín, J. *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital*, Aranzadi, 2021, pp. 367-384; Soriano Arnaz, A.: *"Discriminación algorítmica: garantías y protección jurídica",* ob. cit.; Añón Roig, M. J. "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", ob. cit.

[53] Sáenz Lara, C. *El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación*, p. 48. Pese a estas dificultades existen ejemplos de la aplicación exitosa del Derecho antidiscriminatorio, como la sentencia de 31 de diciembre de 2020, del Tribunal Ordinario de Bolonia, que consideró que se producía una discriminación indirecta por *Deliveroo* en relación con las condiciones de acceso a la reserva de sesiones de trabajo a través de la plataforma, *"en la medida en que el algoritmo no elimina la puntuación negativa de los riders que se ausentan en circunstancias de enfermedad o huelga vulnera sus derechos como trabajadores"*; Castillo Parrilla, J. A. (2020). "Sentencia del Tribunal Ordinario de Bolonia de 31 de diciembre de 2020 (Caso Deliveroo) ¿Discriminación algorítmica o discriminación a través de un algoritmo?", *Derecho Digital e Innovación*, núm. 7, octubre, p. 5.

la igualdad de trato y la no discriminación, que incluye en su ámbito objetivo de aplicación la Inteligencia Artificial y la gestión masiva de datos, así como otras esferas de análoga significación (art. 3.1); si bien se ha señalado su alcance limitado, ya que en principio "*esta ley sólo sería aplicable para los supuestos de discriminación y sesgos algorítmicos vinculados con las categorías especialmente sospechosas de discriminación*"[54].

La igualdad es un valor fundamental intensamente ligado a la dignidad y dirigido al desarrollo ético y social de las comunidades humanas. Reiteradamente, nuestro TC ha venido entendiendo que, cuando la CE dispone que todos los españoles son iguales ante la Ley establece un derecho subjetivo a obtener un trato igual imponiendo a los poderes públicos la obligación de llevar a cabo ese trato igual y, al mismo tiempo, limita el poder de los órganos legislativos y de aquellos encargados de la aplicación de las normas, exigiendo *"que los supuestos de hecho iguales sean tratados idénticamente en sus consecuencias jurídicas y que, para introducir diferencias entre ellos, tenga que existir una suficiente justificación de tal diferencia, que aparezca al mismo tiempo como fundada y razonable, de acuerdo con criterios y juicios de valor generalmente aceptados, y cuyas consecuencias no resulten, en todo caso, desproporcionadas"*[55]. Por tanto, la *"esencia del derecho a la igualdad comporta que sólo aquella desigualdad que introduce una diferencia de trato entre situaciones que pueden considerarse iguales y que además carece de una justificación objetiva y razonable vulnera el referido derecho"*[56]. Solamente se prohíbe la discriminación o desigualdad de tratamiento legal injustificada por no ser razonable. Es decir, la igualdad no es una igualdad absoluta entre todos y en todo, sino que admite la diferenciación de trato cuando esta no sea arbitraria por estar razonablemente justificada y, en consecuencia, *"están prohibidas aquellas desigualdades de trato que resulten artificiosas o injustificadas por no venir fundadas en criterios objetivos suficientemente razonables de acuerdo con criterios o juicios de valor generalmente aceptados"*[57]. Precisamente será este test de la razonabilidad el que nos posibilitará la distinción entre una norma que contiene una discriminación

---

[54] Cotino Hueso, L. (2023). "Los usos de la inteligencia artificial en el sector público, su variable impacto y categorización jurídica", *Revista Canaria de Administración Pública*, núm. 1, p. 236.
[55] STC 91/2019, de 3 de julio. En el mismo sentido, entre otras, STC 74/2020, de 29 junio.
[56] STC 74/2020, de 29 junio.
[57] Ibidem.

prohibida y una "acción positiva", que es una medida permitida y querida por el Ordenamiento jurídico para conseguir una mayor igualdad material[58].

Además de un mandato de igualdad, la CE contiene una expresa prohibición de la discriminación de las personas[59] estableciendo en su art. 14 un específico listado de razones de interdicción de la discriminación, las más frecuentes desde un punto de vista histórico, muchas de ellas estructurales[60]. Cuando se introduzca una diferencia basada en alguno de los supuestos especialmente sospechosos, se exigirá con mayor rigor la prueba de su objetividad y racionalidad y, en consecuencia, las prohibiciones explícitas de discriminación sólo podrán ser utilizadas excepcionalmente como criterio de diferenciación jurídica, debiéndose acreditar que no encubre una conducta lesiva a los derechos fundamentales, contraria a la prohibición de discriminación[61]. Las categorías sospechosas del art. 14 han sido ampliadas en la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que según explica en su Preámbulo, "*viene a dar cobertura a las discriminaciones que existen y a las que están por venir, ya que los desafíos de la igualdad cambian con la sociedad y, en consecuencia, también deberán hacerlo en el futuro las respuestas debidas*". Esta Ley, que completa el extenso acervo jurídico antidiscriminatorio de nuestro país, dispone en su art. 2.1 que "*nadie podrá ser discriminado por razón de nacimiento, origen racial o étnico, sexo, religión, convicción u opinión, edad, discapacidad, orientación o identidad sexual, expresión de género, enfermedad o condición de salud, estado serológico y/o predisposición genética a sufrir patologías y trastornos, lengua, situación socioeconómica, o cualquier otra condición o circunstancia personal o social*".

En el art. 6 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación se definen, además de los tradicionales conceptos de discriminación directa e indirecta, la discriminación por asociación, por error y la

---

58 Carmona Cuenca, E. (1994). "El principio de igualdad material en la Jurisprudencia del Tribunal Constitucional", *Revista de Estudios Políticos* (Nueva Época), núm. 84, abril-junio. Asimismo, Gluk. G. (2022). "Igualdad y no discriminación de las personas mayores", *Teoría y derecho: revista de pensamiento jurídico,* núm. 33, p. 68.

59 Así lo ha entendido el TC desde sus primeras sentencias, entre otras STC 75/1983, de 3 de agosto; 28/1987, de 16 de julio; 166/1988, de 26 de septiembre, 233/2007, de 5 noviembre o 1/2021, de 25 enero.

60 STC 91/2019, de 3 de julio y 71/2020, de 29 de junio.

61 Por todas, STC 233/2007 de 5 noviembre.

múltiple e interseccional, tratando de *"reunir todas las manifestaciones, que a la vista de la experiencia real y judicial, podrían revestir la discriminación"* [62] en la actualidad. De forma concordante con otras normas antidiscriminatorias, define la discriminación directa como aquella situación en que se encuentra una persona o grupo en que se integra que sea, haya sido o pudiera ser tratada de manera menos favorable que otras en situación análoga o comparable por las razones sospechosas incluidas en el art. 2.1. En el ámbito de la IA, esta discriminación se produciría cuando en el proceso automatizado de decisión se haya tenido en cuenta en alguna fase del proceso una categoría sospechosa *"como factor de entrada negativo en la decisión que se adopte"* [63]. Cuando exista sospecha de discriminación directa, corresponderá a quien adopte la medida lesiva, acreditar que esta obedece a motivos razonable, ajenos a cualquier propósito discriminatorio y, en el ámbito de la discriminación algorítmica, deberá justificarse que la inclusión de ese factor en el sistema de IA es necesaria, objetiva, razonable y proporcionada.

La discriminación indirecta se producirá, *"cuando una disposición, criterio o práctica aparentemente neutros ocasiona o puede ocasionar a una o varias personas una desventaja particular con respecto a otras por razón de las causas anteriores"*. Ante una medida que pudiera ser calificada como discriminación indirecta, lo que deberán compararse para determinar su existencia, *"no son los individuos, sino grupos sociales en los que se ponderan estadísticamente sus diversos componentes individuales; es decir, grupos entre los que alguno de ellos está formado mayoritariamente por personas pertenecientes a una de esas categorías especialmente protegidas"* [64]. Se ha señalado que la disposición, criterio o práctica aparentemente neutros

---

[62] García Murcia, J. (2022). "La ley 15/2022 Integral para la igualdad de trato y no discriminación", *Foro*, Nueva Época, Vol. 25, núm. 2, p. 16.

[63] Soriano Arnanz, A. (2022). "Discriminación algorítmica: garantías y protección jurídica", Cotino Hueso, L. (dir.): *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas,* Aranzadi, p. 149.

[64] STC 3/2007, de 15 de enero. En el mismo sentido SSTC 91/2019, de 3 de julio y 79/2020, de 2 julio. Así lo ha entendido también el Tribunal de Justicia de la Unión Europea (TJUE) de 9 de febrero de 1999 (C-167/1997, asunto Seymour-Smith y Laura Pérez) indicando que debe procederse a un análisis estadístico para valorar el porcentaje de trabajadores de uno y otro sexo, afectados por la medida controvertida y si los datos estadísticos disponibles muestran que un porcentaje considerablemente mayor de trabajadores femeninos que de trabajadores masculinos son afectados negativamente por esa norma, resultaría de tal situación *"una apariencia de discriminación basada en el sexo, a menos que la norma controvertida estuviera justificada por factores objetivos y ajenos a toda discriminación por razón de sexo"*.

podría constituirlo aquella *"variable específica introducida en el sistema que, por el valor que le otorga este, genera un resultado discriminatorio para el grupo desaventajado"*[65]. A medio camino entre las discriminaciones directas e indirecta estarían las discriminaciones por inferencia derivadas del uso de *proxies,* que son datos aparentemente neutros, *"pero de los que el sistema de IA acaba derivando un tratamiento perjudicial para colectivos especialmente discriminados"*[66]. Por ejemplo, los datos demográficos, que pueden relacionarse, entre otros, con el origen racial, étnico o de la confesión religiosa en determinadas circunstancias.

En el art. 6 también se recoge la discriminación por asociación, que "*se produce cuando una persona o grupo en que se integra, debido a su relación con otra sobre la que concurra alguna de las causas prohibidas, es objeto de un trato discriminatorio"*[67]. Cuando la discriminación se funda en una apreciación incorrecta acerca de las características de la persona o personas discriminadas, estaríamos ante una discriminación por error y, finalmente, habría discriminación múltiple cuando una persona es discriminada de manera simultánea o consecutiva por dos o más causas de las previstas en esta ley e "*interseccional cuando concurren o interactúan diversas causas de las previstas en esta ley, generando una forma específica de discriminación"*[68]. En el ámbito de la discriminación algorítmica esta última categoría podrá dar respuesta al alto *"nivel de granularidad con el que los sistemas algorítmicos analizan a las personas"*[69] aumentando las posibilidades de que tengan lugar varios supuestos de discriminación.

---

[65] Soriano Arnanz, A. (2021). "La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial", Bonorino Ramírez, R. (dir.).: *Nuevas normatividades: inteligencia Artificial, Derecho y Género*, Aranzadi, p. 76.

[66] Cotino Hueso, L.: *"Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público"*, ob. cit., p. 288.

[67] Así, entre otras, STC 71/2022, de 29 de junio (discriminación por razón de sexo por asociación), y la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 22 de marzo de 2016, asunto Guberina contra Croacia (discriminación por razón de discapacidad por asociación).

[68] *Vid*. Barrere Unzueta, M. A. y Morondo Taramundi, D. (2011). "Subordiscriminación y discriminación interseccional: elementos para una teoría del derecho antidiscriminatorio", *Anales de la Cátedra Francisco Suárez,* núm. 45; y Rey Martínez, F.: "La discriminación múltiple, una realidad antigua, un concepto nuevo", *Revista Española de Derecho Constitucional*, núm. 84.

[69] Soriano Arnanz, A. "La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial", ob. cit., p. 79.

En la medida en que se considera que, en la mayoría de los casos, la discriminación algorítmica es *"una propiedad emergente no intencional"*[70] de la IA, suele reconducirse tradicionalmente a la discriminación indirecta. Sin embargo, coincido con Cotino Hueso en que la mayor parte de las discriminaciones algorítmicas serán discriminación por error[71] en las que se produzcan apreciaciones incorrectas de la persona o personas discriminadas y, en consecuencia a la decisión automatizada no le se aplicará el test de la igualdad, *"sino que el análisis jurídico se centrará en probar la existencia del sesgo o discriminación, determinar si es relevante y qué consecuencias tienen y si se han cumplido las medidas preventivas para evitarlo"*[72].

En este sentido, en el art. 23 de la Ley 15/2022, se prevén determinadas obligaciones para los sistemas de IA involucrados en los procesos de toma de decisiones. Se trata de prevenir las decisiones automatizadas discriminatorias derivadas de los sesgos algorítmicos, en particular en el ámbito de las administraciones públicas. Para ello, se establece que, en el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas "*favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente"*. Estas referencias junto con las que se prevén en su apartado tercero de promover el uso de una IA ética, confiable y respetuosa con los derechos fundamentales, implicará la necesidad de incorporar determinadas medidas preventivas y garantías concretas durante el desarrollo y todo el ciclo de vida del sistema para minimizar el riesgo de discriminación en la decisión y en el uso de los datos y los procesos, para lo que habrán de *"procurarse unas condiciones de transparencia, auditabilidad, aplicabilidad, trazabilidad, supervisión humana y gobernanza, siendo la información facilitada accesible y comprensible"*[73].

---

[70] Añón Roig, M. J. "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", ob. cit., p. 38.

[71] Cotino Hueso, L. "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", ob. cit., p. 286.

[72] Ibidem.

[73] Ester Sánchez, A. T. (2023). "El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales", *Cuadernos Electrónicos de Filosofía del Derecho*, núm. 48, p. 126

Debe señalarse que este precepto no establece obligaciones concretas[74], sino que se limita a indicar que las administraciones públicas favorecerán que se incorporen esos criterios siempre que sea factible técnicamente. Dichos mecanismos se incluirán en el diseño del algoritmo y se aplicarán a los datos de entrenamiento, abordando su potencial impacto discriminatorio, *"para lo que se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio"*. En el segundo apartado del art. 23 se establece que, en su ámbito de competencia, las administraciones públicas priorizarán para los algoritmos involucrados en procesos de toma de decisiones, *la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos*. Por último y en este caso, tanto para el sector público como para el privado, se establece la promoción del *"uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido"*. Este conjunto de previsiones responde también a las dificultades de prueba de la existencia de sesgos y resultados discriminatorios en cualquiera de sus clases si no se garantiza suficientemente el acceso a la información relevante, que permita su auditoría independiente.

Puede afirmarse que esta norma, pionera en nuestro país, aporta algunos elementos innovadores para hacer frente a las situaciones de discriminación algorítmica, como la implementación de medidas para la prevención y eliminación de sesgos, que garanticen la transparencia y la rendición de cuentas. En contra, se debe indicar que se ha desaprovechado la oportunidad de establecer con mayor rotundidad los requisitos que necesariamente deberán cumplir algoritmos y sistemas de IA para garantizar los objetivos de la ley; pues resulta obvio reconocer que el conjunto de estos no se configuran como deberes imperativos sino *"tan solo a un desiderátum o buenas prácticas desprovistas de fuerza vinculante, lo que indudablemente merma la efectividad de la tutela antidiscriminatoria integral pretendida por la Ley"*[75]. En todo caso, pese a que desde este punto de vista su redacción es mejorable, coincido en que es un paso loable que ilustra la preocupación que suscita la discriminación algorítmica y el *"interés del legislador por abordar de*

---

[74] González De Patto, R. Mª. (2023). "Inteligencia artificial y empleo. Análisis crítico del marco regulatorio europeo y español impulsado por el Pilar Europeo de Derechos Sociales", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 168, p. 387.

[75] Ibidem, p. 388.

manera tangible toda esa problemática"[76]. No obstante, se ha desaprovechado la oportunidad de establecer *"la necesaria trazabilidad de los algoritmos o decisiones automatizadas, y a la también necesaria supervisión humana de dichas decisiones o el derecho a impugnar las decisiones adoptadas"*[77]. Es por ello, que si bien completa las exigencias de transparencia previstas en el RGPD, coincido con Mónica Arenas en que no se aportan novedades significativas que no se pudieran solventar con la normativa vigente de protección de datos personales[78].

4. LA PROTECCIÓN DE LOS DATOS PERSONALES Y LA DISCRIMINACIÓN ALGORÍTMICA

Las posibilidades de discriminación de las personas como consecuencia del tratamiento automatizado de sus datos personales ha sido una preocupación clásica, en especial cuando se perfila a los individuos o se adoptan decisiones automatizadas, ya sea por los propios datos que son objeto de tratamiento o como consecuencia del propio tratamiento, que permite inferir determinadas características, algunas de ellas sensibles. Es importante señalar que, tanto los datos iniciales, como los datos inferidos son datos personales en el sentido del RGPD siempre que se refieran a una persona física identificada o identificable. Para una correcta comprensión de la relación entre protección de datos personales y discriminación algorítmica, habremos de partir de su definición constitucional. El derecho a la protección de datos, en palabras del TC, persigue garantizar a la *"persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado"*[79]. Los datos amparados son todos aquellos que identifiquen o permitan la identificación de una persona, pues cualquiera de estos datos puede *"servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier índole, o (...) para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"*[80], cuyo uso podrá tener

---

[76] García Quiñones, J. C. (2023). "Inteligencia artificial y relaciones laborales: entre la significación creciente de los algoritmos y el desmentido de su neutralidad aparente", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 167, p. 80.

[77] Arenas Ramiro, M. "La igualdad a la luz de los derechos digitales", Reche Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías,* ob. cit., p. 133.

[78] Ibidem.

[79] STC 292/2000, de 30 de noviembre.

[80] Ibidem.

como consecuencia su discriminación. A través de la conexión de un gran número de datos individuales, incluso anónimos, la técnica de creación de perfiles puede conducir a incluir a las personas en categorías predeterminadas sin que tengan conocimiento de ello. La falta de transparencia en estos procesos y en su posterior aplicación, así como *"la falta de precisión que puede derivarse de la aplicación automática de reglas de inferencia preestablecidas, pueden suponer graves amenazas para los derechos y libertades de las personas"*[81]. Los efectos de estas operaciones serán especialmente graves cuando se realicen correlaciones utilizando datos sensibles, lo que supondrá *"exponer a las personas a riesgos particularmente elevados de discriminación y de atentados contra sus derechos personales y su dignidad"*[82].

Las posibilidades de discriminación algorítmica a través del uso de perfiles y la adopción de decisiones automatizadas, planean sobre la regulación sobre protección de datos personales y este derecho sigue teniendo un importante papel que desempeñar en este ámbito por lo que *"constituye un marco ineludible y el primero llamado a regular la inteligencia artificial"*[83]. Entre las obligaciones derivadas del principio de responsabilidad proactiva, que establece el art. 5.2 del RGPD, se encuentra la de identificar si la discriminación es uno de los riesgos derivados del tratamiento de los datos y, de ser así, se exige la adopción las medidas y garantías adecuadas para minimizarlo[84]. Entre ellas, tienen un lugar destacado las obligaciones de que se incorporen los principios de privacidad por

---

[81] Recomendación (2010)13 sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles del Comité de Ministros del Consejo de Europa de 23 de noviembre de 2010.

[82] Ibidem.

[83] Huergo Lora, A. "Hacia la regulación europea de la Inteligencia artificial", ob. cit., p. 760.

[84] *Vid*. GT29, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679,* en donde se indica que *"los responsables del tratamiento deben llevar a cabo con frecuencia evaluaciones de los conjuntos de datos que tratan para comprobar cualquier desviación, así como desarrollar formas de abordar cualquier elemento lesivo, incluido el exceso de confianza en las correlaciones. Otras medidas útiles son los sistemas que auditan los algoritmos y las revisiones periódicas de la precisión y pertinencia de las decisiones automatizadas, incluida la elaboración de perfiles. Los responsables del tratamiento deben introducir procedimientos y medidas adecuados para evitar errores, imprecisiones o discriminación sobre la base de los datos de categoría especial. Estas medidas deben utilizarse de forma cíclica, no solo en la fase de diseño, sino también de forma continua, ya que la elaboración de perfiles se aplica a personas. El resultado de las pruebas debe repercutir en el diseño del sistema"* (p. 31). *Vid*. Asimismo entre otras directrices, CEPD: *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, p. 19; Agencia Española de Protección de Datos (AEPD): *Adecuación al RGPD*

defecto y desde el diseño y que se realice una evaluación de impacto relativa a la protección de datos (EIPD) cuando se elaboren perfiles o se adopten decisiones automatizadas (art. 35.3.a) del RGPD). La EIPD no solo es obligatoria porque entraña un alto riesgo para los interesados, sino también porque en ella se deberá *"identificar y registrar el grado de participación humana en el proceso de toma de decisiones y en qué punto se produce esta"*[85]. Además de los propios instrumentos jurídicos preventivos y sancionadores previstos en el RGPD y en la Ley Orgánica 3/2018, de Protección de Datos personales y garantías de los derechos digitales, las autoridades de control han venido extrayendo de forma expansiva muchas obligaciones de transparencia, auditoría y sobre *"gobernanza de los datos, calidad y robustez de los sistemas de IA"*[86], idóneas para la evitación de sesgos y discriminación plenamente aplicables a los sistemas de IA.

El derecho a la vida privada del art. 8 del Convenio europeo de derechos humanos[87] (CEDH) fue la vía que utilizó el Tribunal de Distrito de la Haya, en su sentencia de 2 de febrero de 2020, para anular el sistema SyRI. Si bien no se pronunció sobre la aplicación del art. 22 del RGPD, consideró que la realización, utilización y registro de un informe de riesgo de fraude, produce un efecto significativo en la vida privada del interesado. El Tribunal holandés considera que SyRI no cumple los requisitos establecidos en el CEDH, pues no se logra el "justo equilibrio" entre el interés social al que sirve la legislación y la violación de la vida privada a la que da lugar, teniendo en cuenta la importancia que el derecho a la protección de datos personales reviste en un contexto de aplicación de nuevas tecnologías, en particular en el contexto de la elaboración de perfiles de riesgo de fraude en las prestaciones de la seguridad social y en las obligaciones tributarias. En ningún momento se cuestiona la legitimidad del Estado para utilizar el sistema de evaluación de riesgo con la finalidad garantizar el sistema de prestaciones sociales, que considera una medida necesaria en una sociedad democrática para garantizar un importante interés general. Pese a ello, el sistema no supera el test de necesidad y proporcionalidad por varias razones, que expongo sucintamente.

---

de tratamientos que incorporan Inteligencia Artificial. Una introducción, p. 28 y *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*.

85 AEPD. PS 000209/2022, p. 67.

86 Cotino Hueso, L. "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", ob. cit., p. 322.

87 Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950.

El punto de partica del Tribunal es la amplia noción de vida privada que ha venido reconociendo el TEDH. A partir de ahí, considera que la injerencia en este derecho no es proporcionada, entre otras razones, porque no se garantiza adecuadamente el principio de transparencia en su doble significado: el que tiene en el ámbito de la protección de datos personales y el propio del ámbito de la IA, relacionado con los requisitos de explicabilidad. Reprocha al legislador que no se haya establecido un sistema de información o notificación individualizada al interesado, que no conocerá la realización o la presentación de un informe de riesgo, que podría tener un efecto significativo sobre él y que podría conservarse durante dos años. En consecuencia, se ignora su derecho a poder hacer un seguimiento razonable de sus datos personales y a ser informado sobre el tratamiento de los mismos. Asimismo, el Tribunal reprocha la falta de transparencia respecto del propio sistema de predicción de riesgo de fraude. El Estado no proporcionó información relevante sobre el modelo de riesgo: ni sobre los indicadores que lo componen, ni sobre el funcionamiento del modelo de riesgo o la clase de algoritmos utilizados en el modelo. Tampoco facilitó información sobre el método de análisis aplicado por la Inspección de Asuntos Sociales y Empleo o sobre la validación del modelo o la verificación de los indicadores, puesto que tanto el modelo de riesgo como los indicadores de los datos eran secretos. Esta falta de transparencia hace imposible saber cómo se genera el simple árbol de decisión y de qué pasos se compone. La consecuencia para el interesado es la misma que la ausencia de la primera clase de transparencia: no le será posible defenderse del hecho de que se haya presentado un informe de riesgo sobre su persona o incluso, valorar si sus datos han sido tratados legalmente, aunque no hayan dado lugar a un informe de riesgo.

Otro argumento de peso para considerar insuficientemente justificada la injerencia en la vida privada fue la ausencia de revisión y validación del sistema de forma previa por un tercero independiente, así como que no se realizaran evaluaciones de impacto en la protección de datos para cada proyecto SyRI. En esta resolución queda patente la relación que existe entre *"las obligaciones de transparencia, auditabilidad y explicabilidad del algoritmo"* y los derechos de acceso a la información, al debido proceso y a las garantías judiciales o administrativas[88]. Se tuvo muy presente esta relación entre la transparencia y la verificabilidad de

[88] Cotino Hueso, L. (2020). "Holanda: "SyRI, ¿a quién sanciono?". Garantías frente al uso de la inteligencia artificial y decisones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", La Ley privacidad, núm. 4, abril de 2020.

sistema, porque la utilización del modelo de riesgo y el análisis que se lleva a cabo para la elaboración del perfil de riesgo puede tener como consecuencia efectos discriminatorios, involuntarios o no. Pues, como se señala en la resolución, el análisis de grandes conjuntos de datos, con o sin sistemas de aprendizaje profundo, si bien es innegablemente útil, puede arrojar resultados no deseados, incluida la exclusión o discriminación injustificadas ya que, en cualquier sistema algorítmico de perfilado, existen riesgos de efectos discriminatorios de que se atribuyan incorrectamente a las personas ciertas características (falso positivo), o al revés, las características pueden no atribuirse incorrectamente (falso negativo). El potencial discriminador se encuentra no solo en el algoritmo utilizado sino también en la selección de objetivos, que se utilizaba para investigar, en especial, los barrios conocidos como zonas problemáticas con lo que se aumentan las posibilidades de descubrir irregularidades en dichas zonas en comparación con otros barrios. Esto a su vez provoca un efecto de retroalimentación ya que confirma la imagen de un barrio como zona problemática, contribuyendo a la creación de estereotipos y refuerza una imagen negativa de los ocupantes de dichos barrios, incluso, aunque no se hayan generado informes de riesgo sobre ellos y en consecuencia, se incrementan los efectos discriminatorios y estigmatizadores de SyRI.

En el ámbito del RGPD, la discriminación algorítmica se puede prevenir y enfrentar a través de una correcta aplicación de los principios relativos al tratamiento, mediante la prohibición de tratar categorías especiales de datos y, en particular, a través de las disposiciones del art. 22 que regula la elaboración de perfiles y las decisiones automatizadas[89]. Las exigencias derivadas de la aplicación de los principios relativos al tratamiento tienen indecencia directa en la *calidad de los datos* que se utilizarán en determinadas fases del desarrollo o implementación de un sistema de IA. Por su importancia en relación con la ausencia de sesgos

---

[89] Ante la imposibilidad de abordar correctamente la complejidad de las implicaciones de la elaboración de perfiles, de las obligaciones y de los requisitos derivados del principio de responsabilidad proactiva y de transparencia, así como de las disposiciones del art. 22 del RGPD me remito a mis trabajos anteriores, en particular: *"Decisiones automatizadas basadas en algoritmos y protección de datos personales",* Tomás Mallén, B., García Mahamut, R. y Pauner Chulvi, C. (2021), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español*, Tirant lo Blanch, Valencia, pp. 333-359; y "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 38, enero de 2018, pp. 107-139.

en los sistemas algorítmicos de ayuda o de toma de decisión destacan las obligaciones derivadas del principio de exactitud y del principio de transparencia. Como ha señalado el Comité Europeo de Protección de Datos (CEPD), *"numerosos estudios también han puesto de manifiesto que estos resultados estadísticos del procesamiento algorítmico también pueden estar sujetos a sesgos, en particular los derivados de la calidad de los datos de origen, así como de las bases de datos de entrenamiento"*[90]. El principio de exactitud exige los responsables del tratamiento utilicen información exacta y actualizada y esta obligación lo es, tanto para los datos utilizados para crear y entrenar el software, como para los datos utilizados en su despliegue; pues, la calidad y representatividad de los datos, que representen a diferentes grupos y tipos de personas y que se basan en modelos preentrenados a partir de una base de datos preexistente, es un aspecto fundamental que va a tener incidencia directa en las tasa de error de los sistemas y en "*la precisión de su procesamiento"*[91].

Si bien, la tipología de los sesgos es mucho más amplia[92], la correcta aplicación del art. 5 del RGPD minimizará las inexactitudes en los datos, que podrían implicar que la realidad reflejada por el algoritmo difiera significativamente de la del mundo real, por ejemplo, cuando se utilicen conjuntos de datos que no son generalizables para entrenar aplicaciones de aprendizaje automático[93]. Por lo tanto, a fin de evitar inexactitudes en el conjunto de datos utilizado, en las distintas fases de entrenamiento del sistema habrán de emplearse muestras representativas y suficientes[94], lo que hace necesario que los datos no hayan perdido su vigencia por el paso del tiempo, sean plenamente representativos de la población objetivo[95], estén estructurados y *"adecuadamente depurados"*[96].

---

[90] CEPD. *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement,* p. 19.

[91] FRA. *Facial recognition technology: fundamental rights considerations in the context of law enforcement,* pp. 11-12.

[92] El NIST identifica más de 70 clases de sesgos.

[93] NIST. *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, ob. cit., pp. 26-27.

[94] Zlotnik, A. *"Inteligencia Artificial en las Administraciones Públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación",* ob. cit., p. 27.

[95] NIST. *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* ob. cit., p. 27.

[96] Zlotnik, A. *"Inteligencia Artificial en las Administraciones Públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación",* ob. cit., p. 27. Con este fin, deberían aplicarse las

La relación entre el derecho a la protección de datos personales y la prohibición de discriminación se manifiesta singularmente en la particular protección que brinda a determinadas categorías de datos personales por su especial sensibilidad. Como señaló Pérez Luño, la prohibición de su tratamiento salvo para unos fines muy concretos, tiene relación directa con la prohibición de discriminación y su engarce directo con el valor de la dignidad humana[97]. No obstante, serán las previsiones del art. 22 del RGPD las que deberían tener un papel principal en orden a conjurar determinados riesgos de discriminación algorítmica, en especial tras la sentencia del TJUE de 7 de diciembre de 2023 (asunto C-643/21)[98]. En esta resolución, la primera de Tribunal europeo sobre la aplicabilidad del art. 22, interpreta de forma amplia el alcance del derecho del interesado a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, considerando que *"dicha disposición establece una prohibición de principio cuya inobservancia no necesita ser invocada proactivamente por el interesado"*[99].

El TJUE analiza el alcance y los requisitos de aplicabilidad del art. 22 para determinar si la generación de un valor de probabilidad de un comportamiento

---

técnicas de evaluación de impacto algorítmico para determinar si existen sesgos en los algoritmos utilizados en los sistemas de IA, garantizando la no discriminación en la implementación del modelo, analizando para ello *"la lógica implementada, para que la misma no produzca inexactitudes por diseño, y* (empleando) *modelos maduros de pruebas y test de la lógica para detectar errores de diseño* (AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, p. 36).

[97] Pérez Luño, A. E. (2001). "La tutela jurídica de los datos personales en España", *La Toga*, núm. 131, Ilustre Colegio de Abogados de Sevilla, diciembre, p. VIII.

[98] El TJUE resuelve la decisión prejudicial planteada por un tribunal alemán en base a los siguientes hechos: a la demandante (OQ) le fue denegado un préstamo por un tercero después de que una agencia de información comercial (SCHUFA) generara y facilitara a este información negativa sobre ella. OQ solicitó a SCHUFA que le suministrara información sobre los datos personales registrados y que suprimiera los supuestamente erróneos. En respuesta a esta solicitud, SCHUFA informó a OQ sobre su calificación y expuso, a grandes rasgos, los métodos de cálculo, pero, invocando el secreto comercial, se negó a divulgar los distintos datos que había tenido en cuenta a efectos de dicho cálculo, así como su ponderación. SCHUFA argumentó que ella no adoptaba ninguna decisión sino se limitaba a facilitar información a sus socios, que eran quienes adoptaban las decisiones contractuales propiamente dichas.

[99] En el mismo sentido ya se había manifestado el Grupo de trabajo del art. 29 (GT29) en sus *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.*

futuro de una persona (score o calificación), como el reembolso de un préstamo, a partir de determinadas características de dicha persona, sobre la base de procedimientos matemáticos y estadísticos, constituye una decisión individual automatizada en el sentido del art. 22[100]. Ese valor de probabilidad lo elabora una agencia de información comercial y se lo transmite a una entidad de crédito que es la que, teniendo en cuenta ese valor, va a decidir si concede o deniega un préstamo. A la vista de que la decisión automatizada no la adopta quien realiza la calificación de la probabilidad es preciso, indica el TJUE, interpretar el art. 22 teniendo en cuenta, además del tenor de la disposición, el contexto en que se inscribe y los objetivos y la finalidad que persigue el acto del que forma parte.

La aplicabilidad del art. 22 está sujeta a tres requisitos acumulativos: debe existir una decisión; dicha decisión debe estar *"basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles"*; y debe producir efectos jurídicos que afecten al interesado o que le afecten "significativamente de modo similar". El TJUE señaló que se cumplían los tres, pues el principio de interpretación teleológica a la luz de lo dispuesto Considerando 71 del RGPD determina un concepto amplio de decisión, que *"puede incluir diversos actos con potencial para afectar al interesado de múltiples maneras, ya que es lo suficientemente amplio para englobar el resultado del cálculo de la solvencia de una persona en forma de un valor de probabilidad relativo a su capacidad para hacer frente a sus compromisos de pago en el futuro"* (fundamentos jurídicos 45 y 46). En relación al segundo de los requisitos, considera el TJUE que una actividad que consiste en la generación automatizada de un valor de probabilidad para predecir su capacidad para satisfacer un préstamo en el futuro responde a la definición de "elaboración de perfiles" del RGPD y, también se cumpliría el tercer requisito, ya que la decisión produce un efecto suficientemente importante porque, en la práctica, la asignación un valor de probabilidad insuficiente dará lugar *"a que el banco deniegue la concesión del préstamo solicitado"* (fundamento jurídico 48). Finalmente, el TJUE entendió que se cumplían los requisitos del art. 22, aun cuando quien tomaba la decisión formal fuera un tercero, pues, en circunstancias como las de este caso, *"en las que están implicados tres actores, existiría un riesgo de elusión del art. 22 del RGPD y, en consecuencia, una laguna en la protección jurídica, si se optara por una*

---

[100] La generación de los valores de probabilidad se fundamenta en la hipótesis de que la clasificación de una persona en una categoría con características comparables, que ha mostrado cierto comportamiento, permitirá prever un comportamiento similar.

interpretación restrictiva de esta disposición según la cual la generación del valor de probabilidad debiera considerarse un mero acto preparatorio y solo el acto adoptado por el tercero pudiera, en su caso, calificarse de "decisión", en el sentido del art. 22" (fundamento jurídico 61).

Esta conclusión tiene relevantes efectos prácticos ya que implica que, cuando pueda lícitamente elaborarse un perfil o adoptarse automatizadamente una decisión[101], tendrán que implementarse medidas adecuadas para salvaguardar los derechos e intereses legítimos del interesado[102] y se habrán de garantizar los derechos previstos en el RGPD. En particular, habrá de informarse al interesado de la existencia de decisiones automatizadas, incluida la elaboración de perfiles, proporcionándole información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado, pero también de su derecho a oponerse a la elaboración de perfiles según lo establecido en el art. 21.1 (arts. 13 y 14). También tendrá derecho a obtener detalles de cualquier dato personal utilizado para la elaboración de perfiles, incluidas las categorías de datos utilizados como datos de entrada, así como la información sobre el perfil y los detalles sobre los segmentos a los que se le ha asignado[103]. Igualmente, en su caso, la información sobre la existencia de decisiones automatizadas, la información significativa sobre la lógica aplicada y sobre las consecuencias de dicho tratamiento.

Cuando las decisiones automatizadas se basen en la celebración o ejecución de un contrato o en el consentimiento del interesado habrán de garantizarse también los tres derechos previstos en el propio art. 22: el derecho a obtener intervención humana por parte del responsable, el derecho a expresar su punto de vista y derecho a impugnar la decisión. Señala el GT29 que dicha intervención humana ha

---

[101] Cuando la decisión esté autorizada por el Derecho de la Unión o de los Estados miembros, cuando sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento o cuando se base en el consentimiento explícito del interesado.

[102] A juicio del TJUE, como mínimo estas salvaguardias incluirán a tenor de lo previsto en el Considerando 71, *"la obligación del responsable del tratamiento de utilizar procedimientos matemáticos o estadísticos adecuados, de aplicar las medidas técnicas y organizativas apropiadas para garantizar que se reduzca al máximo el riesgo de error y se corrijan errores, y de asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, los efectos discriminatorios en las personas físicas".*

[103] GT29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, p. 19.

de ser significativa, es decir, la *"revisión debe ser llevada a cabo por una persona con la autorización y capacidad adecuadas para modificar la decisión. El revisor debe llevar a cabo una evaluación completa de todos los datos pertinentes, incluida cualquier información adicional facilitada por el interesado"*[104].

La adopción de medidas adecuadas para salvaguardar los derechos de los interesados es fundamental ya que el algoritmo utilizado puede arrojar resultados sesgados, erróneos o injustos. Así lo ha entendido la AEPD y *"por ello el RGPD fija las garantías que deben adoptarse en el uso de algoritmos que toman decisiones debido al mayor riesgo que comportan, entre ellas se impone al responsable un deber de transparencia"*[105]. E incluso en los supuestos en los que esté autorizada la adopción de una decisión automatizada, *"dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión (...)";* pero, en todo caso, la adopción de este sistema de garantías no eximirá al responsable *"de dar cumplimiento a los deberes de información"* recogidos en el RGPD"[106]. El correcto de cumplimiento de las adicionales obligaciones informativas del responsable es fundamental, pues como ha indicado la AEPD, para poder impugnar la decisión *"antes se han de conocer los datos que se han utilizado en el algoritmo, los resultados obtenidos y el perfil generado"*[107].

---

[104] Ibidem, p. 30. En el art. 22 se establece, además, una limitación en razón de la naturaleza de los datos personales prohibiéndose la adopción de decisiones automatizadas basadas en especialmente protegidos salvo que el interesado haya prestado su consentimiento explícito y esta posibilidad no esté prohibida por el Derecho de la Unión o de los Estados miembros o cuando el tratamiento sea necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. En ambos casos, deberán tomarse medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

[105] AEPD. Resolución de procedimiento sancionador PS 000209/2022, p. 63.

[106] Ibidem, p. 64.

[107] Resolución de 17 enero 2022, núm.: R/00819/2021, p. 8. En el mismo sentido STJUE de 7 de diciembre de 2023, fundamento jurídico 56.

5. LA DISCRIMINACIÓN ALGORÍTMICA EN EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

El día 13 de marzo de 2024 se aprobó finalmente el Reglamento de Inteligencia Artificial, que debería jugar un importante papel, al menos por lo que se refiere a los sistemas de IA de alto riesgo, en la prevención de la discriminación algorítmica. Del complejo conjunto normativo del RIA, en relación con esta cuestión, son varios los aspectos que se pueden destacar. El RIA, al igual que otras normas de la UE que regulan el impacto de las tecnologías digitales en los derechos fundamentales, adopta un enfoque desde el riesgo para prevenir los posibles daños, así ocurre, tanto en el RGPD, como en el Reglamento de Servicios Digitales[108]. La preocupación por los efectos de exclusión o discriminatorios de determinados sistemas de IA, ya sea por el tipo de datos personales que utilizan, sus fines o por sus usos en determinados ámbitos va a implicar que existan determinadas IA prohibidas (las del art. 5), ya que se considera que suponen un riesgo inaceptable para la seguridad, la salud o los derechos de las personas y una segunda categoría de sistemas, que serán calificados de alto riesgo (art. 6).

En relación con el tema que nos ocupa y sin ánimo exhaustivo, destaca la prohibición, con algunas excepciones, del uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de aplicación de la ley, ya que las imprecisiones técnicas de estos sistemas, *"pueden dar lugar a resultados sesgados y conllevar efectos discriminatorios"*, relacionados con el sexo, la etnia, raza la discapacidad, la edad, etc. (Considerando 18); los sistemas de categorización biométrica para inferir características sensibles de las personas (por ejemplo, creencias políticas, religiosas, filosóficas, orientación sexual, raza); los sistemas de reconocimiento facial basados en la extracción no dirigida de imágenes faciales de Internet[109] o imágenes de CCTV y los sistemas de reconocimiento de emociones en el lugar de trabajo y en instituciones educativas, que son escasamente fiables por la variabilidad cultural e individual de su expresión y que pueden dar lugar a resultados discriminatorios y muy intrusivos en los derechos de las personas (Considerando 26c); las evaluaciones predictivas de riesgo

---

108 Reglamento (UE) 2022/2065, de 19 de octubre, de Servicios Digitales (RSD).

109 Esta práctica ya llevó a varias autoridades europeas a sancionar a la empresa *Clearwiew* por recolectar, violando el RGPD, datos biométricos y de geolocalización de ciudadanos europeos: entre ellas las autoridades italiana y francesa le impusieron cada una la sanción de 20 millones de euros.

en la comisión de delitos salvo cuando sirva de apoyo al análisis humano en la implicación de una persona determinada en una actividad delictiva y se base en hechos objetivos y verificables directamente relacionados con esa actividad; o los sistemas categorización y puntuación de las personas en función de su comportamiento social o características personales, conocidas o inferidas Los riesgos discriminatorios de los sistemas de puntuación social son muy elevados y pueden determinar incluso la exclusión de grupos sociales enteros en base a su comportamiento social en diversos contextos o características personales o de personalidad conocidas, inferidas o predichas a lo largo del tiempo (Considerando 17).

El artículo 6 del RIA determina las condiciones que ha de cumplir un sistema de IA para ser considerado de alto riesgo y, en su apartado segundo se dispone que tendrán esa consideración los recogidos en el Anexo III. Entre ellos, se encuentran los sistemas biométricos o de reconocimiento de emociones cuando su uso esté permitido; en el ámbito de la educación cuando sirvan para determinar el acceso a cualquier nivel educativo, para evaluar resultados de aprendizaje o para evaluar el nivel de educación al que podrá acceder una persona, o para supervisar o detectar comportamientos prohibidos por los estudiantes durante las pruebas. También se incluyen los sistemas de IA para la contratación o selección de trabajadores, publicación de anuncios de empleo o para evaluar o filtrar solicitudes, así como los que se empleen para tomar decisiones que afecten a las condiciones de trabajo, la promoción o la extinción de la relación laboral y la asignación de tareas o evaluación del rendimiento o comportamiento en este ámbito. Un tercer grupo de sistemas de alto riesgo lo englobarían aquellos que en el ámbito de las administraciones públicas sirvan para evaluar, conceder, revocar o reclamar el derecho a prestaciones y servicios esenciales de asistencia, incluida la sanitaria. Los que se utilicen para evaluar y atender las llamadas de emergencia, los que evalúen riesgos y tarificación en el ámbito de los seguros o la solvencia crediticia de las personas y para la prevención de fraudes financieros. Asimismo, tienen esta calificación, los sistemas utilizados en el ámbito policial y judicial y los utilizados en la gestión de la migración, asilo y control de fronteras en los supuestos permitidos. En el último grupo se recogen los sistemas de IA para asistir a la autoridad judicial en la interpretación de los hechos o aplicación de la ley, también en el ámbito de la resolución extrajudicial de conflictos y los *"destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento de voto de personas físicas en el ejercicio de su voto en elecciones o referendos"*.

En todos los casos se trata de ámbitos en la que las consecuencias de la discriminación algorítmica sería muy grave privando a las personas o a determinados grupos del acceso a servicios o prestaciones, a la formación profesional o a la educación en los distintos niveles o discriminándola en el ámbito de la investigación policial, el empleo o en la resolución judicial o extrajudicial de conflictos pudiendo verse gravemente perjudicada en sus derechos fundamentales. Para prevenir la discriminación algorítmica, el RIA establece en su art. 9 obligaciones de evaluación y mitigación de riesgos y entre las cuales podemos destacar las siguientes:

a) La implantación de un sistema de gestión de riesgos durante todo el ciclo de vida del sistema, identificando, analizando y evaluando los riesgos y adoptando las medidas necesarias para su gestión y minimización.

b) Que se garantice la calidad de los datos para aquellos sistemas que utilicen técnicas que implican el entrenamiento de modelos con datos.

c) Se prevén obligaciones específicas para la redacción de la documentación técnica.

d) Que se diseñen e implementen archivos de registro que garanticen la trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida.

e) Se prevé el reforzamiento de las obligaciones de transparencia e información para garantizar la correcta interpretación y uso de su información de salida por parte de los usuarios y, asimismo, para que el usuario y el proveedor cumplan las obligaciones previstas en el RIA.

f) Se obliga a diseñar y desarrollar los sistemas de forma que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, dotándolos de una interfaz humano-máquina adecuada a fin de prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando el sistema se utilice conforme a su finalidad prevista o cuando se le dé un uso indebido razonablemente previsible.

g) Que se diseñen y desarrollen de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera consistente en esos sentidos durante todo su ciclo de vida.

Se ha reforzado el conjunto de obligaciones que garantizan la transparencia de los sistemas, *"un elemento clave que incide directamente en la calidad y robustez del sistema, así como respecto de la posibilidad de controlar sesgos, errores o posibles*

discriminaciones"[110], incluyendo además la exigencia de que realice una evaluación del impacto en los derechos fundamentales antes de que un sistema de IA de alto riesgo sea introducido en el mercado por sus implementadores[111].

Asimismo se prevén, en el art. 10, obligaciones muy concretas respecto de los sistemas de alto riesgo que se basen en técnicas de entrenamiento de modelos con datos para los que se exigen elevados requisitos de calidad y que atañen a su pertinencia, representatividad contextual suficiente, que estén adecuadamente seleccionados, preparados, actualizados o etiquetados, sujetos a prácticas adecuadas de gobernanza y gestión, a la adecuada valoración de diseño y de las operaciones de tratamiento, su trazabilidad, etc. En todo caso, se atenderá a la evitación de los posibles sesgos, identificando lagunas o deficiencias y, en definitiva, *"los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la medida de lo posible, estarán exentos de errores y serán completos con vistas a la finalidad prevista"*. Deben adoptarse las medidas técnicas adecuadas para evitar los sesgos inherentes a los conjuntos de datos y que estos sean completos y estén libres de errores especialmente cuando se utilizan datos históricos con el fin de no *"perpetuar y amplificar la discriminación existente, en particular para las personas pertenecientes a determinados grupos vulnerables, incluidos los grupos raciales o étnicos"* (Considerando 44).

El conjunto de medidas proactivas y preventivas que prevé el RIA incluye el mantenimiento de registros durante toda la vida útil del sistema (art. 12), la supervisión humana eficaz durante el período en que el sistema de IA esté en uso (art. 14), el desarrollo de métricas adecuadas para garantizar un nivel adecuado de precisión, solidez y seguridad adecuado (art. 15), la evaluación del impacto sobre los derechos fundamentales (art. 29.bis) o la evaluación de conformidad del sistema (art. 43). También se prevén medidas de control y vigilancia posterior a la comercialización, como el registro de sistemas de IA (art. 51) y, en mi opinión las importantes previsiones de remedio, entre las que merecen un lugar destacado, el derecho de cualquier persona a presentar una denuncia ante un órgano de vigilancia del mercado (art. 68bis) y, particularmente, el derecho de cualquier

---

[110] Cotino Hueso, L. (2023). "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida", *Revista Española de la Transparencia*, núm. 16, enero-junio, p. 33.
[111] Fernández, C. B. (2023). "Los negociadores europeos alcanzan el acuerdo definitivo sobre el Reglamento de inteligencia artificial", *Diario La Ley*, 9 de diciembre.

persona afectada por una decisión adoptada *"sobre la base de los resultados de un sistema de IA de alto riesgo*[112] *y que produzca efectos jurídicos o le afecte significativamente de manera similar de forma que considere que repercute negativamente en su salud, seguridad y derechos fundamentales, tendrá derecho a solicitar al responsable del despliegue explicaciones claras y significativas sobre el papel del sistema de IA en el procedimiento de toma de decisiones y los principales elementos de la decisión adoptada"* (art. 68 quater). El cumplimiento de todas estas medidas de responsabilidad proactiva abarcará desde el momento de concepción, diseño y entrenamiento del sistema, durante su despliegue y, especialmente tras este *"cobra especial protagonismo garantizar la intervención humana y la supervisión de los resultados y reevaluación de su funcionamiento, así como la garantía de los derechos de los interesados afectados de acceso de información frente a posibles vulneraciones de derechos"*[113].

6. CONCLUSIONES

La utilización de la IA plantea riesgos significativos para numerosos derechos fundamentales, también para democracia y el Estado de Derecho. Uno de esos riesgos es la denominada discriminación algorítmica, que, en mi opinión, no puede atribuirse por completo al erróneo diseño o calibrado del sistema de IA. La tecnología no aparece en un páramo estéril, sino que refleja, a través de sus datos de entrenamiento, sus opciones de diseño, sus propósitos y el contexto en que se emplea, los sesgos de quien lo diseña y utiliza, pero también del conjunto de la sociedad. Baste como ejemplo los sistemas basados en aprendizaje automático de las redes sociales que aprenden por retroalimentación de sus usuarios y pueden convertir un sistema conversacional en racista y sexista en menos de 24 horas[114]. La discriminación no es producto exclusivo de la IA, sino que

---

[112] Los del Anexo III a excepción de los del segundo punto, aquellos que se refieren a "Infraestructuras críticas", es decir, los "sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, el tráfico por carretera y el suministro de agua, gas, calefacción y electricidad".

[113] Cotino Hueso, L.: "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", ob. cit., pp. 324-325.

[114] Metz, R. (2018). "El chatbot racista de Microsoft, el mejor ejemplo a evitar para la IA", *MIT Technology Review*, 10 de abril.

es *"un fenómeno estructural, político, económico, social e intelectual"*[115]. No obstante, estas tecnologías poseen una enorme capacidad para perpetuar y exacerbar los prejuicios y la discriminación como ha sido ampliamente documentado en los abundantes estudios existentes. Su potencial para multiplicar el daño a los derechos de las personas es bien conocido en la red y a ha tenido su puntual reflejo en la labor judicial y en la aprobación de nuevas normativas en la Unión Europea, como el Reglamento de Servicios Digitales, que regula los algoritmos que perfilan a los usuarios de los servicios, recomendando o priorizando contenidos (y actitudes), en ocasiones, de forma discriminatoria para mujeres y minorías. En este caso, si bien los daños para los derechos pueden atribuirse en gran medida a la arquitectura de las plataformas y servicios, al diseño de sus algoritmos y a la falta de controles efectivos, no es menos cierto que determinados comportamientos de los usuarios son determinantes para ocasionar la lesión en los intereses y derechos de terceros.

Sin duda *"las decisiones humanas se encuentran sometidas a sesgos tanto o más profundos y abundantes que las algorítmicas"*[116], pero cuando afectan a los derechos e intereses de las personas produciendo un efecto jurídico u otro de similar impacto debe poderse exigir, a unas y a otras, *"control, tanto ex ante como ex post"*[117]. Se trata de sistemas con vocación de aplicarse de forma generalizada y, como consecuencia del gran número de personas afectadas, el número de errores y de personas que se verán perjudicas por estos errores y sesgos intrínsecos, también aumentará, desencadenando interferencias adicionales en los derechos humanos de múltiples maneras[118].

El objetivo de las disposiciones éticas y jurídicas reguladoras de los sistemas de IA es el de *"promover la adopción de una inteligencia artificial centrada en el ser humano y digna de confianza, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales consagrados en la Carta, incluidos la democracia y el Estado de Derecho y la protección del medio*

---

[115] Jaume-Palasí, L. *"Justicia: inteligencia artificial y discriminación - una arqueología"*, ob. cit., p. 79.

[116] Huergo Lora, A. *"Hacia la regulación europea de la inteligencia artificial"*, ob. cit., p. 755.

[117] Berning Prieto, A. D. "La naturaleza jurídica de los algoritmos", Gamaero Cadasado, E. y Pérez Guerrero, F. L., *Inteligencia Artificial y sector público*, ob. cit., p. 113.

[118] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, de 8 de abril de 2020.

ambiente, contra los efectos nocivos de los sistemas de inteligencia artificial en la Unión y apoyar la innovación" (Considerando 1 del RIA). Con este fin se recogen principios relativos al respeto de la autonomía humana, la prevención del daño, la equidad y la explicabilidad[119], pero en cuya base están la dignidad y los derechos y las libertades fundamentales porque ese es el auténtico significado de situar al ser humano en el centro de la protección. Sin duda, en este camino, la aprobación del RIA era urgente, si bien no debe ignorarse que el desarrollo de los sistemas de IA ya estaban sometidos al sistema jurídico que conforma el Derecho positivo español y de la Unión Europea a través principalmente la legislación sobre igualdad de trato y no discriminación y sobre protección de datos personales. En este sentido sus previsiones completan un conjunto normativo que constituyen, en mi opinión, las vías concurrentes y complementarias para abordar la discriminación algorítmica.

Las normas sobre protección de datos personales siguen jugando un papel muy relevante para prevenir la discriminación algorítmica, precisamente, porque a través de las obligaciones que se imponen al responsable del tratamiento derivadas de principio de responsabilidad proactiva se deben adoptar las medidas técnicas y organizativas preventivas suficientes para garantizar la correcta aplicación de los principios de relativos al tratamiento durante todo el ciclo de vida del sistema, es decir, desde el momento de su concepción, diseño y desarrollo hasta el de su despliegue y uso y, para ello, será imprescindible la adecuada valoración del riesgo de discriminación algorítmica a través de una EIPD y la aplicación, entre otros, del principio de privacidad desde el diseño. Por otra parte, la reciente interpretación del art. 22 del RGPD por el TJUE ha confirmado la interpretación que ya venían haciendo las autoridades de control de un amplio concepto de decisión automatizada y, en consecuencia, de la aplicabilidad de los principios anteriores y, en particular el de transparencia que incluye explicaciones sobre la lógica y los parámetros del sistema de IA, a fin de garantizar que el interesado pueda impugnar la decisión. Por otra parte, la protección concurrente que brinda el art. 8 del CEDH, en particular por la amplia noción de vida privada que ha venido estableciendo el TEDH, va a exigir asimismo la adopción de medidas preventivas en el diseño e implementación de los sistemas de IA y de control posterior durante su despliegue a fin de que la injerencia en la vida privada supere el test de necesidad

---

[119] Comisión Europea. *Directrices éticas para una IA fiable*, punto 48.

y proporcionalidad, debiéndose garantizar suficientemente los principios de limitación de la finalidad y minimización de datos, entre otros.

En segundo lugar, la prevención de la discriminación algorítmica es uno de los objetivos del RIA que, por una parte, prohíbe los sistemas de IA que suponen un riesgo inaceptable para los derechos fundamentales y, por otra, impone requisitos técnicos específicos para evitar los sesgos algorítmicos y medidas preventivas y de vigilancia sobre los sistemas de IA de alto riesgo, así como el derecho a presentar una denuncia ante el órgano supervisor y a recibir explicaciones claras y significativas sobre el papel del sistema de IA en la adopción de las decisiones sobre las personas, susceptibles de afectar a sus derechos. Estas explicaciones podrían determinar, junto la obligación de registro de los algoritmos, a la obtención de los indicios o de los medios de prueba necesarios para impugnar la decisión total o parcialmente automatizada por errónea, sesgada o discriminatoria y que, según los casos, determinará la aplicación del principio de igualdad y la aplicabilidad de la legislación antidiscriminatoria. En este sentido, si esta información permite a la persona afectada por la decisión algorítmica, aportar indicios fundados de la existencia de discriminación y estamos ante alguna de las categorías especialmente sospechosas, corresponderá a quien utilice el sistema de IA probar que no es discriminatorio. En los demás casos, cuando no proceda la inversión de la carga de la prueba, la información facilitada podrá utilizarse para probar que el sistema produce errores o *"sesgos relevantes o establece diferencias de trato que son claramente irrazonables"*[120].

Por último, la Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), que actualmente se está tramitando en la Unión Europea, complementará este conjunto normativo para garantizar la reparación de la discriminación algorítmica cuando fallen los sistemas preventivos y de supervisión destinados a evitarla.

---

[120] Cotino Hueso, L.: *"Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público"*, ob. cit., p. 309.

BIBLIOGRAFÍA

Agencia Española de Protección de Datos (AEPD) (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, junio.

Agencia Española de Protección de Datos (AEPD) (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, febrero.

Añón Roig, M. J. (2022). "Desigualdades algorítmicas: conductas de alto riesgo para los derechos humanos", *Derechos y Libertades*, núm. 47, época II, junio.

Arenas Ramiro, M. (2022). "La igualdad a la luz de los derechos digitales", Reche Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías,* Aranzadi, Navarra.

Barocas, S. y Selbst, A. D. (2016). "Big Data's Disparate Impact", *California Law Review*, Vol. 104.

Barrere Unzueta, M. A. y Morondo Taramundi, D. (2011). "Subordiscriminación y discriminación interseccional: elementos para una teoría del derecho antidiscriminatorio", *Anales de la Cátedra Francisco Suárez*, núm. 45.

Belloso Martín, N. (2022). "La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un Derecho a la protección contra los sesgos?", LLANO ALONSO, F. H. (dir.), *Inteligencia artificial y Filosofía del Derecho,* Editorial Laborun, Murcia.

Berning Prieto, A. D. (2023). "La naturaleza jurídica de los algoritmos", Gamaero Casado, E. y Pérez Guerrero, F. L. (coords.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

Boyd, D. y Crawford, K. (2012). "Critical Questions for Big Data. Provocations for a Cultural, Technological and Scholarly Phenomenon", *Information, Communication & Society*, Vol. 15, núm. 5, junio.

Carmona Cuenca, E. (1994). "El principio de igualdad material en la jurisprudencia del Tribunal Constitucional", *Revista de Estudios Políticos* (nueva época), núm. 84, abril-junio.

Castillo Parrilla, J. A. (2020). "Sentencia del Tribunal Ordinario de Bolonia de 31 de diciembre de 2020 (Caso Deliveroo) ¿Discriminación algorítmica o discriminación a través de un algoritmo?", *Derecho Digital e Innovación*, núm. 7, octubre.

Comisión Europea (2019). Dirección General de Redes de Comunicación, Contenido y Tecnologías: Directrices éticas para una IA fiable, Oficina de Publicaciones. https://data.europa.eu/doi/10.2759/14078

Comité Europeo de Protección de Datos (CEPD) (2023). *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, Adopted on 26 April.

Consejo de Europa (2020). *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the Human Rights Impacts of Algorithmic Systems*, April.

Consejo de Europa (2021). *Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling*, November

Cotino Hueso, L. (2023). "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público", GAMAERO CASADO, E. y PÉREZ GUERRERO, F. L. (coords.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

Cotino Hueso, L. (2020). "Holanda: «SyRI, ¿a quién sanciono?». Garantías frente al uso de la inteligencia artificial y decisones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley privacidad*, núm. 4, abril.

Cotino Hueso, L. (2023). "Los usos de la inteligencia artificial en el sector público, su variable impacto y categorización jurídica", *Revista Canaria de Administración Pública*.

Cotino Hueso, L. (2023). "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida", *Revista Española de la Transparencia*, núm. 16, enero-junio.

De Asís Roig, R. (2022). *Derechos y tecnologías*, Madrid, Dykinson.

De Asís Roig, R. (2022). "Sobre la propuesta de los neuroderechos", Derechos y libertades, *Revista de Filosofía del Derecho y derechos humanos*, núm. 47.

Ester Sánchez, A. T. (2023). "El desafío de la inteligencia artificial a la vigencia de los derechos fundamentales", *Cuadernos Electrónicos de Filosofía del Derecho*, núm. 48.

Estévez Almenzar, M., Fernández Llorca, D., Gómez, E. y Martínez Plumed, F. (2022). *Glossary of Human-Centred Artificial Intelligence*, Publications Office of the European Union, Luxembourg. https://doi:10.2760/860665,JRC129614

Fernández, C. B. (2023). "Los negociadores europeos alcanzan el acuerdo definitivo sobre el Reglamento de inteligencia artificial", *Diario La Ley*, 9 de diciembre.

FRA (European Union Agency for Fundamental Rights) (2020). *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. https://doi:10.2811/524628

García Murcia, J. (2022). "La Ley 15/2022 Integral para la igualdad de trato y no discriminación", *Foro*, Nueva Época, Vol. 25, núm. 2, p. 16.

García Quiñones, J. C. (2023). "Inteligencia artificial y relaciones laborales: entre la significación creciente de los algoritmos y el desmentido de su neutralidad aparente", *Temas laborales: Revista andaluza de trabajo y bienestar social,* núm. 167, p. 80.

Garriga Domínguez, A. (2021). "Decisiones automatizadas basadas en algoritmos y protección de datos personales", Tomás Mallén, B., García Mahamut, R. y Pauner Chulvi, C., *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español*, Tirant lo Blanch, Valencia.

Garriga Domínguez, A. (2018). "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, núm. 38, enero.

Garriga Domínguez, A. (2015). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, Madrid.

Gluk. G. (2022). "Igualdad y no discriminación de las personas mayores", *Teoría y Derecho: revista de pensamiento jurídico*, núm. 33.

González Cabanes, F. y Díaz Díaz, N. (2023). "¿Qué es la inteligencia artificial?", Gamaero Casado, E. y Pérez Guerrero, F. L. (coords.), *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

González de Patto, R. M. (2023). "Inteligencia artificial y empleo. Análisis crítico del marco regulatorio europeo y español impulsado por el Pilar Europeo de Derechos Sociales", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 168.

Grupo de Trabajo del Art. 29 (GT29). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018.*

Huergo Lora, A. (2023). "Hacia la regulación europea de la inteligencia artificial", Gamaero Casado, E. y Pérez Guerrero, F. L. (coords.): *Inteligencia artificial y sector público: retos, límites y medios*, Tirant lo Blanch, Valencia.

Jaume-Palasí, L. (2022). "Justicia: inteligencia artificial y discriminación - una arqueología", Reche Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*, Aranzadi, Cizur Menor.

Meseguer González, P. y López De Mántaras Badia, R. (2017). *Inteligencia artificial,* Madrid, Editorial CSIC Consejo Superior de Investigaciones Científicas.

Metz, R. (2018). "El chatbot racista de Microsoft, el mejor ejemplo a evitar para la IA", *MIT Technology Review*, 10 de abril.

NIST (National Institute of Standars and Technology. U. S. Departament of Commerce). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, p. 3/77. https://doi.org/10.6028/NIST.SP.1270.

Palma Ortigosa, A. (2022). "El ciclo de vida de los sistemas de inteligencia artificial. Aproximación técnica de las fases presentes durante el diseño y despliegue de los sistemas algorítmicos", Cotino Hueso, L. (dir.): *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor.

Pérez Luño, A. E. (2001). "La tutela jurídica de los datos personales en España", *La Toga*, núm. 131, Ilustre Colegio de Abogados de Sevilla, diciembre, p. VIII.

Pérez Luño, Antonio E. (1992). "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data", García San Miguel, L. (ed.): *Estudios sobre el derecho a la intimidad,* Tecnos, Madrid.

Rey Martínez, F. (2008). "La discriminación múltiple, una realidad antigua, un concepto nuevo", *Revista Española de Derecho Constitucional*, núm. 84.

Sáenz Lara, C. (2020). "El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 155.

Soriano Arnanz, A. (2022). "Discriminación algorítmica: garantías y protección jurídica", Cotino Hueso, L. (dir.): *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas,* Aranzadi, Navarra.

Soriano Arnanz, A. (2021). "La aplicación del marco jurídico europeo en materia de igualdad y no discriminación al uso de aplicaciones de Inteligencia Artificial", Bonorino Ramírez, R. (dir.), *Nuevas normatividades: inteligencia artificial, Derecho y género*, Aranzadi, Navarra.

STOA (Panel for the Future of Science and Technology) (2020). *The ethics of artificial intelligence: Issues and initiatives*, European Parliamentary Research Service Scientific Foresight Unit (STOA), PE 634.452, March, p. 15.

UNESCO (2020). *Artificial Intelligence and Gender Equality*.

UNESCO (2021). *Recomendación sobre ética de la inteligencia artificial*, adoptada el 23 de noviembre.

Vantin, S. (2021). "Inteligencia artificial y derecho antidiscriminatorio", Llano Alonso, F.h. y Garrido Martín, J., *Inteligencia artificial y Derecho. El jurista ante los retos de la era digital*, Aranzadi, Navarra.

Yuste, R. (2022). "Los neuroderechos: un abordaje de derechos humanos para la neurotecnología", Reche Tello, N. y Tur Ausina, R. (dirs.), *La teoría constitucional frente a la transformación digital y las nuevas tecnologías*, Aranzadi, Cizur Menor.

Zlotnik, A. (2019). "Inteligencia artificial en las Administraciones Públicas: definiciones, evaluación de viabilidad de proyectos y áreas de aplicación", *Boletic*, núm. 84, julio.

Zuiderveen Borgesius, F. (2018). *Discrimination, Artificial Intelligence and Algorithmic Decision-Making,* Consejo de Europa.

Cuarta Parte

ESTUDIOS SOBRE BLOCKCHAIN

Capítulo 11
ESTRUCTURAS DE GOBIERNO EN BLOCKCHAIN

Ana Felicitas Muñoz Pérez
Catedrática de Derecho Mercantil
Universidad Rey Juan Carlos
https://orcid.org/0000-0003-4051-4746

1. INTRODUCCIÓN

Abordamos en este trabajo el estudio de las estructuras de gobierno en blockchain, conocidas como "Organizaciones Autónomas Descentralizadas" –DAOs en adelante–. La noción se refiere a las organizaciones entre miembros que aprovechan la tecnología de registros distribuidos –DLT en adelante– de Blockchain. Aluden al término "DAO" para referir la noción de organizaciones que utilizan reglas establecidas en código informático sobre una red de blockchain con el fin de reunir a una comunidad unida para el desarrollo de un objetivo sin exigencia de intermediarios que faciliten el gobierno y las operaciones y sin subsumir las relaciones necesariamente a un tipo legal concreto de figura jurídica[1].

La tecnología sirve para almacenar información –"transacciones"– que quedan incorporadas en bloques de datos encadenados. Dado que la "arquitectura técnica" de dicho sistema DLT tiene sus propios principios de gobierno –reglas de consenso y criterios de política– algunos refieren también la noción de DAO a todo el sistema técnico de la DLT. Sigue siendo objeto de debate el contenido asociado a la denominación terminológica "DAO". Sin embargo, como se describirá en Punto II, nuestra propuesta es identificar la DAOs como aplicaciones (DApps) en las capas superiores del sistema de registros distribuidos (DLT).

---

[1] Vid. en particular las definiciones incluidas en el trabajo del equipo compuesto por Burgoyne, Trepak, Hunn, Kimber, Wingfield, Twibill y Edwards, denominado "Decentralised autonomous organisations (DAOs) A scoping paper" The Law Comission, 2024. https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/.

Las DAOs en sentido propio son organizaciones de gobierno que utilizan blockchain, activos digitales y otras tecnologías para captar recursos, coordinar iniciativas y adoptar decisiones[2]. Por esta razón se definen de forma genérica como estructuras para desarrollar modelos disruptivos de negocios para fines filantrópicos (Giveth DAO), artísticos (PleasrDAO), la prestación de servicios digitales colaborativos (Aragon) y, en el ámbito más especulativo, para financiar proyectos (figura original "The DAO"), o incluso la puesta en marcha de un nuevo sistema financiero disruptivo (las DEX en las finanzas descentralizadas DeFi"). Los posibles casos de uso de la tecnología de contabilidad distribuida se desarrollan en un amplio espectro de dedicaciones empresariales –automóvil, la banca, la educación, la energía, medicina, los seguros, el derecho, la música, el arte, los bienes raíces, turismo... entre otros–.

Son sistemas de gobiernos innovadores no exentos de desafíos. La falta de reconocimiento legal de estas entidades genera incertidumbre en los operadores. Sorprende la ausencia de una estrategia legislativa completa dirigida a las DAOs. Los denominados modelos de "legal wrapper" que incorporan la DAO en tipos de sociedades tradicionales no han logrado proporcionar la seguridad legal esperada y las propuestas de incorporar normativas específicas, como la iniciativa en el marco del reglamento de mercados de criptoactivos –MICA– en Europa, han fracasado para el desarrollo.

Este trabajo busca explorar algunos aspectos técnicos y la caracterización de las DAOs, con el objetivo intentar aportar claridad y comprensión de estas innovadoras formas de organización que presentan renovado interés en el entorno financiero de las finanzas descentralizadas (DeFi)[3] y en el ámbito de la Web3[4].

---

[2] World Economic Forum, WEF, "Decentralised Autonomous Organization Toolkit Insight Report" 2023. https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf

[3] European Securities and Markets Authority (ESMA) TRV Risk Analysis, "Decentralised Finance in the EU: Developments and Risks" (2023). https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf

[4] Vid. Jennings y Miles, "Principles & Models of Web3 Decentralization", a16z, 2022, https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf

2. LA DAO EN LA ESTRUCTURA DE GOBIERNO DE LA DLT/ BLOCKCHAIN

2.1. La arquitectura

La red DLT es una estructura técnica que ejecuta un sistema de gobernanza independiente aspecto por el que algunos lo definen como "organismo autónomo" –DAO[5]–. La tecnología DLT –cuyo ejemplo más prominente es blockchain–, instaura una red distribuida de nodos para desarrollar un sistema de gestión de información con ulteriores funcionalidades sin la presencia de una autoridad central[6].

Cada sistema DLT organiza el almacenamiento estándar de datos y tiene su propia hipótesis, método, reglas de seguridad y coste de eficiencia en el marco de la "hight-level architecture", que refiere la funcionalidad común de los componentes esenciales de la DLT cuya estructura se organiza las capas que refiere de forma general la siguiente ilustración[7].

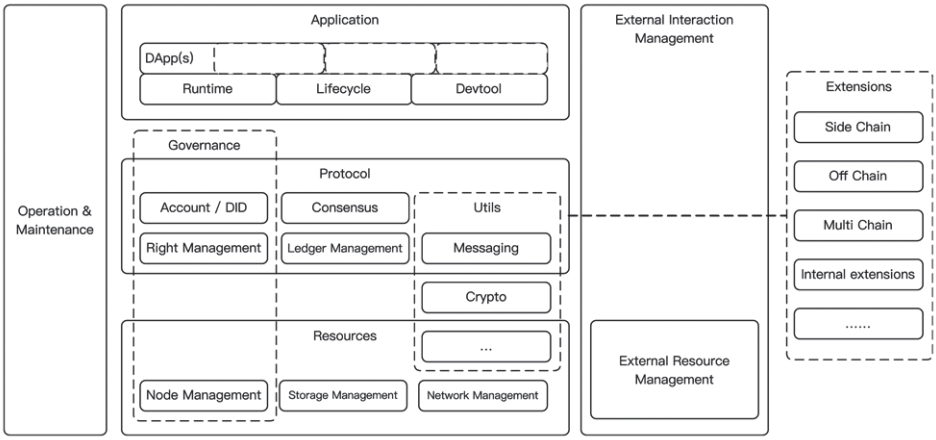
---

[5] Vid. "The International Telecommunication Union" (ITU), serie dedicada DLT por el Focus group on Appplication of Distributed Ledger Technology (FG DLT): Documento D1.1 "Distributed ledger technology terms and definitions", p. 2, sobre definiciones de "decentralized autonomous organization" y Documento D3.1 "Distributed ledger technology reference arquitecture", p. 6.

[6] Vid. El informe técnico del 1 de agosto –ITU-T Focus group on Appplication of Distributed Ledger Technology (FG DLT), Techincal Report FG DLT D4.1 Distributed ledger technology regulatory framework–, resume el funcionamiento. En doctrina Yaga, Mell, Roby y Scarfone (2018), "Blockchain Technology Overview". https://doi.org/10.6028/NIST.IR.8202; FINRA (2017), *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*. https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf; FINRA (2017), *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*. Available at: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf Documento "ITU-T Focus group on Appplication of Distributed Ledger Technology (FG DLT), "Technical Report FG DLT D4.1 "Distributed ledger technology regulatory framework", p. 3.

[7] Documento D3.1 "Distributed ledger technology reference arquitecture", explica que La arquitectura de alto nivel puede abarcar casi todos los libros contables distribuidos, incluyendo las cadenas públicas representadas por Ethereum [b-ethe] y Bitcoin [b-bitc], las cadenas privadas representadas por Hyperledger Fabric y los sistemas de libros contables distribuidos que no son blockchain. p. 6.

Figura 1. High-level conceptual architectute of DLT.



Fuente: ITU technical specification, 3.1 DLT "reference architecture", p. 3.

La infraestructura se define por los "recursos"[8] de que se sirve y el tipo de "protocolos" que implementa para el desarrollo de las "aplicaciones"[9] que se ordenan en capas donde estratifica sus elementos.

El elemento básico es el denominado "libro mayor distribuido" –*Ledger*– que almacena información que replica en cada nodo tras el proceso de validación (por consenso) con el fin de almacenarlo en bloques. Los mecanismos de consenso ("prueba de trabajo" –POW–, la "prueba de participación" –POS– y la "prueba de autoridad" –POA– y Delegated Proof of Stake –DPoS–) sirven para acordar la incorporación de la información registrada y, por ello, se destacan como elementos centrales o "core" del sistema "distributed ledger"[10]. Cada bloque se encadena al bloque anterior con el fin de asegurar la convergencia hacia una versión única e inmutable de dicho "libro mayor".

---

8 ITU, d.3., "Distributed ledger technology reference arquitecture", p. 5.

9 Vid desarrollo detallado en ITU, d.3., "Distributed ledger technology reference arquitecture", pp. 6 y ss. donde refiere las "Cinco funciones" básicas de la infraestructura de red: "Core layes", "Service layer", "Appication service platform", "DLT aplications" y "external service"; explicación en IBAÑEZ JIMENEZ, *Derecho de blockchain*, CI, pp. 31 y ss.

10 Zhang, Shijie y Lee (2020). "Analysis of the main consensus protocols of blockchain". ICT express6.2; Yaga, Mell, Roby y Scarfone (2018). "Blockchain Technology Overview", pp. 18 y ss. https://doi.org/10.6028/NIST.IR.8202

Los protocolos se implementan a partir de la segunda capa donde reside el detalle de los "mecanismos de consenso" y la gestión del "Ledger".

En la tercera capa los "Smart contracts" y las "funciones de gestión de las Dapps", impulsan el contenido de las denominadas "Decentralized application (DApp) functions" dando cabida a las DAOs que serán objeto de particular análisis en la tercera parte de este estudio.

En ocasiones los componentes del sistema DLT pueden tener determinados objetivos que exijan la necesidad de resolver la interacción con datos externos –data interoperability–. Esta extensión de las funciones se incluye en protocolos que están diseñados para mantener estas relaciones externas e.g., "multi-chain", "side-chain", "off-chain", or internal systems, e.g., "child-chain", "sharding" [b-shard1, b-shard2][11]. También las DAOs se sirven de estos recursos.

2.2. El gobierno

La tecnología de contabilidad distribuida se dispone al fin de facilitar el registro y almacenamiento de los datos –"transacciones"–, asistida por el diseño de protocolos donde se incorpora el software que facilita la adopción de decisiones de "gobernanza inteligente".

La DLT actúa como la "columna vertebral" de la DAO para dar infraestructura de soporte a la aplicación y tiene, en sí misma, un determinado sistema de gobierno[12]. Según describe el informe técnico de ITU, la red DLT tiene

---

[11] ITU, d.3., "Distributed ledger technology reference arquitecture", p. 5.

[12] Vid para redes semipermisionadas, IBÁÑEZ JIMÉNEZ (2020), en *Consorcio red Alastria (Origen y reforma de la primera blockchain de España)*, Madrid, p. 158; y las no permisionadas en Seira, Allen, Watsky y Alley (2024), "Governance of Permissionless Blockchain Networks", February 09, FEDS notes. https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html

alternativas[13], con particulares reglas de autogobierno que facilitan la operación de un sistema útil, confiable y eficiente[14].

El sistema elige ser red permisionada, semipermisionada o cerrada, establecer reglas fundamentales para su autoorganización, reaccionar frente a la competencia del mercado, responder a las amenazas de seguridad y tomar otras decisiones estratégicas[15].

Entre los *stakeholders* del sistema de la red –la network– más significativos se mencionan a los "developers", a los "nodos" y a los "usuarios", considerados como "partícipes" de la estructura e identificados por los rasgos de sus funciones en lso siguientes términos.

Los "nodos" (por ejemplo, Mineros/validadores, en redes de consenso POW, o clasificados como "full" o "partial" en función de la información que contienen) permiten a la cadena de bloques validar las transacciones y mantener la seguridad de la red, garantizando que ésta siga estando descentralizada. Entre sus atribuciones más genuinas se encuentra la de controlar de los cambios propuestos en el código fuente de las cadenas de bloques *permisionless*.

Los "usuarios" (grupo de personas u organizaciones –componentes– que utilizan un servicio o consumen la salida del servicio proporcionado por otro componente) podrían ser en una red sin permiso cualquier persona que posea activos digitales relacionados con blockchain ("tokens criptográficos"[16] o "token

---

[13] ITU, Tecnical report FG DLT D4.1 "Distributed ledger technology regulatory framework", pág. 6. Vid. Nabben, Puspasari, Kellher y Sanjay (2021), "Grounding decentralised technologies in cooperative principles: What can "Decentralised Autonomous Organisations" (DAOs) and platform cooperatives learn from each other?". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3979223; Troncoso y Utratiel, "If I Only Had a Heart: A DisCO Manifesto. DisCO", 2019. https://disco.coop/manifesto/, https://www.tni.org/files/profiles-downloads/disco_manifesto_v.1.pdf)

[14] ITU, Tecnical report FG DLT D4.1 "Distributed ledger technology regulatory framework", p .6.

[15] Vid. Seira, Allen, Watsky y Alley (2024). "Governance of Permissionless Blockchain Networks", February 09, FEDS notes. https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html y las referencias doctrinales citadas, señalando tres cuestiones de gobierno: stakeholders, diferencia Bitcoin y Ethereum, el estudio de los forks.

[16] Vid. Shapiro, A. (2022), Functionalist Framework for DeFi Regulation. https://lexnode.substack.com/p/a-functionalist-framework-for-defi. *Digital Assets* (2022). Law Commission Consultation Paper, núm. 256, chapter 14. https://www.lawcom.gov.uk/project/digital-assets/

natives" como "Bitcoin" o "Ether"). Participan en el "gobierno" mediante foros o a instancia de los *developers*.

Los "*developers*" que son los profesionales informáticos especializados en el diseño, construcción y mantenimiento de redes basadas en esta tecnología –"core developers", más influyentes en el gobierno y "application developers"– en ocasiones "proveedores de servicios" por gestionar las interfaces. Diseñan y escriben el software para que funcionen los contratos inteligentes, los protocolos de cadena de bloques y los protocolos de software y ecosistemas de tokens criptográficos. Algunos, por las señaladas facultades, reservan para ellos la titularidad de paquetes de tokens de gobernanza en e incluso la posición de "representantes fiduciarios" frente a los que confían en la red de Blockchain creada[17].

La red organiza un esquema de gobernanza dirigido a ejecutar el sistema de almacenamiento y trazabilidad de la información de la base de datos. La "comunidad" –nodos, usuarios y desarrolladores de software– disponen los mecanismos "on chain" y "off chain" para que el sistema funcione de forma "distribuida"/"descentralizada" con el fin de "agregar" información de forma sincronizada[18].

Pueden ser *blockchains públicas* –transparentes, por ser rastreadas y vistas por cualquier participante de la red y contar con sistema open source software (OSS)– *semipermisionadas* o *privadas*. En las redes abiertas se diferencia entre "gobernanza de la infraestructura" –que se logra a través del propio protocolo, por ejemplo, de Bitcoin– y "gobernanza para la infraestructura" –que es gestionada por la comunidad de desarrolladores y otras partes interesadas, razón por la que a pesar de anunciarse como descentralizada cuentan con elementos de centralización, por ejemplo, Ethereum[19]–.

---

[17] Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/, cit. p. 14.

[18] Vitalik Buterin, "A next generation smart contract & decentralized application platform", Ethereum White Paper; Hassan, Samer y Primavera de Filippi (2021), "Decentralized Autonomous Organization", *Internet Policy Review*, Vol. 10, núm. 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf., p. 3; de Filippi y Wright (2018), *Blockchain and the law: The rule of code*. C.9 "Decentralized autonomous organizations", Harvard, chapter 8, p. 131.

[19] De Filippi y Loveluck, "The invisible politics of bitcoin: governance crisis of a decentralized infrastructure", *Internet Policy Review* 5, núm. 4. https://doi.org/10.14763/2016.3.427. 2016

Una red DLT puede definirse a través de diferentes caracteres, de forma que: en primer lugar, según los principios que inspira su *gobierno* podria ser "anarquico" (Bitcoin), "jerárquico" (Ethereum), "dictatorial" (Ripple) o en forma de "fereder-ación" (Alastria). Por la forma de *acceso a la red* podría ser "abierta" (Bitcoin), "semiabierta" o "semipermisionada" (Alastria) o "cerrada" (como Porject X); Por la forma de *procesar la información* podría ser "descentralizada" (Bitcoin) o "semi-permisionada" (Alastria), o "centralizada" (Project X); por los *incentivos* puede ser "intrínsecos" (Bitcoin), o "extrínsecos" (Alastria); por último las *referencias* pueden ser "endógenas" (Bitcoin) "híbridas" (Ethereum) o "exógenas" (Project X).

2.3. Los elementos

La tecnología se sirve de ciertos elementos que son comunes y se revelan como "esenciales" a las redes DTL: los "activos digitales" y los "Smart contracts" embebidos en los protocolos de sofware que organizan los esquemas de inteligencia artificial que impulsa el funcionamiento:

a) Los *activos digitales* –los tokens criptográficos y los activos criptográficos– originalmente son los elementos que insertan la información en el sistema. En el plano económico, los registros distribuidos –blockchain– y la tecnología asociada *amplían las formas en que los activos digitales se pueden crear, acceder, utilizar y transferir*. La discusión jurídica refiere el debate de su tratamiento jurídico "data object" o "condición legítima del acceso a los contenidos"[20].

b) Los *contratos inteligentes*, incorporan el software para programar y ejecutar "acciones automatizadas" sin intervención humana capaz de ejecutar en esta forma los términos de un contrato[21]. Se desarrollaron originalmente en Ethereum a través de la plataforma informática distribuida y el lenguaje de programación, *Solidity*, que abordó las limitaciones del lenguaje de secuencias de comandos de Bitcoin. Solo el *Smart legal contract*, yendo más allá del simple *smart contract*, sería capaz de generar obligaciones legales vinculantes y satisfacer las condiciones contractuales comunes –como la ejecución, condiciones de pago, los gravámenes, la confidencialidad y conclusión–

---

[20] Digital Assets (2022). Law Commission Consultation Paper núm. 25. https://www.lawcom.gov.uk/project/digital-assets/.

[21] Shakow, D. (2018). "The Tao of the DAO: Taxing an Entity That Lives on a Blockchain".

minimizando la necesidad de intermediarios de confianza[22]. Las DAOs se sirven de la funcionalidad de los "contratos legales inteligentes"[23], aunque en su actual desarrollo no sean completos y, por ello, sea imposible que el contrato "pre-programe" y "determine" *ex-ante* todo escenario posible en que incurra la actividad de la DAO[24].

c) Las DAOs se implementan *en las capas superiores de la DLT*[25], condensando el "protocolo" el conjunto de reglas y operaciones que definen el funcionamiento. Los documentos de la Unión Internacional de Telecomunicaciones (ITU) especifican la arquitectura abstracta típica de los registros distribuidos la arquitectura de la DLT[26], y atribuye a los desarrolladores la definición de la "Decentralized application (DApp) functions" que define el "ecosistema tecnológico" donde trabaja un protocolo para definir una DAO y estandarizar los elementos básicos de la estructura de red donde funciona[27]. En el protocolo se combinan los contratos inteligentes de la

---

[22] Vos (2019). "Cryptoassets as property: how can English law boost the confidence of would-be parties to smart legal contracts?", 2 May, Joint Northern Chancery Bar Association and University of Liverpool Lecture. https://www.judiciary.uk/wp-content/uploads/2019/05/Sir-Geoffrey-Vos-Chancellor-of-the-High-Court-speech-on-cryptoassets.pdf., en especial p. 14., en "Smart Legal Contracts: Advice to Government" (2021), Law Com núm. 401. https://www.lawcom.gov.uk/project/smart-contracts/, señala las principals variables que deben considerarse, que recoge las tres variables serían: el "contrato de lenguaje natural", el "contrato híbrido" y el "contrato registrado". Sobre las nociones de smart contract, SZABO, N., Smart Contracts, Building Blocks for Digital Markets, 1994. http://www.virtualschool.edu/mon/Economics/SmartContracts.html.

[23] Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/. p. 63.

[24] Maskin, E. (2002). 'On Indescribable Contingencies and Incomplete Contracts'. *46 European Economic Review* 725. https://scholar.harvard.edu/files/maskin/files/on_indescribable_contingencies_and_incomplete_contracts_e._maskin.pdf?m=1428327268; Borgogno y Martino (2024). "Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype", núm. 161. EBI, Working paper series.

[25] Vid. Shapiro (2022). "How Protocol DAOs should Work from a Cryptolaw(-ish) Perspective". https://lexnode.substack.com/p/how-protocol-DAOs-should-work-from

[26] ITU-T Technical Specification Telecommunication Standardization Sector, Technical Specification FG DLT D3.1 Distributed ledger technology reference architecture, 2019.

[27] Documentos ITU, D. 11 "DLT terms and definitions",1.2 DLT "overview, concepts, ecosystem", 1.3 DLT "standardization landscape", 2.1 DLT "use cases", 3.1 DLT "reference architecture", 3.3, "Assessment criteria for DLT platforms", 4.1. DLT "regulatory framework", 5.1. "Outlook on DLTs".

aplicación DAO que impulsan actividades concretas sobre la base de las prestaciones de DLT[28].

El "código" organiza la actuación de las relaciones en la DAO de los denominados "activos digitales", "los tokens" –generalmente "de gobernanza" y de "liquidez" en la DAO– con el fin de satisfacer diferentes actividades, nos interesa en particular las empresariales, en un entorno de red distribuida. Como aplicaciones web, pueden combinar servicios fuera de la cadena y servicios dentro de la cadena para dar soluciones a las empresas. Las aplicaciones descentralizadas, o DApps, utilizan las funcionalidades de un contrato inteligente. Los usuarios, pueden utilizar interfaces –por ejemplo, para autenticar su identidad criptográfica–. Firman las "transacciones" los que tienen "acceso legítimo" a las claves privadas, lo que lo convierte en el "propietario" de todos los activos en esa billetera.

La DAO "consolida el funcionamiento" en el grupo de la DLT sobre la base de residenciar en éste ultima el "control técnico" del mecanismo –por ejemplo, el consenso– que se diseña en la primera capa. Por otra parte, existen programas –ejemplo en DeFi–que hacen interoperables las operaciones de distintos protocolos implementados en diferentes DLT, lo que complica la posterior exégesis jurídica.

3. EL GOBIERNO DE LA DAO

3.1. La evolución de "The Dao" al "BORG"

El estudio de la evolución de la DAO permite mayor claridad en la descripción del fenómeno. La doctrina señala en este desarrollo diferentes etapas[29].

Con Bitcoin nace la primera DAO –en el sentido de estructura gobierno de DLT descrito en el anterior apartado–. "Bitcoin" marcó el comienzo de la revolución de Blockchain y la DAO 1.0 queda identificada por la creación de una estructura –o "sistema"– regido por un código que no depende de las acciones de una parte externa para su cumplimiento –"compañía no tripulada"–.

---

[28] Borgogno y Martino (2024). "Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype", núm. 161. EBI, Working paper series.

[29] Tabone, "Dao: the evolution of organization", COINTELEGRAPH.

El proyecto "The Dao" (*The true DAO*) inicia la etapa de DAO 2.0[30], ligada al desarrollo de la tecnología de blockchain con Ethereum y según describimos en este estudio, la DAO en sentido propio[31]. El revolucionario modelo –DAO– se basa en el pre-diseño de funciones básicas en un protocolo de software/contrato inteligente de código abierto implementado en la cadena de bloques gobernado bajo el lema "*The rule of code*"[32]. En una videoconferencia titulada "Ethereum: Freenet or Skynet?", Primavera de Filippi, investigadora de Harvard Berkman Klein Center, resumió sus características: gobierno "autónomo" "autosuficiente" y "descentralizado" cuyos atributos señalamos más adelante (epígrafe 3.3.2.3.). Christoph Jentzsch, programó "The Dao", sobre la base de un *Smart contract* como estructura de empresa "venture" para recaudar fondos en forma de Ether y actuar como "incubadora" de proyectos de "start up" en la red de Ethereum. "Slockt.it" se convirtió en el primer proyecto financiado[33]. Contemporáneo al proyecto "DAO-Dash", creó una revolucionaria estructura que fue replicada en posteriores iniciativas –MolochDAO, MetaCartel, Aragon, DAOstack, Colonia o DAOhaus...[34]–.

---

[30] Buterin (2013). "Bootstrappping a Decentralized Autonomous Corporation: Part I". https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/, September 19.

[31] Vitalik Buterin, "A next generation smart contract & decentralized application platform", Ethereum White Paper; Hassan, Samer y Primavera de Filippi (2021), "Decentralized Autonomous Organization", Internet Policy Review, Vol. 10, núm 2, https://policyreview.info/pdf/policyreview-2021-2-1556.pdf, p. 3.

[32] De Filippi y Wright (2018). *Blockchain and the law: The rule of code*. C.9 "Decentralized autonomous organizations", Harvard, chapter 8, p. 131. Señala World Economic Forum, WEF, "Decentralised Autonomous Organization Toolkit Insight Report" 2023, p. 5 que los marcos de gobernanza codifican en contratos inteligentes el propósito, los roles y las responsabilidades de una organización.

[33] El programa facilitaba compartir proporcionalmente las ganancias y las pérdidas de estas inversions, vid. SHAKOW, D. (2018), "The Tao of The DAO: Taxing an Entity That Lives on a Blockchain", p. 4.

[34] Hassan, Samer y Primavera De FIlippi (2021). "Decentralized Autonomous Organization", Internet Policy Review, Vol. 10, núm. 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf; Shakow, D. (2018). "The Tao of the DAO: Taxing an Entity That Lives on a Blockchain". Describí el nacimiento en Muñoz PÉrez (2019), *Financiación digital y su incidencia en el gobierno corporativo*, Navarra, p. 133; El Faqir El Rhazoui, Arroyo y Hassan, "A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain". https://jisajournal.springeropen.com/articles/10.1186/s13174-021-00139-6

La etapa DAOs 3.0, se identifica por ligar las estructuras de gobierno al nacimiento de las finanzas descentralizadas –DeFi–[35] y el crecimiento de la fusión de tecnologías en el entorno del Metaverso. Las DAOs se dedican a variadas actividades como el juego, la política, el arte y la cultura. De las actividades lúdicas –funcionamiento y "pagos con criptomonedas" en los juegos[36]–, se pasa al desarrollo de los "servicios bancarios"[37] –"pagos"– y al de las Finanzas descentalizadas –"DeFi"–. La estructura de Blockchain se sirve del "internet de las cosas" IOT, "realidad aumentada" y otras tecnologías para organizar ulteriores proyectos de actividad empresarial en la industria –creando las cadenas de suministro, que facilitan la trazabilidad y la desintermediación– y los servicios financieros mediante las tokenizaciones –por ejemplo, en el sector inmobiliario para financiar y vender promociones tokenizando activos–.

La Inteligencia artificial desde el comienzo de las investigaciones potencia las estructuras de gobierno, en particular, las nacidas en blockchain[38]. La fusión de

---

[35] Vid. De Filippi, "Ethereum: Freenet or Skynet?". https://www.guerrillatranslation.org/2014/11/20/ethereum-freenet-or-skynet/

[36] Vid. CAWREY, 37 Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet. CoinDesk. 2014. https://www.coindesk.com/markets/2014/05/20/37coins-plans-worldwide-bitcoin-access-with-sms-based-wallet/

[37] Vid. Cocco, Pinna y Marchesi (2017). "Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. Future Internet", 9:25. https://doi.org/10.3390/fi9030025

[38] Del Castillo (2016). "IBM Watson is working to bring IA to the blockchain" Coinsdesk, April 5. https://www.coindesk.com/markets/2016/04/05/ibm-watson-is-working-to-bring-ai-to-the-blockchain/; Vid. evolución del protagonismo en la IA como mecanismo de adminsitración en Muñoz Pérez (2023), *Las DAOs y el reto de controlar al algoritmo*, Cizur Menor; Kaal (2019), "Blockchain-based corporate governance", Max Plank Institute Luxembourg for procedural Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441904; Calcaterra et al., "Blockchain Infrastructure for Measuring DomainSpecific Reputation in Autonomous Decentralized and Anonymous Systems" (U of St. Thomas (Minnesota) Legal Studies Research Paper núm. 18-11), https://ssrn.com/abstract=3125822; Peltrin, M. (2019). "Corporate Management in the age of AI" UCL *Working Paper Series Corporate Management in the Age of AI*, núm. 3; Mölein, F., "Robots in the Boardroom: Artificial Intelligence and Corporate Law", Woodrow Barfield and Ugo Pagallo (eds.), Research Handbook on the Law of Artificial Intelligence, Edward Elgar (2017/2818, Forthcoming), pp. 665-60; Abriani (2020). "Corporate governance in the era of the algorithm Prolegomena to an impact study of Artificial Intelligence on Corporate Governance", *Rivista Il nuovo diritto delle società*, 3, pp. 261-285; traté este tema en Muñoz Pérez (2020), "La "inteligencia artificial (IA) autónoma" en el órgano de administración", Revista de Derecho de Sociedades, núm. 60; "Inteligencia artificial y los "ciber-consejeros", los miembros robotizados como integrantes del Consejo de administración", Digitalización de sociedades, Carmen Alonso Ledesma y Ana Felicitas Muñoz Pérez (coord.) (2021), ISBN 978-84-18349-90-4,

estas tecnologías señala una inflexión en la última evolución identificada como la "etapa del BORG", cuando la DAO se funde con la IA para generar la Organización Cibernética CybOrg o "BORG", configurando una DAO cibernética "autopoiética" en el ecosistema descentralizado de la Web3, el metaverso y los movimientos DeSci[39]. El usuario poseerá y participará en la propiedad del protocolo –relaciones *peer to peer* y de máquina a máquina–, lo cual revolucionará las relaciones entre personas, empresas y entidades autónomas[40]. En la Web3, los usuarios no serán simplemente beneficiarios de modelos comerciales nuevos, sino "constructores y propietarios de activos" digitalmente únicos, impulsores de dicha tecnología[41].

Los "CybOrg o "BORG'DAOs", en sentido positivo, trasladan los tradicionales valores de la democracia, la paz, la equidad y la sostenibilidad por el acceso

---

pp. 171-190; sobre la implementación de la IA en el entorno de las sociedades tradicionales, vid. Roncero (2019), "BIG DATA y responsabilidad de los administradores de sociedades de capital", *Revolución digital, Derecho Mercantil y Token economía*; Chamorro Domínguez (2020), "La aplicación de sistemas de inteligencia artificial en el seno del órgano de administración de las sociedades de capital", Revista de derecho de sociedades, ISSN 1134-7686, núm. 59.

[39] Delphi Labs, "Assimilating the BORG: A New Framework for CryptoLaw Entities". https://delphilabs.medium.com/assimilating-the-borg-a-new-cryptolegal-framework-for-dao-adjacent-entities-569e54a43f83; interesante descripción en Nabben, "Imagining human-machine futures: blockchain-based "Decentralized Autonomous Organizations" (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953623; Navarro Lerida, "Gobernanza de comunidades en la Web3: el papel de las DAOs", Derecho digital e innovación, núm. 16, abril 2023, Editorial La Ley. La Web1 y la Web2 de forma centralizada ofrecían productos para las personas a través de la monetización de sus datos y la socialización de las pérdidas. En la Web 3.0 las personas podrán acceder a información vinculada rápida y fácilmente impulsada por la tecnología "Blockchain" para permitir las transacciones sin intermediarios, Héctor, Ugarte y Rheinische, "A more pragmatic Web 3.0: Linked Blockchain Data" ["Semantic Blockchain" - Starting Point]. https://www.google.com/search?client=firefox-b-d&q=A+more+pragmatic+Web+3.0%3A+Linked+Blockchain+Data, p. 3, señala la Web 1.0 es la "red de documentos" que servían como portales de información con capacidad básica para vincular sitios web. La Web 2.0 –la "web de las personas" que introdujo a los usuarios a colaborar con la creación y modificación de contenidos–.

[40] Agenda Davos, "How Web3 will level the playing field and unlock income equality". https://www.weforum.org/agenda/2022/05/what-is-web3-why-care-future/; Héctor, Ugarte y Rheinische, "A more pragmatic Web 3.0: Linked Blockchain Data" ["Semantic Blockchain" - Starting Point]. https://www.google.com/search?client=firefox-b d&q=A+more+pragmatic+Web+3.0%3A+Linked+Blockchain+Data, p. 3.

[41] Informe https://www.weforum.org/agenda/2022/05/what-is-web3-why-care-future/

equitativo a la prosperidad y la inserción de los valores ODS[42]. En sentido técnico supone el aprovechamiento de la inteligencia artificial continuando lo que de forma embrionaria se describía en la denominada "entidad algorítmica"[43] para aumentar las potencialidades que caracterizan los nuevos esquemas de gobernanza - "tech-augmented legal entities". Así como los *cy-borgs* ("organismos cibernéticos") de ciencia ficción "aumentan" las facultades de los humanos (personas *naturales*) con órganos y extremidades robóticas o microchips u implantes ópticos, los BORG aumentan las potencialidades de las entidades autorizadas por el estado ("personas *jurídicas*") implementando un "software autónomo" en los estatutos constitutivos, lo que convierte de nuevo al código en el elemento regulador de la entera estructura de gobierno[44]. Algunos preconizan que la IA con ayuda de sofisticadas tecnologías y la simbiosis de ciencias pluridisciplinares –"mapas cognitivos", "redes neuronales"...– alcanzará la "singularidad" en breve periodo de tiempo lo cual señalará un impacto impredecible en la humanidad, las ciencias sociales y un nuevo punto de inflexión en lo que podría denominarse "singularity" DAOs[45].

3.2. Noción y figuras afines

Como venimos señalando, las DAOS tienen el común atributo de ser estructuras de coordinación "autónomas" y "descentralizadas", organizadas sobre la base de una pluralidad de elementos y dirigidas funcionalmente al desarrollo de

---

[42] Navarro Lerida (2023). "Gobernanza de comunidades en la web3: el papel de las DAOs", *Derecho digital e innovación*, núm. 16, abril, Editorial La Ley.

[43] Muñoz Pérez (2023). *Las DAOs y el reto de controlar al algoritmo*, Cizur Menor, capítulo V; LoPUCKI, "Algorithmic Entities", Washington University Law Review, Volume 95I ssue 4. https://openscholarship.wustl.edu/law_lawreview/vol95/iss4/7/, p. 923.

[44] Vid. De Filippi y Wright (2018), *Blockchain and the law: The rule of code*, Harvard, cit. 148; WALCH (2019). "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains", *Regulating Blockchain: Techno-Social and Legal Challenges*, pp. 58 y ss.

[45] Delphi Labs, "Assimilating the BORG: A New Framework for CryptoLaw Entities". https://delphilabs.medium.com/assimilating-the-borg-a-new-cryptolegal-framework-for-dao-adjacent-entities-569e54a43f83; NEWCOMB, un científico afirma que la singularidad llegará en 2031. https://www.esquire.com/es/ciencia/a45801861/cuando-sucedera-singularidad-cientifico-2031/?utm_source=pocket-newtab-es-es

diferentes actividades a través de la implementación de programas en la DLT/blockchain[46].

El fenómeno DAO en el marco de los "blockchain-based business models" define una entidad de gobierno que se sirve de la blockchain para impulsar la "nueva economía tokenizada".

Las DAOs se convierten en los instrumentos para activar las acciones y funciones en el sistema DLT –por regla general en el sistema *permisionless* de Ethereum– y crean, modifican y mantienen sobre el software de código abierto distintas opciones para concretar actividades empresariales. El software de las DAOs ejecuta acciones de forma determinista o programática, integrando en un protocolo una red de contratos inteligentes desplegados en la cadena de bloques –"pública" caso de Ethereum[47]–.

---

[46] Vid. Hassan, Samer y Primavera De Filippi (2021). "Decentralized Autonomous Organization", Internet Policy Review, Vol. 10, núm. 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf, que a partir de 2013, p. 5; Buterin (2014). "DAOs, DACs, DAs and More: An Incomplete Terminology Guide", Ethereum Blog, 4 May. https://blog.ethereum.org/2014/05/06/DAOs-dacs-das-and-more-an-incomplete-terminology-guide/; Nabben, "Imagining human-machine futures: blockchain-based "Decentralized Autonomous Organizations". (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953623; García Rolo (2019). "Challenges in the legal qualificacion of descentralised autonomous organisations (DAOS): the rise of the crypto-partnerchip", R Dtec, pp. 33-87. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3417900; Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/.Keynote Speech by John Glen MP, Economic Secretary to the Treasury, at the Innovate Finance Global Summit during Fintech Week 2022, available at: https://www.gov.uk/government/speeches/keynotespeech-by-john-glen-economic-secretary-to-the-treasury-at-the-innovate-finance-global-summit; Hansard (HC), 7 September 2022, Vol. 719, col 96WH; En nuestra doctrina, Navarro Lerida (2018). "Gobierno corporativo, blockchain y smart contracts. Digitalización de las empresas y nuevos modelos descentralizados (DAOS)", *RMV*, núm. 23, capítulo 11. El poder de decisión societario y "Blockchain" Revolución digital, derecho mercantil y Token economía, María del Carmen de la Orden de la Cruz y Cristina Martínez Laburta (coord.); Ana Felícitas Muñoz Pérez (dir.), 2019, ISBN 978-84-309-7683-6, pp. 287-305. Incluí un primer acercamiento de las DAOs en el entorno de las actividades de financiación en, Muñoz Pérez (2019), *Financiación digital y su incidencia en el gobierno corporativo*, Navarra, p. 133.

[47] Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/, p. 1, *Commodity Futures Trading Commission v Ooki DAO*. https://www.courtlistener.com/docket/65369411/commodity-futures-trading-commission-v-ooki-dao/; "Amicus Curiae brief document" en el caso *Commodity Futures Trading Commission v Ooki DAO (formerly d/b/a bZx DAO)* (Case

La nota de la "Autonomía", se refiere a dicho funcionamiento "predeterminado" por la operativa de los contratos inteligentes que les hace ser "autosuficientes" mediante el cobro de servicios a los usuarios[48]. Las personas se relacionan con un patrón de colaboración gestionados por sistemas de IA. La "autonomía" refiere a la interacción entre los miembros confiada al protocolo –el "código es la ley"–. La "privacidad" de los miembros es otra de sus características, dado que la clave publica se corresponde con otra privada que puede controlar la anonimidad. El rasgo del carácter "distribuido" y "descentralizado" incide en que el control no reside en un solo foco o lugar, pero son caracteres que admiten dimensiones y grados[49].

Hay nociones cercanas –"figuras afines"– que se prestan a confusión con la noción de DAO[50]. Se trata de los "agentes autónomos"-como por ejemplo los virus informáticos que nacidos se cualifican por funcionar de forma independiente-; los "smart contract" –formas simples de programar acciones cuando se cumplen las condiciones de automatización[51]–; los "protocolos" –organización de estructuras que se identifican con la noción de DAOs cuando la pretensión es asumir una actividad de gobierno dirigida a un fin[52]–.

Number 3:22-cv-05416): "Amicus Curiae Brief of LexPunk Regarding Plaintiff's Motion for Alternative Service" (filed 17 October 2022), 2. https://fingfx.thomsonreuters.com/gfx/legaldocs/zdpxolloyvx/frankel-CFTCvbZeroX--lexpunkamicus.pdf

48 Tabone, "Dao: the evolution of organization", Cointelegraph De Filippi "Ethereum: Freenet or Skynet?". https://www.guerrillatranslation.org/2014/11/20/ethereum-freenet-or-skynet/ (2024).

49 Vid. Reyes, Geslevich Packing y Edwards, "Distributed Governance", William & Mary Law Review Online, https://scholarship.law.wm.edu/wmlronline/vol59/iss1/1/, cit. pp. 16 y ss.; vid la nota de la descentralización y la distribución en Muñoz Pérez (2022), "DeFi: la descentralización de las finanzas en blockchain y su controvertida regulación", *Derecho de Sociedades, Concursal y de los Mercados Financieros: libro homenaje al profesor Adolfo Sequeira Martín*, ISBN 978-84-1388-168-3, pp. 869-886, y "Aspectos sobre las finanzas descentralizadas DEFI, protocolo de préstamos", RMV, ISSN 1888-4113, núm. 29, 2021.

50 En el contexto de formas organizativas en sentido amplio están la mencionadas por VITALIK (2014), "DAOs, DACs, DAs and More: An Incomplete Terminology Guide", Ethereum Blog, 4 May. https://blog.ethereum.org/2014/05/06/DAOs-dacs-das-and-more-an-incomplete-terminology-guide/

51 Guillaume y Riva (2022). "How to Resolve a Dispute Involving A DAO". https://sites.duke.edu/thefinregblog/2022/07/21/how-to-resolve-a-dispute-involving-a-dao/

52 Kerr y Jennings. "A Legal framework for decentralized Autonomous Organizations". https://www.researchhub.com/paper/1268581/a-legal-framework-for-decentralized-autonomous-organizations, p. 10.

El termino DAO suele reservarse para las "organizaciones" con miembros poseedores de tokens en una estructura de gobierno y "participes" poseedores de tokens de liquidez que reciben el beneficio de los resultados[53]. La tecnología se convierte en un atractivo para las empresas[54] proponiendo innovadores modelos y un entorno expansivo con un enorme potencial de futuro[55].

3.3. Daos no reguladas

3.3.1. *La falta de consenso en Europa para regular las DAOs en MICA*

La posición negociadora adoptada por el Comité de Asuntos Económicos y Monetarios del Parlamento Europeo el 14 de marzo de 2022, en el marco de elaboración del Reglamento de mercados de criptoactivos de MICA, modificó el borrador original para incluir disposiciones dirigidas a regular las DAOs, iniciativa que suprimió en la versión final[56].

El Parlamento Europeo, proponía añadir un nuevo considerando para reconocer que "algunos tipos de criptoactivos no son emitidos por personas jurídicas, sino que son gestionados por organizaciones autónomas descentralizadas" [Considerando 13(a)]. En particular, se incluía la definición legal de DAOs, como un sistema organizativo basado en reglas que no estaban controladas por ninguna autoridad central y cuyas pautas estaban completamente enrutadas en su algoritmo [art. 3(1) (1a)]. Las DAOs deberían ser admitidas para "ofrecer criptoactivos al público" o "solicitar la admisión de dichos criptoactivos a negociación en una plataforma de negociación de criptoactivos". El Parlamento Europeo propuso

---

53 Vid. Las nociones en Hassan, Samer y Primavera De Filippi (2021), "Decentralized Autonomous Organization", *Internet Policy Review*, Vol. 10, núm 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf; Troncoso y Utratiel, "If I Only Had a Heart: A DisCO Manifesto. DisCO", 2019. https://disco.coop/manifestó

54 Vid. "Databroker DAO". https://firebasestorage.googleapis.com/v0/b/databrokerdao-presale.appspot.com/o/WHITEPAPER_DataBrokerDAO_ENG_v1.2.pdf?alt=media&token=444bb292-d86b-4698-9cd9-06d434459eaa

55 Llyr, Re-envisioning corporations: How DAOs and blockchain can improve the way we organize, Davos agenda, 2022, Head of Blockchain and Digital Assets, CISA, World Economic Forum; Wright (2021). "The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges", Stanford Journal of Blockchain Law & Policy, Jun 30, p. 163.

56 European Parliament (2022). "Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937", COM(2020)0593 - C9 0306/2020 - 2020/0265 (COD).

encomendar a las autoridades competentes la tarea de garantizar que las DAOs cumplieran con todos los requisitos establecidos en la regulación para otros criptoactivos –como la notificación y publicación de un libro blanco apropiado, así como el régimen de autorización– [art. 3(b)].

Sin embargo, la iniciativa de reforma no fue incorporada en la versión final aprobada del Parlamento Europeo y el Consejo una vez alcanzado el acuerdo político provisional el 30 de junio de 2022[57]. Después del acuerdo político de octubre de 2022, MiCA ya no menciona específicamente a las DAO, motivo por el que quedaron excluidas de dicho reglamento comunitario a pesar de que siguen funcionando en la *praxis* y las acciones de sus miembros pueden tener consecuencias legales. Se alega que si las DAO –aunque no estén completamente descentralizadas–, emiten tokens clasificados como criptoactivos y proporcionan servicios que entran dentro del alcance de MiCA, deberían de forma consecuente cumplir con los requisitos de dicha normativa.

A medida que MiCA sea aplicable –finales de 2024–, consideramos oportuno que en las propuestas que algunos expertos avanzan de la revisión del reglamento se incluya una regulación europea que dote a estas estructuras de un reconocimiento legal. El otorgamiento de reconocimiento legal a ciertas DAOs y la dotación del atributo de la personalidad jurídica ayudaría para crear un estatus legal claro, que garantice un nivel de protección de los intereses de terceros, en particular los externos, equivalentes o equiparables a los que gozan las partes en el marco de la actividad de una "persona jurídica"[58].

3.3.2. *El funcionamiento "de hecho" como sistemas de gobierno*

3.3.2.1. *Consideraciones previas*

La DAO funciona en la praxis como modelo de gobierno para la coordinación de actividades de sus miembros a través de programas o reglas autoejecutables

---

[57] European Commission (2020). "Proposal for a Regulation on Markets in Crypto-assets and amending Directive (EU) 2019/1937COM/2020/593 final", 2020/0265(COD) vid. European Council, "Digital finance: agreement reached on European crypto-assets regulation (MiCA)" (30 June 2022).

[58] A estos efectos, son de particular interés los esfuerzos previos del grupo de investigación, COALA, *Model Law for Decentralized Autonomous Organizations*. https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf

implementadas en el software en una red de blockchain[59]. Por esto podría hablarse de una entidad que funciona "de hecho"[60].

El principio básico de regulación es el "código", es decir, el "contrato" como norma para disciplinar el funcionamiento[61]. En política jurídica, implica la total "contractualización" del modelo, que supone añadir al tradicional debate societario que enfrenta a contractualistas e institucionalistas, la dimensión de la "predeterminación", es decir, la exigencia de investigar si es posible configurar todos los eventuales "escenarios simulados" por anticipado para "modelizar su algoritmo"[62].

Pronto se advierte que los contratos "auto-aplicables" en código abierto generan el riesgo, por una parte, de crear estructuras para ejercer el poder "totalitario" por obligar a todos a cumplir las reglas –"el código"– sin ninguna restricción constitucional[63] y por otra, que los "códigos" son "incompletos", al menos en su actual desarrollo, por ser incapaces de crear esquemas de funcionamiento que

---

59 Navarro Lerida (2018). "Gobierno corporativo, blockchain y smart contracts. Digitalización de las empresas y nuevos modelos descentralizados (DAOS)", *RMV*, núm. 23, 1-20; MUÑOZ PÉREZ (2023). Las DAOs y el reto de controlar al algoritmo, Cizur Menor. En doctrina comparada, Hassan, S. y De Filippi, P. (2021). "Decentralized autonomous organization", *Internet Policy Review* (IPR), Vol. 10, núm. 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf; Galaxy Fund Management (2022). "What are DAOs?". https://www.galaxyfundmanagement.com/crypto-101/what-are-DAOs; Gogel, Kremer, Slavin y Werbach, "Decentralized Autonomous Organizations: Beyond the Hype", WEF, Whitepaper, 2022; Borgogno y Martino (2024). "Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype", núm. 161. EBI, Working paper series, p. 33.

60 Las denominan bajo diferentes expresiones (Marverick Daos, "Pure" DAOs, "Unregulated DAOs) para hacer referencia a un fenómeno similar cuya consecuencia en el ámbito legal se reconduce al ámbito de la atipicidad con consecuencias no del todo claras (Vid. LAW COMMISSION, "Decentralised autonomous organizations (DAOs). A scoping paper", 2024, pp. 29 y ss., "Decentralised autonomous organizations (DAOs). Scoping paper", pp. 56 y 63 aludiendo a la alternativa de calificarlo como "Partnership" o bien como "unincorporated association", en función del propósito empresarial lucrativo -"Partnership"-o no -"unincorporated association"-; que conlleva la principal diferencia en torno a la responsabilidad por los propios actos o los actos de los que los representan; Como "unincorporated association" la actuacion de los miembros no conlleva responsabilidades recíprocas como si es obligado en el marco de la "partnership", régimen que se construye sobre la trascendencia jurídica de la vinculación de un "Smart contract".

61 Walch, "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains", in Regulating Blockchain: Techno-Social and Legal Challenges, 2019, pp. 58 y ss.

62 Vid. estas consideraciones en COALA, *Model Law for Decentralized Autonomous Organizations*. https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf

63 Hassan, S. y De Filippi, P. (2021). "Decentralized autonomous organization", *Internet Policy Review* (IPR), Vol. 10, núm. 2. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf

abarquen de forma global cualquier hipótesis de actuación. La inteligencia artificial, en estas últimas consideraciones, está abriendo nuevas potencialidades[64].

El esquema de un software para organizar la DAO es eminentemente "contractual" y, por esto, cuando está desprovista de cobertura legal genera los problemas analizados por la doctrina societaria tradicional. Son clásicos los debates entre "contractualistas" e "institucionalistas" en la construcción e interpretación del régimen de las sociedades y las dificultades allí examinadas comparten paralelos argumentos a los que deben fundar la construcción del régimen de la DAO[65]–. El funcionamiento de las DAOs, como los modelos contractuales de sociedad, se revelan particularmente complicados; en frenar a los acreedores de los socios para la garantía de la autonomía patrimonial –"entity shielding"–; en la defensa de la tutela de los terceros frente a las actuaciones de la entidad; en aclarar el esquema de la responsabilidad general de todos –entidad y miembros– en particular frente a los terceros extracontractuales[66].

El carácter "descentralizado" es idóneo para democratizar estructuras e integrar criterios plurales, pero los mecanismos de gobernanza que hasta ahora se han implementado en las DAOs no consiguen desarrollar estos atributos plenamente[67]. Las innovaciones en los mecanismos de administración no evitan en su funcionamiento el "riesgo esencial de centralización" del control.

Los "clásicos problemas societarios", se extienden en la DAO con razonamientos paralelos también en otros aspectos. Por ejemplo, la exigencia de proteger la minoría, en la DAO se explica en el riesgo de la actividad de partícipes llamados "ballenas" por ser titulares de grandes paquetes de tokens –"Whales"–. Los miembros al "abandonar el juego" por enfado –"*Ragequit*"– en el contexto de

---

[64] Muñoz Pérez. "Algunas consideraciones sobre la convergencia de las tecnologías de Blockchain e IA" (en prensa).

[65] Rohr y Wright (2019). "Blockchains, private ordering and the future of governance", Hacker, Lianos y Dimitropoulos (dirs.), *Regulating blockchain. Techno-social and legal challengues*, UK.

[66] Jentzsch, C, *Decentralized Autonomous Organization to Automate Governance*. https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf

[67] A este fin se tienen en cuenta los estudios que detallan las propiedades de la descentralización. Algunos señalan las dimensiones para dicha evaluación en las DAOs, partiendo de la votación ponderada por tokens, elementos de la infraestructura y gobernanza, entre otros factores, vid. Axelsen, Jensen y Ross, "When is a DAO Decentralized?". Complex Systems Informatics and Modeling Quarterly 31 (2022): 51-75.

la DAO están ocasionando el ejercicio de un "derecho de separación" "*ad nutum*". Las *bifurcaciones contenciosas duras* en el ámbito de la infraestructura donde se apoya el funcionamiento de la DAO suponen una "exclusión de facto" para los "nodos" que, ante decisión de no actualizar, permanecer en la red antigua y quedan expulsados de la nueva. Pero si el cambio propuesto es polémico y suficientes nodos eligen renunciar a la actualización, la red original, en lugar de la red actualizada, podría considerarse la red principal. En ambos casos, habría que determinar el alcance de estas operaciones sobre la DAO que está implementada en su estructura[68]. Por último, el modelo no cierra la determinación de la responsabilidad que se agrava por la circunstancia del carácter "seudo-anómino de los Token holders", la presencia masiva de tenedores.

El "apatía" de los "token-holders" usuarios –denominada "fatiga"– origina el bloqueo del funcionamiento de la DAO. El sistema de "votos" se basa en "incentivos", es decir, mecanismos para "implicar" y "comprometer" a los partícipes de la DAO y evitar el natural desinterés de la "masa" que olvidado pronto el ánimo que les incentivaba la incorporación abandonan el "sentido de comunidad". En ocasiones, las propuestas son complicadas desde un punto de vista de político y económico. Por ejemplo, hay sistemas de incentivos que proponen otorgar retribuciones en los sistemas de consenso "poof of stake" (POS) al "ganador de las apuestas" –"staking"– premiando los aciertos. Esto ocasiona el riesgo "político" de la manipular los votos ligados a los tokens bloqueados en depósito y el riesgo financiero de generar iliquidez en la organización por carencia de tokens en circulación, lo que bloque el funcionamiento de todo el sistema.

La "fatiga" se convierte en el fundamento que justifica la investigación en nuevos sistemas de IA. Fomentan las capacidades que refuerzan el funcionamiento autónomo de la DAO y los procesos de "decisión-taking" con el fin de aligerar la gestión de los asuntos de la entidad, dando mayor protagonismo a la Inteligencia

---

68 Seira, Allen, Watsky y Alley (2024). "Governance of Permissionless Blockchain Networks", February 09. https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html

Artifical[69]. Dicha evolución viene implícita en el nacimiento de los BORG antes mencionados[70].

La implicación de los "developers" en la gestación de la estructura y la frecuencia con la que éstos se convierten en los principales receptores de los tokens creados en la fundación de las DAO, les sitúa en la delicada posición de potencial conflicto de interés similar al que presentan los fundadores en los esquemas societarios financiados por "venture capital". Los fundadores –"deveppers"– cuentan con *información privilegiada* que ocasiona un particular riesgo propio del entorno de las actividades de capital riesgo. En efecto, los fundadores expertos en el negocio que impulsan pueden aprovechar dicho conocimiento técnico en su favor adoptando decisiones en propio interés. Incluso algunos abandonan el proyecto cuando intuyen que no tendrá éxito o lo destinan al fracaso. La ciencia computacional tan complicada de las DAOs incrementa las ocasiones de cometer delitos, por ejemplo, dejando fallos de programación –"bugs"– de forma premeditada para "salir por la puerta de atrás" y sustraer los fondos de la cuenta "treasury"[71].

3.3.2.2. *La fundación. Colocación de tokens y asignación de recursos*

El proceso de fundación surge de la implementación del protocolo a través de una aplicación descentralizada (dApp) que sirve para concretar el destino y la aplicación de los fondos de inversión tokenizados mediante la dotación de la cuenta "treasury"[72].

---

[69] Lumineau, Wang y Schilke (2019). Blockchain Governance - A New Way of Organizing Collaborations? (2021), subraya la importancia del automatismo, basados en emcanismo de administracion automática, en el sentido de las elaboradas por Kaal, "Blockchain-based corporate governance", Max Plank Institute Luxembourg for procedural Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441904; Calcaterra et al., "Blockchain Infrastructure for Measuring DomainSpecific Reputation in Autonomous Decentralized and Anonymous Systems" (U. of St. Thomas (Minnesota) Legal Studies Research Paper núm. 18-11). https://ssrn.com/abstract=3125822; CALCATERRA, "On-chain govenance of decentalized Autonomous Organizations", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188374 (2018)

[70] Delphi Labs. "Assimilating the BORG: A New Framework for CryptoLaw Entities". https://delphilabs.medium.com/assimilating-the-borg-a-new-cryptolegal-framework-for-dao-adjacent-entities-569e54a43f83

[71] Caliskan. "The rise and fall of Electra: emergence and transformation of a global cryptocurrency community", SSRN-id4239199-1.pdf.

[72] Vid. Kerr y Jennings, "A Legal Framework for Decentralized Autonomous Organizations", https://api.a16zcrypto.com/wp-content/uploads/2022/06/dao-legal-framework-part-1.pdf; consultar el íntegro proceso de funcionamiento en Pupyshev, Sapranidi y Khalilov, "Pathway:

Cuando se fundan, las empresas desarrolladoras suelen retener el control sobre ciertos aspectos de los contratos inteligentes para supervisar las operaciones del protocolo mientras se va consiguiendo una base inicial de usuarios y se hace posible la adición de nuevas funciones con el tiempo.

Una vez que se activan los contratos "inteligentes de gobernanza", el control del protocolo pasa de los desarrolladores a los titulares de los tokens de gobernanza y aprovechan a distribuir tokens a los usuarios del protocolo a través de un "airdrop" y a los empleados, accionistas y asesores de la corporación desarrolladora conforme a lo pactado en el acuerdo de fundación, quedando otros retenidos en la tesorería por la corporación desarrolladora para uso futuro, creando así la cuenta de la "treasure" de la DAO.

Señala TABONE[73], que las DAOs prototípicas suelen segregar los derechos políticos y los económicos en "Tokens de gobernanza" –para atribuir el gobierno de la red o del protocolo de software, considerados "activos" de valor a pesar de que no confieren, en ocasiones, la participación en los rendimientos de la DAO[74]– y "tokens de liquidez" –para ligar y atribuir los rendimientos económicos[75]–. Aunque la funcionalidad de los tokens de gobernanza y los contratos inteligentes de gobernanza varían para cada DAO, estos tokens proporcionan un medio para la formulación de propuestas y votación sobre éstas y para controlar las decisiones operativas de la DAO, también para modificar los contratos inteligentes del protocolo subyacente de la DAO.

Los *Smart contracts* que contienen el código de organización, también incluyen las reglas para la asignación de "tokens de gobernanza" –GTs–. Por regla general contempla una asignación inicial –bloque génesis– mediante reparto a los *wallets* de desarrolladores y otros usuarios para que participen en el gobierno e impulsen una definida actividad. Con frecuencia determinan la ejecución del voto según sistemas creados "*off-chain*" (es decir, fuera de la cadena) aunque últimamente hay un esfuerzo para incorporarlos "*on-chain*" (en la cadena) por considerar que

---

a protocol for algorithmic pricing of a DAO governance token" (2022). https://arxiv.org/pdf/2202.06541.

[73] Tabone, "Dao: the evolution of organization", Cointelegraph, p. 2.

[74] Vid. Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/, p. 55.

[75] Vid Galaxy Fund Management (2022). "What are DAOs?". https://www.galaxyfundmanagement.com/crypto-101/what-are-DAOs

consiguen mayor autonomía para la organización. Es posible que la distribución sea posterior –"*on going distribution*"– mediante operaciones de reparto de nuevos tokens que se generan por reglas diferentes atendiendo a los tipos de red e incentivos –ej. por "Minería" en forma de recompensa a los mineros por verificar transacciones y agregar nuevos bloques a la blockchain–; en operaciones de recompensa por "Staking" –a los usuarios que "apuestan" o depositan los tokens si su apuesta es exitosa–; por "Airdrops"– por las que el proyecto distribuye tokens de forma gratuita a los usuarios de la red para incentivar la participación y el uso de la plataforma–; o por la "venta de tokens"–donde los proyectos pueden realizar una ICO o IEO para vender tokens al público, procedimiento que se acompaña de la elaboración del "Whitepaper" donde se concreta las condiciones de suscripción por susbasta –*auction*– en las denominadas operaciones –*initial coin offering* "ICO"/Security Token offering, "STO"–.También los Tokens de liquidez se pueden "quemar" –burned– para rescatar la participación y parte de estos pueden negociados en mercados secundarios DEX (AMM).

La creación de estos tokens democratiza el mercado financiero dada la condición de ser medios de financiación en masa –"crowfunding"–.

Los tokens pasan a ser "propiedad" de aquellos que poseen la clave privada y quedan en posición anónima, identificados por la correspondiente a la "dirección pública" que refiere a la DAO.

Siguiendo la definición del token y observando el paralelismo al derecho de sociedades se dirá que las estructuras DAO y los tokens pueden responder a dos formas básicas –personalistas y de capital– según se participe con *token-based membership*– o bien –*share-based membership*[76]–. Las segundas requieren la constitución de una "DAO formal", en el sentido de que el régimen se estipula en el "envoltorio" de una "legal wrappers" para "embeber" el fenómeno en la disciplina imperativa un tipo de Sociedad de capital[77]. No se trata del tokenizar el mero registro de las acciones o los accionistas de una sociedad de capital

---

[76] Federal Council Report (2018). "Legal gramework for distributed ledger tecnology and blockchain in Switzerland", cit. p. 48.

[77] Aun asi, no queda exenta de duda como cabe apreciar del reciente caso, Zhou "DAOs vs. Nation States: A Wyoming DAO's Experiment with the U.S. Securities and Exchange Commission". https://blogs.law.ox.ac.uk/oblb/blog-post/2024/03/daos-vs-nation-states-wyoming-daos-experiment-us-securities-and-exchange.

en una blockchain para dar transparencia de las titularidades o el ejercicio de los derechos de voto. Entiendo que este limitado propósito sería insuficiente para calificar estos "criptoactivos" como "instrumentos financieros" que incorporen las posiciones de la DAO en el sentido que venimos desarrollando. Solo la promulgación de una "legal wraper" para dotar de estructura de capital a la DAO, o la disposición de un régimen *ad hoc* que defina un esquema normativo expreso a una DAO conseguiría este alcance. El "token" que simplemente "registra" o "legitima" titularidades tienen menor alcance que la de incorporación de la posición de socio en una organización societaria. Caso aparte podría ser el valor de "tokenizar acciones" que en el marco de "pactos para-sociales" proporcionen utilidades singulares, como ejercicio del voto. Se identifica esta opción cuando se afirma, "The linking of a token to membership in a company is binding only on the parties and cannot be asserted against a third party"[78].

3.3.2.3. *La administración en un gobierno "descentralizado" y "autónomo"*

Las DAOs proponen la ventaja de basar la administración en un sistema descentralizado y autónomo[79]. La "descentralización" se detalla en las dimensiones "arquitectónica" –cantidad de computadoras que componen el sistema–, "política" –cantidad de controles que controlan esas computadoras–; y "lógica" –como la forma en que la interfaz y las estructuras de datos se suman–. El diseño de la DAO es descentralizado cuando es resistente a la colusión, por ofrecer un equilibrio a largo plazo e implementar procesos transparentes y generalmente abiertos de gobernanza[80].

La autonomía hace referencia, bien a la capacidad de autogobierno basados en software que permite funcionamiento automático, bien a ser resistentes a la

---

[78] Federal Council Report (2018). "Legal gramework for distributed ledger tecnology and blockchain in Switzerland", p. 49.

[79] Diallo, Shi, Xu, Gao, Chen, Lu, Shah et al. "eGovDAO: A better government using blockchain based decentralized autonomous organization". En 2018 International Conference on eDemocracy & eGovernment (ICEDEG). IEEE, (2018). https://letonchanh.github.io/files/icedeg18.pdf, p. 1.

[80] Axelsen, Jensen y Ross, "When is a DAO Decentralized?". Complex Systems Informatics and Modeling Quarterly 31 (2022), p. 6; sobre el carácter de la descentralizacion, vid. JENNINGS/HOROWITZ, "Principles & Models of Web3 Decentralization", a16zcrypto.com, https://d1lamhf6l6yk6d.cloudfront.net/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf.

censura o el control de terceros[81]. Los *Smart contracts* contienen el código de dichas organizaciones y definen la asignación de tokens de gobernanza –GTs–, a los desarrolladores y los usuarios para que participen en el gobierno e impulsen una definida actividad mediante sistemas de votos "on-chain" y "off-chain" de la entidad. Por ejemplo, "Aragon Govern" es un software ofrecido por AragonDAO para crear y gobernar organizaciones con proyectos para el desarrollo de actividades financieras (DeFi) de código abierto para organizaciones sin fines de lucro, clubes, y empresas de cualquier tipo de organización. Por ejemplo, The DAO creó el formato de archivo ERC-3000, estándar para la votación vinculante "off the chain" fuera de la cadena y reúne, por esta razón, ciertos elementos de centralización al acudir fuera de la red. La descentralización se preserva mejor en los diseños de gobierno de las DAO "on the chain" dirigidos a compensar la falta de dirección jerárquica por creativas opciones de "incentivos" encaminadas a conseguir sistemas de gobiernos descentralizados eficientes –por ejemplo, los denominados "Commons-Based Peer Production (CBPP)"[82]–. Los protocolos automáticos son capaces de programar acciones "en tiempo real" sobre la base del automático *feed back* recibido de la medida implementada –*dynamics feedback loops*– convirtiendo el automatismo en el principal atributo de su eficiencia. El "protocolo de gobierno dinámico" crea actualizaciones en tiempo real a través de bucles de retroalimentación dinámicos[83]. Los mecanismos más sofisticados en este sentido llevan a la configuración de las denominadas "DAOs

---

[81] Vid. alcance de la autonomía en Nabben, "Imagining human-machine futures: blockchain-based "Decentralized Autonomous Organizations" (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953623, p. 6, en particular, las referencias al proyecto de la "singularity net", https://singularitynet.io/research-initiatives/.

[82] Vid. ejemplos en Rozas, Tenorio-Fornés, Díaz-Molina y Hassan, "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance." Sage Open 11, núm. 1 (2021). https://doi.org/10.1177/21582440211002526

[83] Expone Kaal (2019). "Blockchain-based corporate governance", Max Plank Institute Luxembourg for procedural Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441904, p. 31, que las DAO pueden generar reglas mayoritarias *ex-post* sin necesidad de que estas reglas mayoritarias sean dispuesta *ex-ante* y funcionan como mecanismos de "retroalimentación descentralizada". Cabe afirmar que las reglas mayoritarias *ex-post* basadas en código no están sujetas a las mismas asimetrías de información que las reglas *ex-ante* que se disponen con carácter estable y presuntamente de forma óptima. Wright las denomina algoritmicas en "The rise of decentralized autonomous organizations: Opportunities and challenges". Stan. J. Blockchain L. & Pol'y 4 (2020). https://stanfordjblp.pubpub.org/pub/rise-of-daos

algorítmicas"[84]. Con los mecanismos dinámicos de gobierno de las DAOs, los poseedores de tokens de DAO pueden votar por un cambio de cualquier código obsoleto o defectuoso a medida que se materializan los defectos o en previsión de futuras contingencias. De esta forma, la infraestructura tecnológica que sustenta las DAO en una blockchain permite continuas actualizaciones a través de los contratos inteligentes sin superar el carácter de ser programas "incompletos" por la incapacidad a pesar de las mencionadas actualizaciones de contemplar todos los escenarios posibles.

3.3.3. *Tratamiento jurisprudencial*

Las partes de un contrato de organización que no tienen definida la estructura ni tienen cobertura legal exponen a sus miembros a la responsabilidad ilimitada según criterio de la doctrina y la jurisprudencia de los organismos de supervisión que comienzan a pronunciarse de forma reciente[85].

Los programadores eliminan la trascendencia de la responsabilidad ilimitada con el argumento de que los programas inteligentes tienen pre-programados todos los esquemas incluso la previsión de las eventuales indemnizaciones para las hipotéticas lesiones[86] causadas a futuro que vienen solucionadas determinando los siniestros y los mecanismos de compensación que lo restauren, de lo que se colige que no es necesario desencadenar régimen de responsabilidad por ser inexistente el presupuesto[87].

---

[84] Explica Kaal, "Blockchain-based corporate governance", Max Plank Institute Luxembourg for procedural Law (2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441904, p. 12, que esta idea surgió del problema que nació en el proyecto de "The DAO" cuando los programadores tuvieron problemas para reactualizar el programa para evitar el hackeo de la red, dado que la condición de entidad descentralizada impedía esta actuación. El problema que en aquel caso se solucionó con la figura del curator, al que precisamente se acusaba al inicio considerando que representaba la centralización de poderes en "The Dao".

[85] *Commodity Futures Trading Commision v. OokiDAO*, el documento "Order concluding that service has been achieved", ase núm. 3:22-cv-05416-WHO; Mattila, Dwivedi, Gauri y Ahbab. "Mapping out the DAO Ecosystem and Assessing DAO Autonomy" (2022). https://www.researchgate.net/publication/358694594

[86] Vid las estudiadas, a modo de ejemplo, en el documento de COALA para solucionar las hipotéticas actuaciones en conflicto de interés de los que administran la DAO en COALA, Model Law for Decentralized Autonomous Organizations. https://coala.global/wp-content/uploads/2022/03/DAO-Model-Law.pdf.

[87] Borgogno (2022). "Making decentralized autonomous organizations (DAOs) fit for legal life: mind the gap", Questioni di Economia e Finanza, Banca d´Italia. https://www.bancaditalia.it, p. 12.

Por otra parte, alegan que la DAO no tiene "subjetivación" "ni existencia", ya que se trata de una colección de *scripts* informáticos en la cadena de bloques, por regla general, Ethereum[88].

Sin embargo, la práxis ha demostrado lo contrario. Las DAOs pueden inferir daños a los usuarios como terceros sujetos vinculados a su funcionamiento y los tribunales se enfrentan a la necesidad de pronunciarse lo que va generando en la doctrina la tendencia de asimilar la hipótesis al fenómeno de expresión de una sociedad y buscar en este entorno la solución del régimen a aplicar.

Cuando la DAO no se funda en el envoltorio de alguna norma –"legal wrapper"–los supervisores orientan la búsqueda de las normas en el ámbito de las sociedades lo que ocasiona el riesgo de "re-caracterización de los tokens". Asimilando el fenómeno organizativo a una entidad de "hecho", se impone el régimen legal de las entidades no inscritas –"an unincorporated association"– convirtiendo a ciertos partícipes en "miembro/s responsable/s de la DAO" y tratados como "socios generales" por involucrarse en el gobierno de la estructura[89]. La responsabilidad ilimitada por las actuaciones lesivas se aplica, en contra del código del contrato inteligente que predica el control de todas las hipótesis de funcionamiento, previsión que excluye que se pueda incurrir en un supuesto de responsabilidad por la actividad.

Participo de la opinión de aquellos que consideran que sin las protecciones que proporciona la inclusión de la DAO en un "legal wrapper", o la creación expresa de un "esquema normativo ad hoc" (estudiadas seguidamente en el epígrafe 3.4), aprobado con el expreso fin de limitar la responsabilidad, la configuración de la organización no puede confiarse "por entero" al código, en particular, aquellos aspectos que suponen el perjuicio de intereses de terceros.

La señalada opinión es participada por la estrategia de la Comisión de Comercio de Futuros de Productos Básicos (CFTC) de Estados Unidos en el caso de Ooki DAO, en la que se presentó una demanda contra una DAO –Ooki DAO–, por operar "sin licencia" en un mercado de derivados –swaps de criptomonedas–

---

88 Vid. Infome Amicus Lexpunk, p. 9 e "Infome Amicus, Paradigm operations LP, p. 2, "DAOs can in fact leverage traditional corporate entities that can be held liable".

89 Borgogno (2022). "Making decentralized autonomous organizations (DAOs) fit for legal life: mind the gap", Questioni di Economia e Finanza, Banca d´Italia. https://www.bancaditalia.it, p. 12.

descentralizado (DEX). La demanda también acusa a Okii DAO de no tener medidas para prevenir el fraude y la manipulación del mercado. La solución presentada por el organismo supervisor pasa por imponer el régimen de la "asociación no incorporada" a la entidad con el fin de imputar a los titulares de tokens de control de la gobernanza de la DAO de ciertas responsabilidades frente al resto de los "usuarios" de los protocolos –usuarios del entorno de las finanzas descentralizadas, DeFi[90]–. Aplicando la ley de California, Ooki DAO –según la CFTC– es un "grupo de dos o más personas" unidas por expresión de un "consentimiento mutuo" para un "propósito legal común" y que "funciona bajo un nombre común" en circunstancias en las que la equidad requiere que el grupo sea reconocido como una entidad legal[91]. El fin de lucro, caracterizaba la organización que se planteaba usar y distribuir los fondos generados por la actividad desde la cuenta *treasury*[92]. En el informe *amicus* de LexpunK alegaba en contra que la DAO no estaba incluida en la noción de una "asociación", por ser un simple software autónomo. Sólo las "DAOs Legalwrappers", que gozan de personalidad jurídica a través del expediente de la sociedad tradicional que la envuelve, podrían adquirir esta condición[93]. El 20 de diciembre del 2020, el tribunal rechazó esta

---

[90] La US Commodity Futures Trading Commission (CFTC) aplicó este criterio en el análisis legal de Ooki DAO. Los miembros de la "unincorporated association" fue definido por la CFTC como aquellos tenedores de tokens de Ooki que habían votado en las propuestas con respecto a los negocios en curso. https://www.cftc.gov/PressRoom/PressReleases/8590-22

[91] Versión sostenida en demanda *Commodity Futures Trading Commision v. OokiDAO*, el documento "Order concluding that service has been achieved", ase núm. 3:22-cv-05416-WHO, pp. 7 y ss.

[92] El control de la LLC fue transferido a Ooki DAO. La CFTC podría haber demandado a la LLC –la entidad predecesora de la DAO por el control del protocolo bZeroX–, que otorgaba a los socios de control la posibilidad de realizar cambios en el software y decidir la distribución de beneficios (que defraudaba a los usuarios), así como efectuar cambios en el control del software a través de la administración de las llaves. Puesto que el control se había cedido a Ooki DAO, la CFCT demandó a la "organización" Ooki DAO por las decisiones adoptadas colectivamente por los titulares de tokens de la DAO (p.7 CFTC v OokiDAO). La noción de unincorprated association, se remite a la de un grupo voluntario de personas que sin escritura de mutuo acuerdo se proponen en desarrollo de un fin común (762 F 3d 921, 927, 9th Cir. 2014) está presente en las sentencias *Comm. For Idaho´s Hight Desert, Inc. v. Yost*, 92 F.3d 814, 820 (9th Cir. 1996) y en *Cal. Darts Ass´n* 762 F.3d en 927.

[93] Vid. Infome Amicus Lexpunk, p. 9 e "Infome Amicus, Paradigm operations LP, p. 2. "DAOs can in fact leverage traditional corporate entities that can be held liable". BRUMMER y SEIRA, "Legal wrapper and DAOs, 2022, (6-9). Según El Corp. Cod. Californiano una "unincorporated association" es un grupo de dos o más personas que consienten en desarrollar en común de

oposición de manera sumaria[94] y, finalmente, los tribunales legitimaron la orden administrativa de la CFTC que determinaba que los "fundadores de bZeroX" eran responsables como personas controladoras del protocolo y como miembros de Ooki DAO de cualquier deuda que surgiera por las violaciones de la normativa de valores por parte de Ooki DAO[95].

En último extremo cabría preguntarse si la imputación de responsabilidad ilimitada a muchos partícipes por pequeños importes –como suelen ser los casos de *crowfunding*– añade tutela en favor de los instantes de responsabilidad, puesto que dicha demanda plural suele ser ineficiente en términos económicos.

3.4. Iniciativas de regulación

3.4.1. *Planteamiento*

Los recientes pronunciamientos de la doctrina y la jurisprudencia en la línea de considerar las DAOs sin regular en el entorno de la noción de los contratos societarios revestidos de notas personalistas –"Partnerships"– (en contra de lo pretendido por los "desarrolladores" y miembros de considerar que los esquemas de organización son "a-legales"[96] por estar "no normados" y por ello, de incierta responsabilidad), ha suscitado el interés por regular el fenómeno. La opción de ser DAOs "no formales" ofrece el riesgo de ser "re-caracterizadas" y reconducidas al régimen imperativo de la "Partnership", sociedades contractuales en su forma más básica, e imponer sobre la estructura un complejo régimen de responsabilidad[97].

Se han desarrollado varias tendencias que forman parte de una especie de crisis de identidad o crisis existencial que actualmente inciden en las DAO, que les ha hecho evolucionar hasta convertirse en empresas complejas fuera de la cadena,

---

un propósito, tenga o no fin de lucro (Cal. Corp.Code & 18035). Son elementos de la noción la existencia de "grupo de personas", "consentimiento" y "fin común"y Amicus de PARA.MOT (pp. 17-23).

[94] *Commodity Futures Trading Commision v. OokiDAO*, el documento "Order concluding that service has been achieved", ase núm. 3:22-cv-05416-WHO.

[95] "Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory", 9 Junio 2023. https://www.cftc.gov/PressRoom/PressReleases/8715-23

[96] Lindahl (2013). *Fault Lines of Globalization: Legal Order and the Politics of A-Legality*, Oxford University Press.

[97] Rosenberg (2022). 'Getting down with DAOs: Decentralised Autonomous Organizations in Bankruptcy', 41 American Bankruptcy Institute Journal 12.

que no cumplen con las normas y que colocan a sus participantes en un riesgo legal extremo. A pesar de llamarse DAOs no son autónomos ni descentralizados, lo que crea una extrema confusión y exacerban los problemas legales[98].

Sólo es factible conseguir cierta seguridad en la determinación del tipo y la limitación de responsabilidad si el legislador la otorga expresamente, debatiendo con argumentos clásicos societarios, la posibilidad de blindar contractualmente la responsabilidad de los miembros de la organización y del patrimonio social[99].

La propuesta de dotarles de seguridad jurídica lleva a la creación de "legal wrapers" –sobre el principio de extender los efectos de la personalidad jurídica del "envoltorio legal" a los partícipes de los contratos inteligentes/protocolos de software[100]–. En otros casos –como la mencionada propuesta del grupo de investigación Coala–, las propuestas se dirigen a la configuración de un régimen legislativo "ad hoc" para resolver la incertidumbre legal[101].

Anticipamos que, aun así ("legal wrapper" o régimen expreso), subsiste cierto riesgo legal. Recientes estudios doctrinales sobre la base de los pronunciamientos de la SEC, siguen denunciando inseguridad jurídica[102]. A pesar de la intención clarificadora del legislador dictando adaptaciones en el régimen de las sociedades típicas para que las DAOs queden "envueltas" en las denominadas "legal wraper", la SEC duda del carácter de los tokens emitidos por las DAOs y si éstos son auténticos "securities" según la *Securities Act* de 1933 y la *Securities Exchange Act* de 1934, vacilación del regulador propaga creando la confusión al mercado y generando inseguridad en los operadores que afecta a las iniciativas de fundar las DAO[103].

---

98 Delphi Labs. "Assimilating the BORG: A New Framework for CryptoLaw Entities". https://delphilabs.medium.com/assimilating-the-borg-a-new-cryptolegal-framework-for-dao-adjacent-entities-569e54a43f83

99 En nuestra literatura más clasiva, vid. Girón Tena, Derecho de sociedades, Valladolid, 1951.

100 "Law Commission Governance UK, "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/

101 Son las propuestas del grupo de investigación Coala que publicó la "Ley modelo".

102 Vid. las consideraciones criticas de Zhou "DAOs vs. Nation States: A Wyoming DAO's Experiment with the U.S. Securities and Exchange Commission". https://blogs.law.ox.ac.uk/oblb/blog-post/2024/03/daos-vs-nation-states-wyoming-daos-experiment-us-securities-and-exchange

103 Vid. criticas a la regulacion en Zhou "DAOs vs. Nation States: A Wyoming DAO's Experiment with the U.S. Securities and Exchange Commission". https://blogs.law.ox.ac.uk/oblb/blog-post/2024/03/daos-vs-nation-states-wyoming-daos-experiment-us-securities-and-exchange,

3.4.1.1. *Las "Legal wrapers"*

Las "legal wrappers" son propuestas legales para que las DAOs amolden el funcionamiento en el marco del régimen de sociedades tradicionales. Estas iniciativas del legislador tienen un claro propósito de ganarse a la comunidad cripto[104] a través del expediente de ofrecer regímenes más favorables –"friendly"– para el desarrollo de su actividad. Existe cierto consenso en la praxis acerca de que sólo las "DAOs envueltas en "Legalwrappers", gozan de personalidad jurídica por extender a estas organizaciones el atributo de la sociedad tradicional que la envuelve[105]. La DAOs se amoldan al esquema de una sociedad típica con el propósito de convertirle en sujeto de imputación y caso de violar la ley evitar la responsabilidad ilimitada de las personas que actúan en nombre de esa empresa[106].

Las estructuras tradicionales típicas –sociedades personalistas, de capital, cooperativas, fundaciones, e incluso estructuras de perfil más difuso ligadas a clubs de inversión[107]–, compiten en el debate de ser el "tipo" que mejor se adapta a las

---

en particular señalando que la remision de la SEC al documento "Securities and Exchange Commission (SEC): Release No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAOs, 25.07.2017, para aclarar dudas no tiene dicho efecto ilumnador.

104 Vid. crítica de Borgogno, "Making decentralized autonomous organizations (DAOss) fit for legal life: mind the gap", Questioni di Economia e Finanza, Banca d´Italia, 2022. https://www.bancaditalia.it, p. 19.

105 Vid. infome Amicus, Paradigm operations LP, p. 2. "DAOs can in fact leverage traditional corporate entities that can be held liable" remitiendo la cita a Brummer y Seira, "Legal wrapper and DAOs, 2022, 6-9.

106 Kaal (2021). "Decentralized Autonomous Organizations - Internal Governance and External Legal Design", University of St. Thomas (Minnesota) Legal Studies Research Paper, núms. 20-14, 43; Borgogno (2022). "Making decentralized autonomous organizations (DAOs) fit for legal life: mind the gap", Questioni di Economia e Finanza, Banca d´Italia, https://www.bancaditalia.it, p. 19; Schsuter (2020). "Cloud Crypto Land", 84 Modern Law Review 5; Brummer y Seira (2022). "Legal Wrappers and DAOss", Working Paper.

107 Gogel, Kremer, Slavin y Werbach (2022). "Decentralized Autonomous Organizations: Beyond the Hype", WEF, Whitepaper, p. 11. Vid. Kerr y Jennings, "A Legal framework for decentralized Autonomous Organizations". https://www.researchhub.com/paper/1268581/a-legal-framework-for-decentralized-autonomous organizations, pp. 7 y ss. con imágenes particularmente interesantes que describen las estructuras partícipes de los procesos de fundación de dichas entidades.

necesidades de la DAO[108]. Mencionamos las siguientes iniciativas por ser las estructuras legales –"legal wrapers"– más frecuentes:

a) *Sociedades limitadas* (LLCs) en Estados Unidos. Son las iniciativas de los estados de *Wyoming* en los EE. UU.; La denominada "Tennessee DO LLC", abril de 2022, siguiendo los pasos de Wyoming; el estatuto de la "organización descentralizada DO" de Tenessy, que omite el término "autónomo" por reconocer que en la realidad funcional la mayoría de las DAOs permanecen en manos de los partícipes; el modelo de "blockchain-based Limited Liability Company" de *Vermont* –(BBLLC)[109]–, uno de los estados que reconoció de forma más temprana el régimen legal de las DAOs; el modelo OpenLaw *de Delaware*, "Limited liability autonomous organization" or "LAO" a "decentralized autonomous organization"[110]; y el "decentralized autonomous organization" de Islas Marshall. Todos ellos, con mecanismos diferentes destacan el propósito de encajar la DAOs en una sociedad de responsabilidad limitada o LLP[111]. En otro contexto territorial se destaca la iniciativa de HongKong –"company limited by guarantee"– que se adapta bien a la naturaleza descentralizada de las DAOs[112].

---

[108] Edmund Schuster, "DAOss are better than corporations?", The Blockchain Debate Podcast. Afirma el autor que las DAOs son salas de chat con una cuenta bancaria conjunta. Los DAOs que son más sofisticados codifican las decisiones de gestión de tesorería para que sean dictadas por los resultados de la votación de la comunidad en cadena. Los DAOs generalmente operan con una cultura de máxima transparencia en tiempo real. Y existen reglas muy restrictivas sobre lo que puede hacer el órgano rector de las DAOs. A medida que las DAOs ganan popularidad, subrayan las ventajas frente a las sociedades tradicionales. En Wyoming incluso aprobó una ley relacionada con DAOs que brindaría protección de responsabilidad a los miembros de DAOs que se organicen como una LLC de Wyoming. Pero cabe preguntarse si las DAOs son formas de gobierno tan verdaderamente revolucionarias como se supone que son y por tanto el debate cuestiona en si la propia relevancia de la figura.

[109] Biggs, dOrg Founders Have Created the First Limited Liability DAOs, Coindesk 11.06.2019. https://www.coindesk.com/markets/2019/06/11/dorg-founders-have-created-the-first-limited-liability-DAOs/

[110] Kaal, Decentralized Autonomous Organizations - Internal Governance and External Legal Design, University of St. Thomas (Minnesota) Legal Studies Research Paper núms. 20-14, 2021, 43.

[111] Mienert, "How can a decentalized autonomous organization (DAOs) be legally structured?", Legal Revolutionary Journal LRZ, 2021, p. 3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3992329

[112] No More Tax, "Legal aspects of decentralized autonomous organisations (DAOss)". https://nomoretax.eu/legal-aspects-of-decentralized-autonomous-organisations-DAOss/

b) Esquemas de *fundaciones* en jurisdicciones como Suiza, Panamá, Islas Cayman bajo la regulación de la "The Foundation Companies Law" de 2017[113]. Esta envoltura se presenta particularmente adecuada por presentar las notas de las fundaciones similares atributos a los de las DAOs[114]. Similares a la fundación son los "*trust y fideicomisos*", populares en jurisdicciones de *common law* como el Reino Unido, las Islas del Canal, o Singapur", regímenes legales respecto de los que se trata de forma principal de evitar las tácticas de fraude[115].

c) *Sociedades y cooperativas*, por ser las estructuras que ofrecen formas alternativas para que las DAOs se integren en el marco legal existente, permitiendo una cierta flexibilidad en su operación y gobernanza propias de "gobiernos descentralizados". Algunos proponen la integración en el marco de las sociedades simples por la flexibilidad[116]. En suiza se propuso que las denominadas Asociaciones Autónomas Descentralizadas (DAA) se basaran en el esquema de una asociación[117].

3.4.1.2. *Régimen específico - "distinct body of law"*

La segunda opción consiste en elaborar un texto legal específico, *ad hoc*, para las DAOs. Malta se ha destacado como un líder en la regulación de tecnologías blockchain y DAOs. La Ley de Arreglos y Servicios de Tecnología Innovadora

---

113 "The Foundation Companies Law", de 201725th April 2017, Cayman Islands, available under: http://www.dlp.gov.ky/portal/pls/portal/docs/1/12408397.PDF

114 Mienert (2021). "How can a decentralized autonomous organization (DAOs) be legally structured?", Legal Revolutionary Journal LRZ. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3992329, p. 9. CALISKAN "The rise and fall of Electra: emergence and transformation of a global cryptocurrency community", 2022, p. 20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4239199&dgcid=ejournal_htmlemail_cryptocurrency:research:ejournal_abstractlink, fue un fracasado proyecto de fundación que se explica por la salida del fundador.

115 Borgogno (2022). "Making decentralized autonomous organizations (DAOss) fit for legal life: mind the gap", Questioni di Economia e Finanza, Banca d´Italia. https://www.bancaditalia.it, p. 16.

116 Vid. C III, del Law Commission Governance UK, "Decentralised autonomous organisations (DAOss). Call for evidence", Nov. 2022. https://www.lawcom.gov.uk/project/digital-assets/

117 Wehrmüller, Glarner, Linder y Meyer, "Decentralized Autonomous Association (DAA)" MME Legal Tax Compliance. https://www.lexology.com/library/detail.aspx?g=8cbb3694-164d-48da-abde-9115260bc873

(ITAS) de Malta, de 2018, es un ejemplo de cómo un marco legal puede ser adaptado para abordar las especificidades de las DAOs[118]. El carácter precursor de las pioneras legislaciones de algunos Estados Miembros en EE. UU. se han seguido con iniciativas más recientes de carácter federal, como la "Responsible Financial Innovation Act" (RFIA) enfocada al tratamiento en particular de la DAO para solucionar aspectos fiscales[119].

Destaca por su interés doctrinal, la propuesta de "Ley Modelo para Organizaciones Autónomas Descentralizadas (DAOs)" de 2021 efectuada por la "Coalición de aplicaciones legales automatizadas" (*Coalition of Automated Legal Applications* –COALA–). La Ley Modelo de DAO busca obtener reconocimiento legal para estas organizaciones, otorgándoles ciertos derechos y obligaciones, subrayando su particular naturaleza. El sector reconoce que los actores comerciales necesitan certeza con respecto a las contrapartes contractuales con las que están negociando, así como tener seguridad en la determinación de los activos que están disponibles para hacer frente a eventuales pasivos futuros. El grupo de trabajo internacional COALA, integrado por expertos del ámbito jurídico y tecnológico, ha impulsado la elaboración de una "ley modelo" destinada a ayudar a los estados miembros a modernizar su marco jurídico en materia de derecho de sociedades mediante la adopción de normas de derecho sustantivo que den soluciones a las DAOs[120].

Partiendo de un modelo legislativo nacional y con base en los principios de la autorregulación proponen reglas de funcionamiento para la comunidad blockchain con la finalidad de que, sobre una base voluntaria, incorporen un código fundacional que se preste al funcionamiento de las DAOs. El documento se convierte en una propuesta para que el legislador estudie la oportunidad de promulgar una "Ley Modelo de Organismos Autónomos Descentralizados (DAOs)", configurando un "marco legal" para las DAOs.

---

[118] Aznar, "Desafíos legales y estructuras de las Organizaciones Autónomas Descentralizadas (DAOs): Un breve análisis para el marco jurídico actual". https://www.baeslegalcripto.eu/legalcripto/desafios-legales-y-estructuras-de-las-daos/

[119] https://www.congress.gov/bill/117th-congress/senate-bill/4356/all-info. https://www.gillibrand.senate.gov/news/press/release/-lummis-gillibrand-introduce-landmark-legislation-to-createregulatory-framework-for-digital-assets.

[120] Borgogno y Martino (2024). "Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype", núm. 161. EBI, Working paper series, p. 14.

El enfoque original de la Ley Modelo sobre DAOs radica en el hecho de que ofrece un régimen legal único con expresión de distintas opciones tipo para las DAOs, rompiendo con el esquema de las "legal wrappers" de extender las normativas societarias existentes con la adaptación de ciertas menciones que incluyen las características para adaptar la tecnología de blockchain.

Hay normas que abordan la técnica de blockchain y definen realciones sociales dirigidas, en primer lugar, a abordar la *naturaleza de las relaciones entre los miembros y la DAOs*, en segundo lugar, *entre los propios miembros de la DAOs* y, en tercer lugar, *entre la DAOs y los terceros*. Se contemplan las disposiciones que definen la finalidad de la entidad, la configuración de sus recursos y el modelo de gobierno.

La Ley Modelo, propone un determinado esquema de condiciones –técnicas y societarias– para que la DAO que pretenda caracterizarse como tal y consiga el objetivo de alcanzar la personalidad jurídica y la limitación de responsabilidad. Los requisitos mínimos se refieren a: a) estar implementada en una *red de blockchain* "*no permisionada*" [art.4.1.a)]; b) la exigencia de tener una "*única dirección pública*" de forma que cualquiera pueda contemplar las actividades y pueda controlar las operaciones [art. 4.1.b)] lo que identifica la cadena de bloques en la que se basa la DAOs, salvo el caso de que ocurra un *Hard Fork*; c) debe tratarse de red de código *sofware* en formato "open-source" de forma que la DAOs se someta a examen en un foro público [art. 4.1.c)]; d) el código software de la DAO debe estar sujeta a una "*quality assurance*", esquemas de seguridad de acuerdo con los estándares de la industria [art.4.1.d)]; e) debe *contar con una GUI* con el fin de que los aspectos técnicos de comunicación de los miembros con la estructura queden sujetos a ciertos indicadores [art. 4.1.e)]; f) la DAOs debe contar con unos "*Estatutos*" que sean comprensibles para un lego técnico y estar en un sistema de acceso libre a través de un "GUI" o un foro público. La "GUI" alude a la interface o sistema de comunicación de los miembros y participes de la DAOs [art. 4.1.f)]; g) el *sistema de gobierno tiene que ser descentralizado* en varios sentidos "técnico" (una misma entidad no puede controlar todo el proceso): "arquitectónica"(porque se apoye funcionalmente en diversos nodos); "política" (porque sea válido en varias jurisdicciones); "lógica" (porque funcionalmente adquiera la estructura de sistema distribuido "como enjambre") [art. 4.1.g)]; h) las DAOs tienen que *contar al menos con un miembro* en todo momento; i) tiene que contar con un *Sistema de publicidad* que facilite a una persona no experta comunicar con la DAOs y que los administradores y los miembros de la DAOs tengan acceso al sistema de

comunicación [art. 4.1.i)]; j) la DAOs debe contar con un *sistema de resolución para los conflictos* entre los miembros y los partícipes a sus decisiones "Blockchain Dispute Resolution" (BDR) [art. 4.1.j)]; y k) deben contar con un *sistema de resolución de conflictos con terceros* [art. 4.1.k)].

Se trata de una construcción de un régimen que analiza las disposiciones del tipo en "clave contractual" y por ello algunas cuestiones clave se discuten con argumentos paralelos a las clásicas discusiones en derecho de sociedades, particularmente cuando se examinan la responsabilidad de los miembros y el blindaje e independencia patrimonial del ente. Las cláusulas de exoneración de responsabilidad por vía contractual (por no eludir por entero el riesgo subsistente frente a "terceros con responsabilidad extracontractual") son legalmente inseguras, en términos económicos ineficientes y propensas a generar "conflictos de interés" entre los miembros de la DAO por generar incentivos para actuaciones oportunistas.

Por esta razón, en líneas generales podría decirse que sería prácticamente imposible –sin normas legales especiales "ad hoc"– crear un blindaje de la entidad –"entity shielding"– efectiva para el ente y eficaz para eludir las responsabilidades en el marco de las relaciones de la DAO, en particular, frente a terceros[121].

4. CONCLUSIONES

El gobierno el blockchain se desenvuelve en el marco de la arquitectura técnica de la DLT, descritas como "sistemas" "descentralizados" de redes –*permisionadas, semi permisionadas o cerradas*– donde los stakeholders –*nodos, usuarios y desarrolladores*–, asistidos de ciertos elementos esenciales –*los activos digitales y los contratos inteligentes*– mantienen la funcionalidad del sistema dirigido a la finalidad primigenia de almacenar información pero habilitando una compleja infraestructura de las reglas, que pueden reaccionar a la competencia del mercado y tomar decisiones estratégicas que permitan el funcionamiento eficiente y seguro de la red y mantener sus aplicaciones. Desde esta perspectiva, para algunos, se trata de una primera noción de DAO.

---

[121] Hansmann, Kraakamn y Squire (2006). "Law and the Rise of the Firm" 119, *Harvard Law Review* 1333.

En sentido más propio, la Blockchain/DLT es la "columna vertebral" para la gobernanza de las DAOs que se implementan en estos sistemas como aplicaciones en las capas superiores en las que estratifica el funcionamiento de esta organización. Las Organizaciones Autónomas Descentralizadas (DAOs) son aplicaciones de gobierno que funcionan en la DLT con finalidades propias y que su evolución tiende a incrementar la incorporación progresiva de la IA. La DAO 1.0 surgieron con Bitcoin, como paradigma de la estructura de gobierno de las tecnologías de Ledger Distribuido (DLT). Con el proyecto "The DAO" en Ethereum –etapa DAO 2.0– nacieron las aplicaciones. La DAO 3.0, se vincula al desarrollo de las Finanzas Descentralizadas (DeFi) y la convergencia de tecnologías en el Metaverso marco en el que se incorporará una administración más sofisticada, siendo el punto culminante de esta evolución la fusión con la inteligencia artificial (IA) en la denominada Organización Cibernética CybOrg o "BORG" en el camino de los que preconizan que la IA alcanzará la "singularidad" son impredecibles consecuencias.

Las DAOs se caracterizan por las notas de la "autonomía" y la "descentralización", cercanas a las figuras de los "agentes autónomos", los "smart contracts" y los "protocolos". Algunas DAO atraen el interés de empresas por sus modelos innovadores por referirse a las organizaciones que permiten a los miembros participar en el gobierno y percibir los beneficios mediante la posesión de tokens y éstas son las que proyectan tener un potencial de crecimiento significativo en un entorno internacional en el entorno de DeFi y la Web3.

Europa ha renunciado hasta el momento a regular la figura por quedar excluida del texto final de MICA, lo que no impide que dichas organizaciones funcionen en la praxis, "de hecho", como sistemas de gobierno para coordinar actividades a través de programas o reglas autoejecutables implementadas en software en una red de blockchain.

La falta de reconocimiento legal específico ha generado incertidumbre legal y riesgos para los participantes. Enfrentados los supervisores a la actividad de las DAOs como cuando funcionan como entes no registrados, sin un marco legal claro, las subsumen en el marco de los fenómenos societarios simples y les aplica la responsabilidad ilimitada para ciertos participantes.

La iniciativas de regularlas (ya sea creando "legal wrappers" para "envolver" el funcionamiento de la DAOs al marco legal de sociedades tradicionales en sus diversas variables típicas –en esquemas societarios o de fundación–, o bien

desarrollando regímenes específicos para las estructuras DAO siguiendo las orientaciones de la Ley Modelo del grupo de investigación de COALA, ambas dirigidas al propósito de establecer las condiciones técnicas y societarias precisas para la obtención de personalidad jurídica y limitación de responsabilidad) no solventan todos los problemas de riesgo legal como señalan recientes pronunciamientos de la SEC.

BIBLIOGRAFÍA

AbrianI (2020). "Corporate governance in the era of the algorithm Prolegomena to an impact study of Artificial Intelligence on Corporate Governance", *Rivista Il nuovo diritto delle società*, 3, pp. 261-285.

Axelsen, Jensen y Ross (2022). "When is a DAO Decentralized?", Complex Systems Informatics and Modeling Quarterly 31.

Aznar. "Desafíos legales y estructuras de las Organizaciones Autónomas Descentralizadas (DAOs): Un breve análisis para el marco jurídico actual". https://www.baeslegalcripto.eu/legalcripto/desafios-legales-y-estructuras-de-las-daos//

Biggs (2019). dOrg Founders Have Created the First Limited Liability DAOs, Coindesk 11.06.2019. https://www.coindesk.com/markets/2019/06/11/dorg-founders-have-created-the-first-limited-liability-DAOs/

Borgogno y Martino (2024). "Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype", núm. 161. EBI, *Working paper series*.

Buterin (2013). "Bootstrappping a Decentralized Autonomous Corporation: Part I". https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274, September 19.

Buterin (2014). "DAOs, DACs, DAs and More: An Incomplete Terminology Guide", Ethereum Blog, 4 May. https://blog.ethereum.org/2014/05/06/DAOs-dacs-das-and-more-an-incomplete-terminology-guide/

Calcaterra et al. "Blockchain Infrastructure for Measuring DomainSpecific Reputation in Autonomous Decentralized and Anonymous Systems" (U of St. Thomas (Minnesota), *Legal Studies Research Paper*, núm. 18-11. https://ssrn.com/abstract=3125822

Caliskan. "The rise and fall of Electra: emergence and transformation of a global cryptocurrency community", SSRN-id4239199-1.

Cawrey (2014). 37 Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet. CoinDesk. https://www.coindesk.com/markets/2014/05/20/37coins-plans-worldwide-bitcoin-access-with-sms-based-wallet/

Chamorro Domínguez (2020). "La aplicación de sistemas de inteligencia artificial en el seno del órgano de administración de las sociedades de capital", *Revista de Derecho de Sociedades*, ISSN 1134-7686, núm. 59.

Cocco, Pinna y Marchesi (2017). "Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. Future Internet", 9:25. https://doi.org/10.3390/fi9030025

De Filippi y Wright (2018). *Blockchain and the law: The rule of code*. C.9, "Decentralized autonomous organizations", Harvard, chapter.8, p. 131.

De Filippi y Loveluck (2016). "The invisible politics of bitcoin: governance crisis of a decentralized infrastructure", *Internet Policy Review* 5, núm. 4. https://doi.org/10.14763/2016.3.427

Del Castillo (2016). "IBM Watson is working to bring IA to the blockchain" Coinsdesk, April 5. https://www.coindesk.com/markets/2016/04/05/ibm-watson-is-working-to-bring-ai-to-the-blockchain/

Delphi Labs. "Assimilating the BORG: A New Framework for CryptoLaw Entities". https://delphilabs.medium.com/assimilating-the-borg-a-new-cryptolegal-framework-for-dao-adjacent-entities-569e54a43f83

Diallo, Shi, Xu, Gao, Chen, Lu, Shah et al. (2018). "eGovDAO: A better government using blockchain based decentralized autonomous organization", en 2018 International Conference on eDemocracy & eGovernment (ICEDEG), IEEE. https://letonchanh.github.io/files/icedeg18.pdf

El Faqir El Rhazoui, Arroyo y Hassan. "A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain". https://jisajournal.springeropen.com/articles/10.1186/s13174-021-00139-6

Finra (2017). *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*. https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

Galaxy Fund Management (2022). "What are DAOs?". https://www.galaxyfundmanagement.com/crypto-101/what-are-DAOs

García Rolo (2019). "Challenges in the legal qualificacion of descentralised autonomous organisations (DAOS): the rise of the crypto-partnerchip", R Dtec, 33-87. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3417900

Guillaume y Riva (2022). "How to Resolve A Dispute Involving A DAO". https://sites.duke.edu/thefinregblog/2022/07/21/how-to-resolve-a-dispute-involving-a-dao/

Hansmann, Kraakamn y Squire (2006). "Law and the Rise of the Firm", 119, *Harvard Law Review* 1333.

Hassan, Samer y Primavera De Filippi (2021). "Decentralized Autonomous Organization", *Internet Policy Review*, Vol. 10, núm. 2, p. 3. https://policyreview.info/pdf/policyreview-2021-2-1556.pdf.

Héctor, Ugarte y Rheinische. "A more pragmatic Web 3.0: Linked Blockchain Data" "Semantic Blockchain" - Starting Point. https://www.google.com/search?client=firefox-b-d&q=A+more+pragmatic+Web+3.0%3A+Linked+Blockchain+Data

Ibáñez Jiménez. *Derecho de blockchain*.

— (2020) *Consorcio red Alastria (Origen y reforma de la primera blockchain de España)*, Madrid.

Jennings y Horowitz. "Principles & Models of Web3 Decentralization", a16zcrypto.com, https://d1lamhf6l6yk6d.cloudfront.net/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf

Jentzsch, C. *Decentralized Autonomous Organization to Automate Governance*. https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf

Kaal (2019). "Blockchain-based corporate governance", Max Plank Institute Luxembourg for procedural Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441904,

Kerr y Jennings. "A Legal framework for decentralized Autonomous Organizations". https://www.researchhub.com/paper/1268581/a-legal-framework-for-decentralized-autonomous-organizations

Llyr (2022). Re-envisioning corporations: How DAOs and blockchain can improve the way we organize, Davos agenda, Head of Blockchain and Digital Assets, CISA, World Economic Forum.

Lumineau, Wang y Schilke (2021). Blockchain Governance - A New Way of Organizing Collaborations?

Martínez Cañellas (2023). "Inteligencia artificial y Derecho de sociedades. Una primera aproximación", en Herbosa Martínez y Fernández de Retana Gorostizagoiza (dirs.) *Derecho e inteligencia artificial. El jurista ante los retos de la era de la Inteligencia artificial*, Navarra.

Martínez Cañellas (2024). "Sociedades mercantiles administradas por inteligencia artificial: DAOS y entidades algorítmicas autónomas en Derecho español", *Derecho Digital, Estudios, La Ley mercantil*, núm. 112, abril, Editorial La Ley.

Maskin, E. (2002). 'On Indescribable Contingencies and Incomplete Contracts', *46 European Economic Review* 725. https://scholar.harvard.edu/files/maskin/files/on_indescribable_contingencies_and_incomplete_contracts_e._maskin.pdf?m=1428327268;

Mienert (2021). "How can a decentralized autonomous organization (DAOs) be legally structured?", *Legal Revolutionary Journal* LRZ. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3992329, p. 9.

Mölein, F. "Robots in the Boardroom: Artificial Intelligence and Corporate Law", Woodrow Barfield y Ugo Pagallo (eds.), Research Handbook on the Law of Artificial Intelligence, Edward Elgar (2017/2018, Forthcoming), pp. 665-60.

Muñoz Pérez, A.F. (2023). *Las DAOs y el reto de controlar al algoritmo*, Cizur Menor.

Muñoz Pérez, A.F. (2020). La "inteligencia artificial (IA) autónoma" en el órgano de administración, *Revista de Derecho de Sociedades*, núm. 60.

Muñoz Pérez, A.F. (2021). "Inteligencia artificial y los "ciber-consejeros", los miembros robotizados como integrantes del Consejo de administración",

Digitalización de sociedades, en Carmen Alonso Ledesma y Ana Felicitas Muñoz Pérez (coord.), ISBN 978-84-18349-90-4, pp. 171-190.

Muñoz Pérez, A.F. (2022). "Blockchain, criterios ESG y objetivos ODS. Consideraciones sobre las DAOS sostenibles". *Revista de Derecho del Mercado de Valores* 31.

Muñoz Pérez, A.F. "Algunas consideraciones sobre la convergencia de las tecnologías de Blockchain e IA" (en prensa).

Nabben (2021). "Imagining human-machine futures: blockchain-based "Decentralized Autonomous Organizations". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953623

Nabben, Puspasari, Kellher y Sanjay (2021). "Grounding decentralised technologies in cooperative principles: What can "Decentralised Autonomous Organisations" (DAOs) and platform cooperatives learn from each other?". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3979223

Navarro Lérida (2023). "Gobernanza de comunidades en la web3: el papel de las DAOs", *Derecho digital e innovación*, núm. 16, abril, Editorial La Ley.

Navarro Lérida (2018). "Gobierno corporativo, blockchain y smart contracts. Digitalización de las empresas y nuevos modelos descentralizados (DAOS)", núm. 23, *RMV* 23, 1-20.

Peltrin, M. (2019). "Corporate Management in the age of AI", *UCL Working Paper Series Corporate Management in the Age of AI*, núm. 3.

Pupyshev, Sapranidi y Khalilov (2022). "Pathway: a protocol for algorithmic pricing of a DAO governance token". https://arxiv.org/pdf/2202.06541.pdf

Reyes, Geslevich, Packing y Edwards. "Distributed Governance", *William & Mary Law Review Online*. https://scholarship.law.wm.edu/wmlronline/vol59/iss1/1/

Rohr y Wright (2019). "Blockchains, private ordering and the future of governance", en Hacker, Lianos y Dimitropoulos (dirs.), *Regulating blockchain*. *Techno-social and legal challengues*, UK.

Roncero (2019). "BIG DATA y responsabilidad de los administradores de sociedades de capital", *Revolución digital, Derecho Mercantil y Token economía*.

Rozas, Tenorio-Fornés, Díaz-Molina y Hassan (2021). "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance". Sage Open 11, no. 1. https://doi.org/10.1177/21582440211002526

Seira, Allen, Watsky y alley (2024). "Governance of Permissionless Blockchain Networks", February 09, FEDS notes. https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html.

Shakow, D. (2018). "The Tao of the DAO: Taxing an Entity That Lives on a Blockchain".

Shapiro, A. (2022). Functionalist Framework for DeFi Regulation. https://lexnode.substack.com/p/a-functionalist-framework-for-defi.

Szabo, N. (1994). Smart Contracts, Building Blocks for Digital Markets. http://www.virtualschool.edu/mon/Economics/SmartContracts.html.

Tabone. "Dao: the evolution of organization", Cointelegraph.

Troncoso y Utratiel (2019). "If I Only Had a Heart: A DisCO Manifesto. DisCO". https://disco.coop/manifesto/, https://www.tni.org/files/profiles-downloads/disco_manifesto_v.1.pdf)

Vitalik Buterin. "A next generation smart contract & decentralized application platform", *Ethereum White Paper*.

Vos (2019). "Cryptoassets as property: how can English law boost the confidence of would-be parties to smart legal contracts?", 2 May, Joint Northern Chancery Bar Association and University of Liverpool Lecture. https://www.judiciary.uk/wp-content/uploads/2019/05/Sir-Geoffrey-Vos-Chancellor-of-the-High-Court-speech-on-cryptoassets.pdf.

Walch (2019). "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains", *Regulating Blockchain: Techno-Social and Legal Challenges*, pp. 58 y ss.

Wehrmüller, Glarner, Linder y Meyer. "Decentralized Autonomous Association (DAA)", MME Legal Tax Compliance. https://www.lexology.com/library/detail.aspx?g=8cbb3694-164d-48da-abde-9115260bc873

Wright. "The rise of decentralized autonomous organizations: Opportunities and challenges". Stan. J. Blockchain L. & Pol'y 4 (2020). https://stanfordjblp.pubpub.org/pub/rise-of-daos

Yaga, Mell, Roby y Scarfone (2018). "Blockchain Technology Overview". https://doi.org/10.6028/NIST.IR.8202, pp. 18 y ss.

Zhang, Shijie y Lee (2020). "Analysis of the main consensus protocols of blockchain", ICT express6.2.

DOCUMENTOS

"ITU-T Focus group on Appplication of Distributed Ledger Technology" (FG DLT), "Techincal Report" FG DLT D4.1 "Distributed ledger technology regulatory framework" ITU, D. 11 "DLT terms and definitions", 1.2; DLT "Overview, concepts, ecosystem", 1.3; DLT "Standardization landscape", 2.1; DLT "Use cases", 3.1; DLT "Reference architecture", 3.3, "Assessment criteria for DLT platforms", 4.1. DLT "Regulatory framework", 5.1. "Outlook on DLTs".

Digital Assets (2022). *Law Commission Consultation Paper*, núm. 256, Chapter 14. https://www.lawcom.gov.uk/project/digital-assets/

Law Commission Governance UK (2022). "Decentralised autonomous organisations (DAOs). Call for evidence", Nov. https://www.lawcom.gov.uk/project/digital-assets/, p. 63.

Agenda Davos, "How Web3 will level the playing field and unlock income equality". https://www.weforum.org/agenda/2022/05/what-is-web3-why-care-future/

Federal Council Report (2018). "Legal gramework for distributed ledger tecnology and blockchain in Switzerland", cit. p. 48.

World Economic Forum (WEF) (2023). "Decentralised Autonomous Organization Toolkit Insight Report".

Capítulo 12
LAS APLICACIONES DE LA TECNOLOGÍA DE REGISTROS DISTRIBUIDOS EN LAS SOCIEDADES DE CAPITAL

Reyes Palá Laguna
Catedrática de Derecho Mercantil
Universidad de Zaragoza
https://orcid.org/0000-0002-9059-5698

1. INTRODUCCIÓN[1]

La tecnología basada en sistemas de registros distribuidos (TRD), una de cuyas concreciones más conocidas es la de cadena de bloques o *blockchain*, tiene en un plano teórico evidentes utilidades en el funcionamiento de las sociedades de capital. No sólo en el ámbito interno en la organización y funcionamiento de la propia sociedad (*ad intra*) sino también *ad extra*, desde el momento en el que los potenciales inversores pueden, a través de estas tecnologías, financiar la actividad de la sociedad en el mercado.

La velocidad con la que se producen avances y mejoras en el uso de esta tecnología hace que algunos problemas que puede plantear su aplicación en un tiempo determinado se solucionen con relativa rapidez: por ejemplo, la crítica certera al insostenible gasto energético que produce el funcionamiento de la red pública *blockchain* con las validaciones algorítmicas (*proof of work*) por los "mineros" de las operaciones en las cadenas de bloques, se matiza cuando la tecnología permite un nuevo sistema de validación de las transacciones en los nodos que integran el registro distribuido (*proof of stake*), a la que le puede

[1] Trabajo realizado en el marco del proyecto I + D de investigación estatal "Blockchain y Derecho societario (2). Bigdata, Fintech y la protección del usuario de los servicios financieros" (PID2022-137502NB-I00), II.PP., Reyes Palá Laguna y Pedro-José Bueso Guillén.

sustituir la *proof of authority* en una red permisionada que requiere autorización para formar parte de ella[2].

No es este el lugar para describir el funcionamiento de las diversas manifestaciones de la tecnología de registro distribuido, pero es necesario precisar, a los efectos de este trabajo, que un registro distribuido es una base de datos (a veces se le denomina libro mayor electrónico) que conecta diversos nodos para validar determinada información a través de un mecanismo de consenso en clave criptográfica, de forma que la certeza e inmutabilidad de esta queda garantizada, en un planteamiento general, por el propio funcionamiento de validación de los datos introducidos en el registro conforme al protocolo de creación de la red[3].

---

[2] Ibáñez Jiménez, J. W. e Ibáñez Jiménez, E. M. (2023). "NFT Legal and Market Challenges in Permissioned Blockchain Networks", AA. VV., *Blockchain Applications: Transforming Industries, Enhancing Security and Addressing Ethical Considerations,* V. Chernyshenko y V. Mkrttchian (dirs.), DOI: 10.5772/intechopen.106460, epígrafe 3 de la versión digital.

[3] Bech, M. y Garrat, R. (2017). "Central Bank Cryptocurrencies", *BIS Quaterly Review*, septiembre, pp. 55-70, p. 58. En otras palabras, un registro distribuido es una base de datos descentralizada y única gestionada por varios participantes que se actualiza de manera sincronizada. La novedad de la TRD es la implantación de un sistema para verificar colectivamente los datos que acceden al registro antes de compartirlos (Romero Ugarte, J. L. (2018), "Tecnología de registros distribuidos (DLT): una introducción", *Boletín Económico del Banco de España,* octubre, p. 1). Esta tecnología se basa en sistemas de conexión consorciados y plurilaterales desde redes "nodales" en un esquema compartido de registro de datos. En los sistemas basados en TRD, la transacción no tiene por qué consistir en un contrato de valor económico; puede ser un mero intercambio de datos de un usuario de la red a otro que habrán de ser validados por los nodos del sistema conforme al protocolo de funcionamiento de la red; es entonces cuando se sella la transacción de forma criptográfica (*hash)* para quedar indeleble e irreversiblemente incluida en un nodo o bloque de la red distribuida (estas ideas, en Ibáñez Jiménez, J. W. (2021), "Financiación digital distribuida", en AA. VV., *Digitalización de sociedades,* C. Alonso Ledesma y A.F. Muñoz Pérez (coord.), *Cuadernos de Derecho para Ingenieros*, 54, pp. 22-48, pp. 30-31). Contamos ya con buena bibliografía sobre la TRD en castellano; de ella, destacamos los trabajos publicados por tres autores: el citado Ibáñez Jiménez, A. F. Muñoz Pérez y A. Muñoz García. Estos dos últimos autores publicaron recientemente interesantes trabajos en la *RDBB* 170, 2023. Encontramos definiciones de esta tecnología en el derecho positivo europeo en el art. 2 del Reglamento 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo, sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado, que define la TRD (a la que denomina tecnología de registro *descentralizado* y no tecnología de registro *distribuido*, que es la expresión utilizada por el legislador español en la LMV) como "una tecnología que permite el funcionamiento y el uso de registros descentralizados"; "registro descentralizado" se define como "un repositorio de información que lleva registros de operaciones y se comparte a través de un conjunto de nodos de red TRD y está sincronizado entre dichos nodos, utilizando un mecanismo de consenso"; "mecanismo de consenso" son "las normas y procedimientos

Concepto esencial en la aplicación de esta tecnología es el de "toquen" o "criptoactivo", definido en el Reglamento sobre los mercados de criptoactivos como "representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar"[4]. Un paso más a nuestros efectos es cuando el toquen queda vinculado a un *smart contract* o programa que contiene un conjunto de normas codificadas que, acaecido un determinado evento, se ejecutan automáticamente sobre los toquens del registro[5].

Quizá el ámbito más evidente de las aplicaciones de la TRD sea el financiero, por la simplicidad y teórico abaratamiento de costes que implica la desintermediación financiera frente a la tradicional inversión intermediada a través de empresas de servicios de inversión. Cierto es que el derecho español parte de un modelo de registro distribuido, pero no necesariamente descentralizado; ello se deduce de la, por el momento, escasa normativa la respecto (arts. 5 a 15 de la LMV), como veremos más adelante

En este trabajo no nos ocuparemos de la financiación societaria a través de lo que se conoce como DeFI (finanzas descentralizadas), por estar en un incipiente estado de desarrollo; ni tampoco de las organizaciones autónomas descentralizadas (DAOs) que se crean para gestionar una red *blockchain*. Queda al margen asimismo el análisis de los mercados de criptoactivos regulados en el Reglamento MiCA –norma de próxima aplicación directa al derecho español– sin perjuicio de que hagamos alguna referencia en el texto: la razón de ello es

mediante los cuales se llega a un acuerdo de validación de una operación entre los nodos de red TRD" y "nodo de red TRD" es aquel "dispositivo o proceso que forma parte de una red y que posee una copia completa o parcial de los registros de todas las operaciones en un registro descentralizado".

[4] Art. 3.5 del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA).

[5] Una definición legal de *smart contract* ("contrato inteligente") la encontramos en el artículo 2.39 del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización (Reglamento de Datos): "programa informático utilizado para la ejecución automatizada de un acuerdo o de parte de este, que utiliza una secuencia de registros electrónicos de datos y garantiza su integridad y la exactitud de su orden cronológico". Aplicada esta definición a los sistemas basados en TRD, la ejecución automatizada del programa se integra en la red de registro distribuido y se vincula a un toquen.

que los criptovalores negociables emitidos por las sociedades de capital (*security tokens*) quedan fuera del ámbito objetivo de este Reglamento MiCA[6].

Nos centraremos en las páginas que siguen en la aplicación de la TRD al funcionamiento de las sociedades de capital, cuya aproximación doctrinal y legal parte de redes permisionadas en las se requiere autorización o, al menos, existe un control de acceso para acceder a la red, por oposición a la red no permisionada[7]; ejemplo de esta última es *bitcoin*.

Las funcionalidades de esta tecnología se vinculan, no solo al toquen sino al *smart contract* en la TRD. Es entonces cuando se produce la *revolución*[8] en la representación y circulación de los derechos, de manera que, al igual que sucedió con los títulos-acciones o títulos valores en general –calificados como la mayor contribución del Derecho mercantil a la economía moderna–[9], estamos ahora ante una nueva forma de representación –criptográfica– de los derechos, representación que puede suponer una nueva revolución en el ámbito financiero, como aconteció con la incorporación del derecho al documento en la teoría general de los títulos valores a finales del siglo XIX y que convirtió a las sociedades anónimas en "máquinas del capitalismo", en la conocida expresión de Ripert[10].

Estas redes o sistemas distribuidos pueden ser utilizados por las sociedades de capitales en el marco de su organización y gestión interna, esto es, en relación con el funcionamiento de los órganos de la sociedad y de los derechos del socio, o bien en el ámbito externo, cuando la sociedad apela a los mercados de capitales para obtener financiación a través de activos digitales o toquens. Pero queda lejos

---

[6] V. considerando 9 y art. 4 a) del Reglamento MiCA y Palá Laguna, R., Canalejas Merín, J. C. (2023). "A qué criptoactivos no se aplicará el Reglamento MiCA", *Análisis GA_P*, 20 de junio.

[7] Un resumen de las clasificaciones de las distintas redes *blockchain* en Herrero Morant (2020), "La tecnología DLT en el mercado de valores, en especial respecto de las acciones de las sociedades cotizadas. Aspectos generales y análisis de una posible desintermediación del mercado", en *RDMV*, 26, versión digital, *In extenso*, Ibáñez Jiménez, J. W. (2018). *Blockchain, primeras cuestiones en el ordenamiento español,* Dykinson, Madrid, con especial atención a las redes permisionadas en pp. 139 y ss.

[8] La expresión, en Garrido, J. (2023). "Digital Tokens: A Legal Perspective", *IMF wp/23/151*, julio, p. 13.

[9] Ascarelli, T. (1940). voz "Titoli di crédito", *Nuovo Digesto Italiano*, Vol. XII, Turín, p. 205.

[10] Ripert, G. (1950). *Aspectos jurídicos del capitalismo moderno*, Bosch y cía eds., Buenos Aires, p. 125.

aún ese ideal del *blockchain*[11], en el que los socios custodian directamente sus acciones en su *wallet* (o delegan la custodia de sus claves privadas en entidades inscritas en el registro administrativo del Banco de España), acciones emitidas directamente en *blockchain* por la sociedad y que se transmiten por medio de la red, quedando registrada automáticamente esa transmisión de forma indeleble, en tiempo real y con certeza y seguridad jurídica para ambas partes, sin necesidad de intermediarios ni custodios[12].

Por el momento de lo que se trata es de beneficiarse de las ventajas que presenta la tecnología de registro distribuido de forma más modesta, utilizando la TRD en redes permisionadas en la que exista una entidad –la sociedad o un tercero– responsable de la administración y registro de los toquens en el sistema, con los pertinentes controles de acceso y de ciberseguridad que permitan a los usuarios conocer las transacciones en ella realizadas que quedan registradas en el registro distribuido de forma inmutable.

---

[11] Takahashi, K. (2021). "Blockchain-based Negotiable Instruments (with Particular Reference to Bills of Lading and Investment Securities)", octubre, disponble en https://ssrn.com/abstract=3937664, p. 9.

[12] Ideal que por otra parte en España despareció para la circulación de las acciones al portador representadas mediante título (en papel) con el Decreto dado en Burgos el 19 de septiembre de 1936 al exigirse en su transmisión la intervención de corredor colegiado de comercio o de agente de cambio y bolsa como requisito *ad solemnitatem* para gozar de la irreivindicabilidad del art. 545 del C. Com ("Los títulos al portador serán transmisibles por la tradición del documento. No estará sujeto a reivindicación el título cuya posesión se adquiera por tercero de buena fe y sin culpa grave. Quedarán a salvo los derechos y acciones del legítimo propietario contra los responsables de los actos que le hayan privado del dominio."), sin perjuicio de la validez del negocio causal *inter partes*. Esta previsión se establece hoy en el art. 11.5 LMV referida, lógicamente, a la intervención del notario en la transmisión de títulos al portador ("La suscripción o transmisión de valores negociables sólo requerirá para su validez la intervención de notario cuando, no estando admitidos a negociación en un mercado regulado, estén representados mediante títulos al portador y dicha suscripción o transmisión no se efectúe con la participación o mediación de una sociedad o agencia de valores, o de una entidad de crédito").

2. LAS APLICACIONES DE LA TRD EN EL FUNCIONAMIENTO DE LAS SOCIEDADES DE CAPITAL

2.1. Consideraciones generales

Los sistemas basados en TRD con validación de las transacciones sobre toquens en bloques o nodos requieren de un número mínimo de usuarios para garantizar la seguridad de la red frente a los ciberataques. Por ello, no parecen especialmente idóneos para los actos y acuerdos de las sociedades con un reducido número de socios. A la vista además de los costes vinculados al mantenimiento del registro distribuido, no parece de momento idóneo el recurso a esta tecnología para los registros de sociedades cerradas –en principio con un menor número de socios–. En este grupo se adscribirían la mayoría de las sociedades de responsabilidad limitada y las sociedades anónimas cerradas –con un número de socios inferior, por ejemplo, a cincuenta– frente a las grandes sociedades anónimas cotizadas, en las que se pueden generar multitud de toquens que instrumentan valores mobiliarios o determinados derechos del socio de forma que se permita el funcionamiento del sistema basado en la TRD con seguridad y por tanto inmutabilidad de las transacciones sobre toquens en él realizado.

Por otra parte, la práctica evidencia que ello es lo que ha sucedido en el caso de las acciones representadas mediante anotaciones en cuenta: solo las cotizadas –por mandato legal, art. 496 LSC[13]– y otras contadas anónimas, representan sus acciones en anotaciones en cuenta[14].

Por ello, tampoco vemos la utilidad de celebrar las reuniones del consejo con TRD o el cómputo de los votos de los consejeros por este sistema, estemos ante una sociedad abierta o cerrada (pensando en las reuniones por escrito y sin sesión, su realización por *blockchain* parece, de momento, lejana, aunque no desdeñable en el caso de las juntas generales de las grandes cotizadas). Las tecnologías de

---

[13] No solo las acciones de las sociedades cotizadas en mercado regulado (Bolsas de Valores, Sistema de Interconexión Bursátil) han de estar representadas mediante anotaciones en cuenta, sino también las de las cotizadas en sistemas multilaterales de negociación –por ejemplo, en España, BME Growth– por la remisión que al régimen de la cotizada en mercado regulado realiza la disp. ad. 13º LSC para las sociedades admitidas en estos sistemas multilaterales de negociación.

[14] Puede consultarse al respecto el registro de entidades encargadas de la llevanza del registro contable de valores negociables no admitidos a negociación, registro de acceso público a través de la página web de la Comisión Nacional del Mercado de Valores (CNMV).

comunicación permiten la celebración de los consejos de administración por videoconferencia sin especiales problemas prácticos. Si bien las restricciones a la movilidad consecuencia de la pandemia generada por la Covid-19 apremiaron al legislador a regular la celebración de la junta por medios íntegramente telemáticos, previsión hoy contenida en el artículo 182 bis LSC[15], por lo que respecta al órgano de administración, las reuniones del consejo antes de la legislación de urgencia podían celebrarse *on line*, con alguna excepción, sin mayores impedimentos legales[16].

Sentado lo dicho, no cerramos la puerta a las innovaciones tecnológicas que permitirían trasladar la validación de las operaciones a través de los distintos bloques o nodos por un sistema alternativo menos riguroso, también de registro distribuido. Piénsese por ejemplo en el libro registro de socios de la sociedad limitada (artículo 104 LSC) al que podría tener acceso en la TRD el registrador mercantil del domicilio social de forma que quedaran registradas en el sistema las titularidades originarias y las sucesivas transmisiones, voluntarias o forzosas, de las participaciones sociales, así como la constitución de derechos reales y otros gravámenes sobre las mismas, participaciones sociales y derechos reales previamente toquenizados.

A diferencia de lo que sucede con las acciones de las anónimas –cuestión que trataremos más adelante– la ley no exige una determinada forma de representación para las participaciones sociales, los derechos reales y cualesquiera otros gravámenes sobre estas. Cierto es que la transmisión de participaciones sociales, así como la constitución del derecho real de prenda, deberán constar en documento

---

[15] Una exposición de cuestiones conflictivas en relación con las juntas exclusivamente telemáticas y la posibilidad de impugnar los acuerdos sociales por causas derivadas de la tecnología aplicada en la celebración de la junta, en Gállego Lanau, M. (2022). *La junta exclusivamente telemática en las sociedades de capital cerradas,* Aranzadi, pp. 183-188.

[16] Por todos, Díaz Moreno, A. (2000). "Consejos de administración virtuales y adopción de acuerdos por escrito y sin sesión durante el estado de alarma", *Análisis GA-P*, 17 de marzo; y Hernández Sáinz, E. (2020), "La asistencia virtual al consejo en las sociedades cotizadas", *RDMV*, 27, versión digital. El impedimento legal al que hemos aludido lo encontramos en el art. 246.2 LSC (solicitud de convocatoria del consejo por un tercio de los miembros cuando su presidente, previa petición, no hubiera hecho la convocatoria en el plazo de un mes), puesto que la norma prevé en este caso su celebración "en la localidad donde radique el domicilio social". Será por ello necesario expresa previsión estatutaria para la celebración del consejo *on line* en este concreto supuesto (Díaz Moreno, *op. cit*, p. 2).

público, y la constitución de otros derechos reales en escritura pública (art. 106 LSC). Pero la decidida apuesta por la digitalización de actos societarios realizada por la Ley 11/2023, de 8 de mayo y el Real Decreto 442/2023, de 13 de junio permite el otorgamiento telemático (por videoconferencia) de la escritura pública[17], con lo que al menos las transmisiones voluntarias y la constitución de derechos reales podrán instrumentarse ante notario *on line* e incorporar a un toquen esa transmisión o derecho real, que accedería al registro distribuido con conocimiento del registrador mercantil. De esta forma, el registro de socios y la existencia de derechos reales sobre participaciones sociales estarían permanentemente actualizados en el ámbito registral, a diferencia de lo que ahora sucede con el libro registro de socios, del que el registrador va conociendo conforme se comunica por los administradores al registro mercantil la transmisión de una o varias participaciones sociales.

2.2. Los registros societarios en TRD

En el ámbito interno societario, puesto que los sistemas basados en TRD no dejan de ser un registro informático, aunque distribuido, los registros a cargo de la sociedad pueden llevarse mediante la toquenización de los datos que en ellos deben o pueden hacerse constar[18]. La cuestión es que no se nos alcanza

---

[17] Destacamos al respecto, además de la modificación de la LSC, la reforma de la Ley del notariado por la Ley 11/2023 que permite la digitalización de todo el ciclo vital de la sociedad de capital: el nuevo art. 17 ter contempla el "otorgamiento y autorización a través de videoconferencia como cauce para el ejercicio de la función pública notarial", entre otros, de "la constitución de sociedades, nombramientos y apoderamientos mercantiles de toda clase previstos en la legislación mercantil, así como el otorgamiento de cualquier otro acto societario, siempre que en caso de contener aportaciones de los socios al capital social sean dinerarias", así como la elaboración de las actas de la junta general "y las de referencia en estricto" junto con los testimonios de legitimación de firmas o la cancelación de garantías.

[18] Respecto a la posibilidad de instrumentar los registros societarios en TRD, en los Estados Unidos, el primer estado federado que legisló al respecto fue Delaware en 2017, al que siguieron, entre otros, Arizona en 2018, Wyoming en 2019, Nueva Jersey en 2020 o Iowa en 2021, con una normativa inspirada en la aprobada por el estado de Delaware (más un millón de entidades mercantiles, entre ellas, el 66% de las sociedades que integran la lista Fortune 500 están domiciliadas en este Estado, https://corp.delaware.gov/aboutagency/). La s. 224 (capítulo 8) del Código de sociedades de Delaware establece que la llevanza de cualquier registro –directa o indirectamente– por la sociedad, en el desarrollo de su actividad, incluyendo el libro registro de socios y los de contabilidad y de actas, puede realizarse a través de una o varias redes electrónicas o bases de datos distribuidas electrónicamente, siempre que el contenido de los registros

la utilidad de acudir a ella, de momento, para determinados libros obligatorios de los empresarios, como los libros de contabilidad –cuya llevanza se realiza de forma completamente digitalizada–, o los de actas de las juntas y de otros órganos colegiados, por no ver de momento la utilidad que tendría, por ejemplo, la inclusión de los datos del libro registro de actas de las juntas generales de la sociedad –ni siquiera el de las reuniones del consejo de administración– a través de la TRD, al no ser compleja en el primer caso –y tampoco en el segundo–, la llevanza de este registro para la sociedad en cuestión: no se aprecian por ello las ventajas que la TRD podría aportar en la llevanza de estos registros de reuniones, bien esporádicas (junta), bien mensuales (consejo). Cosa distinta es que los registradores mercantiles, que cuentan con suficientes medios y están al día de los avances tecnológicos, establecieran un sistema de interconexión nacional entre todos los registros territoriales creándose una red distribuida entre todos ellos en la que se incluyeran los datos que han de constar en estos libros de actas de las sociedades mercantiles.

Como hemos indicado en otro lugar, además de los libros citados, junto con el libro registro de socios la sociedad mantiene otros registros que podrán ser llevados mediante sistemas basados en la TRD: piénsese en la lista de asistentes a una junta general de la cotizada, los votos emitidos en estas juntas, la delegación de los derechos de asistencia y de voto, los socios legitimados para percibir el concreto dividendo aprobado por la junta y su abono, el ejercicio del dividendo flexible (*scrip dividend*), los aceptantes de una OPA, los suscriptores de una oferta pública de suscripción o los adquirentes en una OPV, los titulares de acciones de voto adicional por lealtad en las sociedades cotizadas, etc. De lo que se trata es de convertir determinados datos en un criptoactivo, en un toquen, que incluya, por ejemplo, los datos los relativos a la identidad del socio y su domicilio, el número de acciones de las que es titular y el resto de los datos a los que se

---

pueda ser convertido en "papel claramente legible" en un período razonable de tiempo. Se recogen expresamente en otras secciones del capítulo 8 como registros susceptibles de ser llevados con tecnología de registros distribuidos el listado de socios con derecho a voto en la junta general, el de las acciones parcialmente desembolsadas, las acciones dadas en garantía, la delegación del derecho de voto y el registro de transmisión de acciones. Tras siete años de vigencia de la nueva legislación en Delaware, que nos conste, no se ha implantado de forma masiva la llevanza de registros societarios con tecnología de registros distribuidos por las sociedades allí domiciliadas. Probablemente los elevados costes de implantación y la continua evolución en el desarrollo de esta tecnología llevan a la sociedad a esperar prudentemente nuevos avances en su aplicación.

refiere el artículo 116 LSC, añadiéndose cuantos datos se consideren necesarios, por ejemplo, el código LEI o el ISIN de los valores si la sociedad es cotizada[19].

Estos datos pueden ser toquenizados al no existir norma legal que lo impida. Se trata además de registros internos societarios no de libre acceso –sin perjuicio de que la CNMV pueda acceder a ellos en el ejercicio de sus facultades de policía administrativa– y por tanto estaríamos ante una red permisionada[20].

A continuación, expondremos los principales registros societarios en TRD que pueden crearse por la sociedad anónima a propósito de la celebración de la junta general y los problemas que podría solucionar el recurso a esta tecnología.

2.3. El ejercicio de los derechos del socio a través de sistemas basados en la TRD en las juntas generales de las grandes sociedades

En el ámbito interno societario, hemos indicado que nada impide toquenizar los derechos del socio, todos o algunos de ellos, de manera que se facilite su ejercicio sin necesidad de realizar una reforma legal, por ejemplo, para toquenizar el derecho de asistencia y de voto en las juntas generales de las sociedades cotizadas (o su delegación)[21]. Iberdrola ha sido la primera cotizada española del Ibex 35 en utilizar una red blockchain para el registro de la asistencia telemática, la delegación o el voto del accionista en su junta general del 2022.

---

[19] Palá Laguna, R. (2021). "Digitalización de registros societarios", *Cuadernos de Derecho para Ingenieros*, 54, pp. 88-110.

[20] Como se indica para las sociedades cotizadas en el preámbulo de Ley 5/2021, de 12 de abril, por la que se modifica la LSC "el carácter anónimo de los socios se reputa respecto de terceros como consecuencia del carácter capitalista y no personalista de la sociedad y del privilegio de la limitación de la responsabilidad; pero no es consustancialmente aplicable en el plano interno".

[21] Plantea como una posible aplicación de la TRD la gestión de la privación del derecho de voto al socio moroso y su exclusión en el cobro del dividendo mientras persista esta situación, así como la venta de sus acciones o participaciones (arts. 83 y 84 LSC) Sanjuan y Muñoz, E. (2021), "Aplicación de la tecnología blockchain al funcionamiento de las sociedades de capital y los medios judiciales de control", en *Estudios sobre Derecho digital*, R. Perea Ortega (coord.), Aranzadi, pp. 757-616, epígrafe VI.1 de la versión digital. Lógicamente en España ello no es viable en el caso de sociedades cotizadas, al estar en la práctica todas las acciones íntegramente desembolsadas. Por otra parte, este autor analiza la admisión *ex art.* 299 LEC de la prueba telemática (TRD) en juico, siendo los principales problemas al respecto el acceso a las fuentes de prueba y los criterios de valoración por el juez (*op. cit*. ep. VI.2).

En la doctrina extranjera se ha defendido que la TRD podría ayudar a mejorar la participación del socio especialmente en la junta general[22]. Sin embargo, nosotros no podemos afirmar que exista relación directa entre el recurso a esta tecnología para el ejercicio de los derechos del socio y un mayor activismo accionarial, en el sentido de que pueda solucionar el problema de la constatada apatía racional de los miles de accionistas dispersos de las grandes cotizadas[23].

Pero podría contribuir a garantizar el efectivo conocimiento por la sociedad de la identidad de sus accionistas –derecho que le reconoce el art. 497 LSC–así como a facilitar la comunicación entre la sociedad y sus socios[24] y el ejercicio de los derechos del socio, en la medida en la que estamos ante una tecnología de registro distribuido que permite delegar los derechos de asistencia y voto o votar a través del sistema, por mencionar dos de sus aplicaciones más evidentes[25]. Si el

---

[22] Panisi, F., Buckley, R. y Arner, D. (2023). "Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance?", 2 *Stanford Journal of Blockchain Law and Policy* 2019. Con matices, Lafarre, A. y Van der Elst, C., "The Viability of Blockchain in Corporate Governance", junio. *ECGI Law Working Paper* 712/2023, disponible en https://ssrn.com/abstract=4483621

[23] La apatía racional del accionista es un fenómeno bien estudiado por la doctrina estadounidense y, en España, ya por Trías Sagnier, M. (1998) *Los Inversores Institucionales y el Gobierno de las Grandes Sociedades*, McGraw Hill, Madrid, pp. 48 y ss. Con posterioridad, Herrero Morant, R. (2019), entiende que el accionariado disperso podría continuar sin emitir su voto pese a la existencia de una red *blockchain* para hacerlo en *Los inversores institucionales en las sociedades cotizadas españolas: caracterización y activismo accionarial*, Marcial Pons, Madrid, p. 288. Muy crítico con las bondades de esta tecnología para revitalizar el papel de la junta ("los apáticos racionales seguirán siéndolo con o sin *blockchain);* Portellano Díez (2021), "Repercusión de la tecnología *blockchain* sobre el órgano de administración", *Cuadernos de Derecho para Ingenieros* 54, pp. 131-148, p. 137; y Peinado, J. I. y Bednardz, Z. (2021), "Cuestionando las bondades de la "blockchain" en las juntas generales", *RdS* 61, versión digital, *passim.* Noval Pato apunta que no parece que la clave para lograr la revitalización de la junta resida en una reforma técnica para una mejor canalización de la participación de los inversores en la junta (Noval Pato, J. (2022). "Sociedades mercantiles y digitalización de la actuación de los órganos", en AA. VV. *Blockchain: aspectos jurídicos de su* utilización, E. Valpuesta y J.C. Hernández Peña (dirs.), La Ley, Madrid, pp. 205-237, p. 228).

[24] Lafarre, A. y Van der Elts, C. (2021). "Shareholder Voice in Complex Intermediated Proxy Systems: Blockchain Technology as a Solution?", 4 *The Stanford Journal of Blockchain Law and Policy*.

[25] Sobre los problemas que se plantean en las grandes cotizadas en relación con el derecho de voto en las juntas generales, un interesante análisis en BEDNARDZ, Z. (2020), "El uso de la tecnología Blockchain para el ejercicio del derecho de voto por los socios", *Derecho de sociedades: los derechos del socio*, B. González Fernández y A. Cohen Benchetrit (dirs.), Tirant lo blanch, Valencia, pp. 523-544, esp. pp. 526 y ss. Gallego Lanau (2021) analiza con detalle la TRD como

socio puede fácilmente ejercitar estos derechos políticos y comprobar además que efectivamente su ejercicio consta en el registro, podría ser un instrumento más eficaz que los existentes para el fomento del ejercicio de los derechos del socio.

2.3.1. *La elaboración de la lista de asistentes a la junta*

Como paso previo al análisis de las dos cuestiones planteadas *supra,* la toquenización de la identidad del socio –de sus datos–, permitiría elaborar con mayor precisión temporal la lista de socios legitimados para asistir a la junta general de la sociedad, registro que serviría de base para la elaboración de la lista de asistentes (presentes o representados) en la concreta reunión del órgano[26]. La acreditación de la identidad del socio que permita su incorporación al listado de socios legitimados, probablemente por el momento se ha de realizar *off chain* con la colaboración de las entidades depositarias de las acciones de la cotizada y del depositario central de valores[27]. Esta acreditación de la identidad puede instrumentarse a través de sistemas de identidad digital como puede ser el de la

---

plataforma que permitiría articular todas las fases de la junta, desde el anuncio de la convocatoria hasta la aprobación del acta, en "El funcionamiento virtual de la junta general de las sociedades de capital y *blockchain*", AA. VV. *El sistema jurídico ante la digitalización. Estudios de Derecho privado,* M. Paniagua Zurera (dir.), Tirant lo Blanch, Valencia, pp. 441-462. García Mandalóniz (2020) plantea la posibilidad de una junta general *blockchanizada* con algunas referencias a ensayos al respecto en *Una sociedad mercantil simplificada y digitalizada. Un ecosistema emprendedor innovador, inclusivo y sostenible*, Dykinson, pp. 273 y ss.

Defiende una aplicación prudente y más realista de la TRD con carácter complementario en algunas fases del proceso de votación en la junta, Gallego Corcoles, A. (2019), "El *blockchain* en la junta general", en AA. VV: *Revolución digital, Derecho mercantil y token* economía, A. Muñoz Pérez (dir.), Tecnos, Madrid, pp. 306-339.

[26] M*utatis mutandis*, respecto a la configuración de la lista de asistentes, sería de aplicación el art. 182 bis 4 LSC previsto para la junta exclusivamente telemática ("El anuncio de convocatoria informará de los trámites y procedimientos que habrán de seguirse para el registro y formación de la lista de asistentes, para el ejercicio por estos de sus derechos y para el adecuado reflejo en el acta del desarrollo de la junta. La asistencia no podrá supeditarse en ningún caso a la realización del registro con una antelación superior a una hora antes del comienzo previsto de la reunión).

[27] Sobre la posibilidad de acreditar la identidad del socio a través de la *blockchain* (autenticación criptográfica), v. Recalde Castells, A. (2022), "Comentario al artículo 189", en AA. VV., *La junta general de las sociedades de capital: Comentario de los artículos 159 a 208 LSC,* J. Juste y A. Recalde (coords.), Cívitas, Madrid, pp. 501-513, parágrafo 25 y la bibliografía allí citada.

Fábrica Nacional de Moneda y Timbre, a la espera de la aprobación del Reglamento e-IDAS 2[28].

En el derecho español, el art. 179.3 LSC recoge un sistema de legitimación anticipada del accionista en virtud del cual la sociedad no puede impedir el ejercicio del derecho de asistencia a los socios que con cinco días de antelación a la fecha de la celebración de la junta general tengan inscritas sus acciones, en el caso de las cotizadas, en el registro de anotaciones en cuenta (fecha de registro o *record date*)[29]. Estatutariamente puede establecerse un plazo más breve[30]. Contar con un registro de socios en TRD a los efectos de su legitimación para asistir a la junta, permitiría conocer con certeza la identidad de los socios en un plazo menor de cinco días respecto al *dies ad quem* previsto en el art. 179.3 LSC. Con ello se podría conseguir un registro más exacto de la titularidad accionarial de la sociedad puesto que quedarían reflejadas los cambios en el accionariado posteriores a la *record date* y anteriores a la celebración de la junta general. No queremos decir que actualmente la sociedad cotizada no tenga acceso a la información de los titulares de las acciones representadas por anotaciones en

---

[28] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (COM/2021/281 final). El Parlamento Europeo aprobó el 29 de febrero de 2024 el texto de la Propuesta [P9 TA(2024)0117)], sobre el que se había alcanzado un acuerdo con el Consejo en julio de 2023. La norma crea una "cartera europea de identidad digital", definida como un medio de identificación electrónica que permite al usuario almacenar, gestionar y validar de forma segura datos de identificación de la persona y declaraciones electrónicas de atributos con el fin de proporcionarlos "a las partes usuarias y a otros usuarios de carteras europeas de identidad digital", así como firmar por medio de firmas electrónicas cualificadas o sellar por medio de sellos electrónicos cualificados" (nuevo apdo. 42 del art. 3 del Reglamento de 2014), cartera digital que se construye con técnicas criptográficas a través de los proveedores de servicios de confianza y cuyos datos estarán encriptados de forma que sólo su titular pueda operar con ella con autenticación reforzada.

[29] Para las anotaciones en cuenta, recuérdese que en virtud de lo dispuesto en el art. 11 TRLMV, la inscripción de la transmisión de los valores anotados a favor del adquirente "producirá los mismos efectos que la tradición de los títulos" Para los tokens, "La transmisión de los valores representados mediante sistemas basados en tecnología de registros distribuidos tendrá lugar mediante la transferencia registrada en el registro distribuido". La persona que aparezca legitimada en los asientos del registro contable o en el sistema basado en tecnología de registros distribuidos se presumirá titular legítimo y, en consecuencia, podrá exigir de la entidad emisora que realice en su favor las prestaciones a que dé derecho el valor negociable (art. 13 LMV).

[30] León Sanz, F., "Comentario al artículo 179", en AA. VV. *La junta general de las sociedades de capital: Comentario de los artículos 159 a 208 LSC,* cit., pp. 357-380, parágrafo 83.

cuenta –esta información se la proporciona el depositario central de valores–, sino que la sociedad, por medio de su propio registro distribuido, tenga acceso inmediato a esta información

Con la tecnología de registros distribuidos, la sociedad puede conocer la identidad real de sus socios a través del registro de acciones (art. 497 LSC y art. 25 del Real Decreto 814/2023), identidad que puede no coincidir en todo caso con los titulares inscritos en la fecha de registro. No entramos en este epígrafe en la determinación del accionista último (beneficiario último, *beneficial owner*) de las acciones en el caso de que estén depositadas en un custodio internacional de valores al analizarlo en el epígrafe siguiente. En estos casos, consta en el registro como titular registral la entidad depositaria, lo que también sucede en otros casos de titularidades fiduciarias de los intermediarios financieros, cuestiones estudiadas por nuestra doctrina a las que se refiere, por ejemplo, el art. 497 LSC[31].

Lo que en un principio pudiera considerarse que beneficia al consejo de administración, que en teoría va a conocer con suficiente antelación (mínimo cinco días) quién podrá ejercer el derecho de voto en la junta, máxime cuando la mayoría de los minoritarios que lo delegan lo han hecho a través de la entidad de crédito o sociedad de valores en la que están depositadas las acciones (art. 522 bis LSC), puede volverse en su contra, ya que la práctica es muy rica y pone de manifiesto la existencia de voto oculto a partir de la fecha de registro (téngase en cuenta que si la participación es significativa, se ha de comunicar *ex art*. 105 LMV). Estas anomalías podrían mitigarse con el recurso a la TRD si el toquen reflejara quién está legitimado realmente para el ejercicio del derecho de asistencia y voto en la junta; no olvidemos que las maniobras especulativas se pueden producir en la actualidad no sólo a través de contratos de préstamo de valores, sino también de

---

[31] Perdices Huetos, A. (2016). "Estructura del accionariado e intervención de intermediarios financieros: ejercicio del voto y otorgamiento de delegaciones de voto por parte de entidades intermediarias titulares de los registros contables", en AA. VV., *Junta general y consejo de administración en la sociedad cotizada,* F. Rodríguez Artigas *et al.* (dir.), Tomo I, Aranzadi, pp. 803-814 y la bibliografía allí citada. Con datos de la CNMV (excluidos los casos de cotitulatidad de las acciones), la participación de los inversores minoristas en el total de las compras negociadas del Ibex 35 se situó en 2023 en el 7,4% (6,2% en 2022) y en el total de las ventas fue del 9,1% (7,0% en 2022) (Comunicado CNMV de 28 de febrero de 2024, *La participación de los inversores minoristas en bolsa prosiguió su crecimiento en 2023*). Al cierre del año 2022, la participación de las familias en sociedades cotizadas se situó en el 16,2% del total de inversores (*Informe BME sobre la propiedad de las acciones españolas cotizadas*, 2023, p. 8).

derivados financieros por los que el socio se obliga a delegar su voto en la contraparte del derivado. La TRD podría ser una técnica útil para la sociedad, en la medida en la que puede conocer con escasas horas de antelación a la celebración de la junta la persona legitimada para el ejercicio del derecho de voto.

De hecho, el legislador, para el caso concreto de las entidades de crédito y empresas de servicios de inversión que se encuentren en algunas de las situaciones previstas en la Ley 11/2015, de 18 de junio, de recuperación y resolución de entidades de crédito y empresas de servicios de inversión, permite a estas entidades –previa constancia estatutaria– la convocatoria de la junta en un plazo inferior a un mes para decidir sobre una ampliación de capital, siempre y cuando dicha junta no se celebre en un plazo inferior a diez días a partir de la convocatoria, y la ampliación de capital sea necesaria para evitar las condiciones de resolución bancaria o de empresas de servicios de inversión. Pues bien: en este caso no se aplicarán los plazos previstos en el art. 179.3 LSC (disp. ad. décima 2. LSC). No se recoge en esta disposición adicional un sistema alternativo al de la *record date*, probablemente porque se está pensando en entidades de crédito cotizadas, que acudirán a los datos que les proporciona Iberclear para elaborar el listado de socios de la sociedad en dificultades financieras que pretende acogerse a la situación de actuación temprana prevista en los artículos 8 y siguientes de la Ley 11/2015. En el bien entendido de que en los registros de Iberclear no necesariamente aparecerá el socio beneficiario último sino, en ocasiones, el intermediario financiero custodio de las acciones.

Ante dificultades financieras graves de estas entidades, se trata de agilizar la convocatoria y celebración de la junta que acuerde en su caso la ampliación de capital. Prevalece el interés superior del buen funcionamiento del sistema financiero frente al derecho de asistencia del socio que tiene inscritas a su nombre las acciones con cinco días de antelación al de la celebración de la junta o en un plazo menor si los estatutos de la entidad de crédito cotizada así lo han establecido. Este precedente en materia de supresión del sistema de la fecha de registro puede ser un argumento más para eliminar la previsión del artículo 179.3 LSC, aunque por razones distintas, en los casos en los que la tecnología permita un sistema de legitimación del socio para asistir a la junta que enerve la prohibición recogida en este precepto.

No debe olvidarse que la Directiva sobre derechos de los accionistas de sociedades cotizadas permite a los Estados miembros no aplicar el sistema de

la *record date* "a las sociedades que puedan determinar el nombre y la dirección de sus accionistas a partir de un registro de accionistas actualizado el día de la junta general"[32]. Con ello estamos yendo más allá del listado de accionistas registrados elaborado por la entidad encargada de la llevanza del registro contable de las acciones. Un sistema basado en la TRD podría agilizar el proceso y prescindir de los intermediarios financieros, si bien habría de contarse con su colaboración para, en el caso de que no se admita finalmente por el legislador la representación generalizada de las acciones mediante toquens, elaborar la lista de accionistas de partida que se incluirán en el registro distribuido.

2.3.2. *El uso de la TRD para conocer la identidad del socio*

La reforma de la LSC operada en 2021, por la necesaria transposición de la normativa europea[33], reconoce a la sociedad en el nuevo artículo 497 bis el derecho a conocer la identidad de los beneficiarios últimos de las acciones en los casos en los que la persona legitimada como accionista en virtud del registro contable sea una entidad intermediaria que custodia las acciones por cuenta de beneficiarios últimos o de otra entidad intermediaria (es frecuente la existencia de cadenas de intermediarios financieros).

En el sistema establecido por la LMV (sistema de doble escalón), junto con el registro que lleva el depositario central de valores (Iberclear) aparecen las entidades financieras en las que están *depositadas* las acciones de la sociedad, entidades financieras que conocen la identidad de los accionistas que con ellas han celebrado el contrato de depósito y administración de valores[34]. El problema viene

---

[32] Art. 7.2, 2º párr., de la Directiva 2007/36/CE del Parlamento Europeo y del Consejo, de 11 de julio sobre el ejercicio de determinados derechos de los accionistas de sociedades cotizadas.

[33] Directiva 2017/828 del Parlamento Europeo y del Consejo de 17 de mayo de 2017 por la que se modifica la Directiva 2007/36/CE en lo que respecta al fomento de la implicación a largo plazo de los accionistas en las sociedades cotizadas. Algunos contenidos de esta directiva fueron incorporados al derecho español con casi dos años de retraso. Con datos de diciembre de 2023, somos el cuarto país por la cola –superados sólo por Bélgica, Portugal y Bulgaria– en la transposición de las directivas europeas relacionadas con el mercado único (https://single-market-scoreboard.ec.europa.eu/enforcement-tools/transposition_en).

[34] En sede de cotizadas, son los depositarios centrales de valores (primer escalón) quienes han de informar al emisor sobre la identidad de sus accionistas. La norma reglamentaria les obliga a establecer procedimientos para informar a la sociedad de la identidad de sus beneficiarios últimos, entendiendo por tales a los referidos en el artículo 497 bis LSC y habrán de prestar también "sin que ello pueda implicar el mantenimiento en los mismos de ficheros permanentes, el servicio

con las acciones titularidad de inversores extranjeros que pueden estar en manos de custodios internacionales de valores que son quienes aparecen como titulares del registro de valores anotados (y no el beneficiario último[35]).

Por ello se ha afirmado que la TRD puede ser una solución que aporte claridad al problema de la titularidad real de las acciones, reduciendo la necesidad de servicios de intermediación entre el emisor y los inversores. Pero como indican las Autoridades Europeas de Supervisión en materia bancaria y de mercados de valores (EBA y ESMA, respectivamente, por sus acrónimos en inglés),

---

de canalización de las solicitudes que las sociedades formulen con ocasión de la celebración de cualquier Junta general y con referencia a la fecha contemplada en el artículo 179" de la LSC. Las entidades que integran el segundo escalón, participantes de los depositarios centrales de valores, están obligadas a facilitarles los datos necesarios para el adecuado cumplimiento de sus obligaciones de suministro a emisores de información sobre titularidades y beneficiarios últimos (art. 25 RD 814/2023, de 8 de noviembre). En el Reglamento de Iberclear, depositario central de valores que presta, como servicio auxiliar, la "tramitación de actuaciones societarias", como las relativas a "la asistencia a juntas generales y de información", se detalla esta función de canalizar (art. 26. 2) "hacia sus entidades participantes las solicitudes que realicen las entidades emisoras para conocer la identidad de sus accionistas con ocasión de la celebración de Junta General o en cualquier momento en que lo soliciten para poder comunicarse con sus accionistas en los términos previstos en la ley". En estos casos, Iberclear facilitará a la entidad emisora la relación de titulares de sus respectivos valores a una fecha concreta, incluidas las direcciones y medios de contacto que faciliten las entidades participantes. V. asimismo la norma 6.ª de la Circular núm. 04/2016, de 29 de enero, de Iberclear que permite a las entidades emisoras solicitar del depositario central "la comunicación diaria de los datos de titularidad relativos a operaciones liquidadas que se realicen sobre sus acciones o participaciones". Una de las pocas previsiones que se han salvado de la purga a la que fue sometido el RD 814/2023 tras el dictamen del Consejo de Estado al que nos referimos en el epígrafe III de este trabajo es la contenida en su art. 25.6 en virtud de la cual la sociedad emisora, el depositario central de valores y sus entidades participantes, podrán exigir a la entidad responsable de la administración y el registro de las criptoacciones la identificación de los accionistas de la sociedad incluidos los beneficiarios últimos. El legislador reglamentario traslada las previsiones para sociedades cotizadas en mercados españoles a las acciones representadas en TRD, entendemos que, en una interpretación prudente, para los supuestos en los que se creen infraestructuras de mercado basadas en esta tecnología.

[35] V. Perdices Huetos, A. (2016). "Estructura del accionariado e intervención de intermediarios financieros: ejercicio del voto y otorgamiento de delegaciones de voto por parte de entidades intermediarias titulares de los registros contables", en AA. VV., *Junta general y consejo de administración en la sociedad cotizada,* F. Rodríguez Artigas et al. (dir.), t. I., Aranzadi, Cizur Menor, pp. 803-814 y la bibliografía allí citada. Los inversores no residentes elevaron hasta al 50,3% su participación en las cotizadas españolas a cierre de 2022, (*Informe BME sobre la propiedad de las acciones españolas cotizadas*, octubre de 2023, p. 5).

contamos con evidencias muy limitadas respecto a la aplicación en la práctica de esta tecnología[36].

La existencia en España del registro de titularidades reales permite conocer la identidad de los accionistas personas físicas que posean o controlen una participación superior al 25% del capital social o de los derechos de voto de una persona jurídica, lo que no es muy útil a nuestros efectos para las sociedades cotizadas, con miles de pequeños accionistas. Más interés tiene en este sentido el registro administrativo de participaciones significativas a cargo de la CNMV, en donde los umbrales de comunicación son inferiores[37]. Por debajo de estos umbrales, la sociedad puede no conocer la identidad del beneficiario último, y tener solo los datos la entidad financiera que actúa como custodio de sus acciones y aparece como titular formal en el registro de valores anotados.

La TRD podría ser una solución para la efectiva aplicación del derecho de la sociedad a conocer la identidad de sus socios (beneficiarios últimos). Aunque quizá no deba llevarse al último extremo este derecho de la sociedad en los casos de titularidad indirecta de acciones: piénsese en el extranjero que deviene socio por su condición de partícipe en un fondo de inversión que invierte en acciones de una cotizada española: la naturaleza de los fondos de inversión, patrimonios sin personalidad jurídica pertenecientes a una pluralidad de inversores, implica que el extranjero es copropietario de un determinado porcentaje del patrimonio del fondo. Si en ese patrimonio se integran acciones de sociedades cotizadas, el copropietario lo es de un determinado porcentaje de cada acción que integra el patrimonio del fondo. En estos supuestos, muy probablemente el inversor no invierte en el fondo para ser socio de una determinada cotizada –más allá de su elección de inversión en un determinado fondo por la cartera de valores que agrupa, integrada por ejemplo por acciones comprendidas en un índice bursátil como Standard & Poor's o el Ibex 35–, ni tiene interés en participar activamente

---

[36] ESMA y EBA, *Report on Implementation of SRD2 provisions on proxy advisors and the investment chain*, 27 de julio de 2023, p. 49.

[37] Sobre el registro de titularidades reales, creado para la prevención del blanqueo de capitales y la financiación del terrorismo, v. la disp. ad. tercera de la Ley 10/2010, de 28 de abril y el Real Decreto 609/2023, de 11 de julio, por el que se crea el Registro Central de Titularidades Reales y se aprueba su Reglamento. Respecto a la obligación de comunicación de participaciones significativas en sociedades cotizadas, el art. 23 del Real Decreto 1362/2007, de 19 de octubre, sitúa el umbral mínimo en el 3% de los derechos de voto.

en la vida societaria; lo hará por la rentabilidad que le ofrece el fondo y quizá también por el prestigio de su sociedad gestora o por su política de sostenibilidad. Por ello, quizá carezca de sentido llevar hasta sus últimos extremos el derecho de la sociedad a conocer la identidad de sus accionistas beneficiarios últimos. Será en principio suficiente la constancia en el registro de socios de la identidad de la sociedad depositaria de instituciones de inversión colectiva o de fondos de inversión alternativos. Siempre además se podría establecer, al modo del registro de los titulares de participaciones significativas en las cotizadas, un registro interno de la sociedad gestora en los casos en los que un partícipe tenga la titularidad de un número elevado de participaciones del fondo.

Los sistemas de registro distribuido no cabe duda de que ofrecen la posibilidad de conocer, con las salvedades expuestas, de manera más sencilla por la sociedad, la identidad de los últimos tenedores de las acciones de las sociedad (*beneficial owners*) cuyas acciones están depositadas a través de largas cadenas de intermediarios. Si bien la práctica evidencia que el funcionamiento de la cadena de intermediarios no impide el cobro de los dividendos por el accionista último, no sucede lo mismo en el caso del ejercicio de otros derechos del socio en las cadenas transfronterizas de intermediarios financieros: las prácticas divergen a lo largo de la Unión Europea en lo que respecta al flujo de información relativa a la identificación del socio, la información sobre eventos corporativos y el ejercicio de derechos políticos del socio[38]. Recordemos que en España la LSC (art. 522 bis) recoge la obligación de las entidades intermediarias legitimadas como accionistas en virtud del registro contable de las acciones y de las que participen en la cadena de intermediarios, de facilitar el ejercicio por los beneficiarios últimos de los derechos inherentes a las acciones custodiadas por ellas, incluido el derecho a participar y a votar en las juntas generales, y de ejercer los derechos derivados de las acciones según la autorización y las instrucciones del beneficiario último y en su interés.

---

[38] ESMA/EBA, *Report on Implementation of SRD2 provisions on proxy advisors and the investment chain,* ESMA32-380-267, 27 de julio de 2023, esp. pp. 35 y ss. En este informe los supervisores europeos proponen establecer un concepto único de accionista a los efectos del ejercicio de sus derechos en la sociedad cotizada.

2.3.3. *La regla de la posesión de un número mínimo de acciones para asistir a la junta*

Si la sociedad decide implantar un sistema de registro distribuido para la identificación de los accionistas que permita acreditar su legitimación para asistir a la junta general, quizá debiera plantearse la innecesariedad de la prohibición contenida en el artículo 521 bis LSC en relación las limitaciones del derecho de asistencia del socio: "los estatutos no podrán exigir para asistir a la junta general la posesión de más de mil acciones", al menos en los casos de juntas íntegramente telemáticas. La legitimación anticipada del socio sirve a los intereses de la sociedad en la medida en que se trata de facilitar la organización de la junta general[39]; la exigencia estatutaria de un número mínimo de acciones para asistir a la junta pretende también evitar una excesiva afluencia física de los socios a la junta de la sociedad; estos siempre pueden agruparse con otros y designar un representante común. La cuestión es si tiene sentido mantener esta prohibición en juntas íntegramente telemáticas en las que por definición no hay presencia física del socio, juntas telemáticas en las que la elaboración (telemática) del registro de los accionistas legitimados para asistir a la junta no supone una carga de trabajo excesiva para la sociedad si se incluyen a todos los accionistas titulares de una acción en adelante. Como tampoco parece serlo, *mutatis mutandis,* en caso de elaborar el registro de socios legitimados a través de la TRD.

2.3.4. *El establecimiento de canales de comunicación para la asistencia personalizada al socio*

Una cuestión relacionada con las juntas íntegramente telemáticas –o el recurso a la TRD para la elaboración de la lista de socios o de personas legitimadas para asistir a la junta–, es si el recurso por la sociedad a la tecnología puede dificultar el acceso de determinados socios que, por diversas razones, tengan problemas con el uso de estas nuevas –o no tan nuevas– tecnologías. En estos casos, la sociedad debiera habilitar canales de información y ayuda para estas personas legas en tecnologías de la información y comunicación a fin de evitar posteriores impugnaciones

---

[39] León Sanz (2022), quien añade, con cita de Girón Tena, que el precepto (ya previsto en la LSA de 1951) también pretende evitar maniobras especulativas anteriores a la celebración de la Junta general (León Sanz, F., "Comentario al artículo 179", cit., parágrafo 79). Sin embargo, como hemos indicado, la irrupción en el mercado de los contratos de derivados financieros permite estas maniobras especulativas al margen del accionista que aparece legitimado para asistir a la junta *ex art*. 179.3 LSC.

de acuerdos sociales cuando el socio no ha podido ejercitar su derecho de asistencia a la junta ante las dificultades que le plantea el programa informático puesto a su disposición por la sociedad. No es tanto una cuestión de canales de comunicación con la sociedad cuanto de permitir en todo caso la opción de requerir intervención humana a fin de cumplir con estas actuaciones previas del socio de cara a la celebración de la junta íntegramente telemática, o para el acceso al sistema de registro distribuido que ha de utilizar, por ejemplo, para delegar su derecho de asistencia. No nos constan problemas al respecto en juntas presenciales en el caso de accionistas que carezcan de oficina bancaria en su localidad –las entidades de crédito actúan como entidades depositarias de las acciones de las cotizadas– a la hora de tramitar por la cotizada sus delegaciones de asistencia y voto en la junta general, puesto que normalmente la documentación se remite al socio por correo postal y las entidades financieras contactan telefónicamente con el socio a fin de comprobar la efectiva recepción por el accionista de la documentación relativa a la junta general (orden del día, tarjeta de asistencia, de delegación de la representación y de voto a distancia). Ello es así especialmente en los casos en los que se prevean problemas por la cotizada para alcanzar un determinado quórum de asistencia a la junta.

Una solución en el caso de dificultades para el socio con el recurso a la tecnología a la hora de delegar su derecho de asistencia y voto o de ejercer su voto a distancia, podría ser la que se ofrece en la futura reforma del artículo 197 LMV respecto a la prestación personalizada de servicios de inversión; las empresas de servicios de inversión –y las entidades de crédito autorizadas para la prestación de servicios de inversión y de servicios auxiliares, como es la custodia y administración por cuenta de clientes de los instrumentos financieros– "asegurarán a su clientela la disponibilidad de canales presenciales, ya sea permanentes o intermitentes, o telefónicos o telemáticos para la prestación de servicios de inversión, atendiendo al principio de prestación personalizada. Se entiende por prestación personalizada aquella que tiene en consideración la edad, la situación de discapacidad de la persona a la que está prestando o va a prestar servicios de inversión, las características de la zona geográfica en la que reside la persona en términos de población y el nivel de competencias digitales de dicha persona, entre otras cuestiones"[40].

---

[40] Anteproyecto de Ley por la que se crea la Autoridad Administrativa Independiente de Defensa del Cliente Financiero para la resolución extrajudicial de conflictos entre las entidades financieras y sus clientes, de diciembre de 2023 (disp. final decimoctava, de modificación de este art. 197 LMV).

Pero la participación a distancia del socio, sea por correspondencia postal, electrónica o por cualquier otro medio de comunicación a distancia en los términos del artículo 521 LSC, no le permite conocer si efectivamente, una vez cumplimentada por él, el documento o la participación a través de internet ha sido recibida por la sociedad y ha sido efectivamente computado su voto a distancia ni, en el caso de que hubiera dado instrucciones de voto, si estas han sido seguidas por el representante designado para asistir a la junta y votar en su representación. De esta cuestión nos ocupamos a continuación.

2.3.5. *La aplicación de la TRD en la comprobación de la delegación del derecho de asistencia y voto*

En el marco de las diversas aplicaciones de la TRD a propósito de la celebración de la junta[41] uno de los problemas que se pueden plantear en la práctica es cómo puede el socio comprobar que la delegación del derecho de asistencia y voto en un tercero ha sido efectivamente computada por la mesa de la junta. Especial interés tiene la cuestión de que pueda conocer el socio si efectivamente se han registrado correctamente las instrucciones de voto que en su caso haya podido impartir al representante. En la actualidad, como hemos indicado, el artículo 521 LSC habilita a las sociedades cotizadas para permitir la participación a distancia del socio en los términos establecidos en sus estatutos, bien en formato cartular, bien en formato electrónico. El artículo 527 bis LSC obliga a la sociedad a enviar al accionista que emite su voto por medios electrónicos la confirmación electrónica de la recepción de su voto. Pero el socio –especialmente el pequeño inversor– no tiene forma de conocer fácilmente si en la adopción de los acuerdos sociales se ha tenido en cuenta, por ejemplo, su orden de abstención en la votación de un determinado punto del orden del día, su voto a favor o su voto negativo[42].

---

[41] Sobre los distintos modelos de implementación del voto a través de la TRD en la junta general, v. Jiménez Gómez, B.S. (2022), "El derecho de voto en las sociedades cotizadas a través de la tecnología *blockchain*", *Revista de Derecho Bancario y Bursátil,* 168, pp. 141-170, epígrafe VI. 3 de la versión digital.

[42] Como indica Recalde, no hay garantías de que ese voto haya sido computado. Recalde Castells, A., "Comentario al artículo 189", en AA. VV., *La junta general de las sociedades de capital: Comentario de los artículos 159 a 208 LSC*, cit., parágrafo 18. Plantea la desconfianza que genera esta situación Gallego Lanau, M., "El funcionamiento virtual de la junta general de las sociedades de capital y *blockchain*", en AA. VV., *El sistema jurídico ante la digitalización. Estudios de*

Instrumentar telemáticamente esta posibilidad a través de un sistema basado en la TRD permitiría al socio conocer que efectivamente se ha registrado el sentido de su voto[43]. Si bien el socio no necesariamente tiene los conocimientos informáticos suficientes para entrar en la red, sea a través de su participación en la cadena de bloques, sea a través de otro sistema de validación de las transacciones, existen hoy en día aplicaciones como *blockchain explorer* que funcionan, por decirlo gráficamente, como un *google* en la *blockhain*, de forma que el socio con el *hash* remitido por la sociedad al registrar la toquenización de sus derechos de asistencia y voto que va a ejercer mediante delegación, podría encontrar en el registro de votos la efectiva inclusión de su voto en el cómputo de la aprobación o rechazo de cada uno de los acuerdos sociales que figuran en el orden del día.

3. LA TRD *AD EXTRA*: LA FINANCIACIÓN DE LA SOCIEDAD

3.1. La posibilidad de instrumentar los valores negociables en toquens

Hemos optado por incluir en este epígrafe una cuestión fundamental cual es la del reconocimiento en el derecho español con carácter general de criptoacciones y cripto-obligaciones, esto es, si es posible de *lege data* en nuestro país la emisión de acciones y de obligaciones representadas mediante sistemas basados en TRD, como una tercera forma de representación de derechos-valor junto con los títulos y las anotaciones en cuenta. Si bien la LMV reconoce estas tres formas de representación de los valores negociables en su artículo 6[44], la respuesta, en

---

Derecho privado, cit., p. 447. En la junta general de Procter & Gamble de 2017, un inversor titular de una participación significativa pretendía un puesto de consejero en la sociedad. Perdió la votación con un margen de 0,2%. El inversor solicitó un recuento independiente que reveló que se había aprobado su nombramiento por un margen del 0,0016%. Otro recuento demostró que el margen de votos en su contra fue de medio millón. Después de meses de recuentos de votos discrepantes en cuanto al resultado de la votación, la sociedad le ofreció a este inversor un puesto en el consejo de administración, sin que se resolviera definitivamente el problema de los votos que llevaron al rechazo de su nombramiento en la junta (Daniels, A., 2018) "Blockchain & shareholder voting: a hard fork for 21st-century corporate governance", *University of Pennsylvania Journal of Business Law*, 405, pp. 405-441, p. 422.

[43] Algunas experiencias sobre el ejercicio del derecho de voto a través de una *blockchain* ya en Gallego Corcoles, A., "El *blockchain* en la junta general", cit., pp. 313 y ss.; v. asimismo Bednardz, Z. (2020), "El uso de la tecnología *blockchain* en las sociedades cotizadas: la implicación de los accionistas", *Revista de Derecho de Sociedades,* 58, epígrafe III.2 de la versión digital.

[44] Art. 6.1 LMV: "Los valores negociables podrán representarse por medio de anotaciones en cuenta, títulos o sistemas basados en tecnología de registros distribuidos. La modalidad

nuestra opinión, requiere un análisis previo del derecho europeo de los mercados de valores. De ser afirmativa, es necesario delimitar el alcance de la extensión de esta tercera forma de representación de las acciones en las sociedades anónimas, en las que se patrimonializa la posición jurídica del socio a través de los valores negociables[45]. Esta cuestión está directamente relacionada con los efectos que el ordenamiento español anuda a la suscripción o transmisión de estos valores mobiliarios, ya representados directamente en TRD desde su emisión, ya toquenizados una vez que han sido emitidos.

La seguridad jurídica en la transmisión de los criptoactivos o toquens –la eficacia y oponibilidad de su transmisión frente a terceros– es esencial para permitir su emisión y circulación en el tráfico económico. De lo que se trata es de analizar si la ficción jurídica que ha permitido la ágil transmisión de los derechos mediante su corporeización en un título valor, ficción jurídica sobre la que se construyó el régimen de las anotaciones en cuenta –valores representados digitalmente– en la LMV de 1988, permite establecer una tercera *fictio iuris* para el reconocimiento de los valores representados mediante sistemas basados en TRD como derechos-valor transmisibles a través de registros distribuidos (ejecución del *smart contract*) con plena eficacia frente a terceros.

En nuestra opinión, la seguridad jurídica al respecto sólo se predica en un determinado ámbito delimitado por el Reglamento de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras de mercado basadas en TRD[46], al que la LMV anuda la admisión a *negociación* de acciones y obligaciones representadas en TRD en un determinado mercado (sistema multilateral de negociación). Pero no cualquier acción u obligación, sino sólo de las de aquellas sociedades

---

de representación elegida habrá de aplicarse a todos los valores negociables integrados en una misma emisión".

[45] Alonso Ureba, A. (2023). "Derecho de sociedades y función económico social de la gran empresa ("interés social" vs "interés de empresa": Una cuestión abierta)", en AA. VV., *Derecho de sociedades y sostenibilidad,* C. Chamorro y J. A. Viera (coords.), La Ley, Madrid, pp. 27-92, p. 11 de la versión digital.

[46] Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado. Este Reglamento modifica el art. 4.1.15 de la MiFID II para incluir en la definición de instrumento financiero a "aquellos que se hayan emitido mediante tecnología de registro descentralizado", previsión incorporada al art. 2.2 de la LMV.

que cumplan determinados requisitos previstos en el reglamento europeo[47]. Ello es así porque la LMV únicamente extiende el régimen previsto, *mutatis mutandis*, para los valores representados mediante anotaciones en cuenta –*fictio iuris* sobre la *fictio iuris* de la corporeización del derecho en los títulos-valor– a los representados mediante TRD en los casos en los que las acciones y las obligaciones estén admitidas en un sistema multilateral de negociación autorizado al amparo del citado reglamento europeo[48].

La inminente aplicación directa el 23 de marzo de 2023 del reglamento europeo llevó al legislador español a incluir unas apresuradas previsiones *de minimis* en la LMV de 17 de marzo de 2023, esto es, a reconocer la posibilidad de emisión, registro y transmisión de instrumentos financieros mediante sistemas basados en la TRD (art. 2.1 LMV[49]) en el marco del reglamento sobre un régimen

---

[47] El art. 3 del reglamento circunscribe su ámbito subjetivo a las acciones y obligaciones emitidas o negociadas en TRD por sociedades de capital, en el caso de las acciones, a las de sociedades de mediana capitalización bursátil (hasta 500 millones de euros, la mayoría de nuestras cotizadas en el mercado continuo). Para las obligaciones, han de ser emisiones de importe moderado (hasta mil millones de euros).

[48] Art. 6.2 LMV: "Los valores negociables admitidos a negociación en centros de negociación estarán necesariamente representados mediante anotaciones en cuenta o mediante sistemas basados en tecnología de registros distribuidos *en el marco del Reglamento UE 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022*" (cursiva nuestra).

[49] Decimos "apresuradas previsiones" puesto que, si bien la LMV reforma el art. 517 de la LEC y se reconocen como títulos que llevan aparejada ejecución los certificados no caducados expedidos por las "entidades responsables de la administración de la inscripción y registro respecto de los valores representados mediante sistemas basados en tecnología de registros distribuidos a los que se refiere la Ley del Mercado de Valores siempre que se acompañe copia de la escritura pública de representación de los valores o, en su caso, de la emisión, cuando tal escritura sea necesaria, conforme a la legislación vigente", el legislador omitió la reforma del art. 270 5.º de la Ley Concursal y no se contemplan como acreedores con privilegio especial (como sí se hace sobre los valores gravados con los titulares de créditos con garantía de valores representados mediante anotaciones en cuenta), a los titulares de créditos con garantía de valores representados mediante TRD. con lo que se deja sin valor esa garantía en el caso de que el deudor concedente devenga insolvente (v. Gónzalez Vázquez, J. C., entrada "Píldoras mercantiles: aprobación de la ley 6/2023, de 17 de marzo, de los mercados de valores y de los servicios de inversión: aspectos relevantes (III)", 3 de marzo de 2023, disponible en https://www.linkedin.com/pulse/pildoras-mercantiles-aprobaci%25C3%25B3n-de-la-ley-62023-17-y-jos%25C3%25A9-carlos-1e/?trackingId=Gt8JTPdiQwqkdgL8c3M2Ag%3D%3D

piloto, confiando al desarrollo reglamentario de la Ley la concreción de ulteriores aspectos, desarrollo reglamentario que aún no se ha producido[50].

En la LMV se parte de un modelo en cierta medida centralizado[51], desde el momento en el que ha de existir siempre un organismo rector o responsable del mercado secundario en el que se negocien los valores representados mediante sistemas basados en la TRD, sociedad rectora que ha de contar con la previa autorización administrativa de la CNMV. El modelo centralizado que se manifiesta también, al igual que sucede con las anotaciones en cuenta, en la existencia de una entidad encargada de la administración y registro de los valores representados en TRD (art. 8 LMV), que ha de ser una entidad de crédito o una sociedad de valores. Ello se confirma si atendemos al régimen de supervisión, inspección y sanción de la LMV, al declarar sujetas a este régimen, a cargo de la CNMV, a las entidades responsables de la administración de la inscripción y registro de los valores negociables representados mediante sistemas basados en TRD "conforme a lo dispuesto en esta ley y en su normativa de desarrollo y en la normativa europea de aplicación" [art. 232.1. a) 12.º LMV], tipificándose en el artículo 279 como infracciones muy graves y graves una serie de conductas en relación con la representación de los valores negociables, entre las que se recogen la atribución por el emisor de la responsabilidad de la administración de la inscripción y registro de los criptovalores a una entidad no autorizada para esta actividad [art. 279.1.e) LMV]. Quizá por ello los redactores de la LMV han preferido la expresión "tecnología de registro distribuido" frente a la utilizada en la versión española del reglamento sobre un regimen piloto, que se refiere a la tecnología de registro descentralizado.

---

[50] El Consejo de Estado dictaminó correctamente, respecto a la inclusión del desarrollo del régimen de los criptovalores negociables en el hoy Real Decreto 814/2023 sobre instrumentos financieros que "un Gobierno en funciones no puede aprobar el régimen jurídico reglamentario que ha de aplicarse a los instrumentos financieros de estas características". Por ello, se suprimieron de este Real Decreto 814/2023, de 8 de noviembre de 2023, con carácter previo a su publicación en el BOE, el grueso de los desarrollos en materia de criptovalores o, en general, de criptoinstrumentos financieros.

[51] Modelo centralizado que es, parece, por el que va a optar el legislador europeo a propósito del euro digital. Estaríamos ante un sistema híbrido, al combinarse la TRD con la gobernanza del registro por el Banco Central Europeo (v. SANZ BAYÓN, P., "Emisión y regulación del dinero público digital: análisis de las monedas digitales de Banco Central", *RDMV*, 29, 2021, epígrafe II).

Por las razones expuestas, carecemos de un régimen completo sobre los cripto-instrumentos financieros a diferencia de otros ordenamientos jurídicos como el suizo, el italiano, el francés[52] o el alemán; queda la reforma legal limitada –en nuestro caso a los efectos del reglamento sobre un régimen piloto– a los artículos 5 a 15 de la LMV insertos en el capítulo II del título I de la LMV, rubricado "De los valores negociables")[53].

3.2. La toquenización de acciones y obligaciones al margen del derecho del mercado de valores

Con ello no queremos decir que al amparo de la autonomía privada no puedan toquenizarse las acciones de una sociedad anónima y las obligaciones emitidas por las sociedades de capital; pero su transmisión al margen de los mercados (SMN) que puedan crearse en nuestro país en aplicación del reglamento sobre un régimen piloto, se regirá por el derecho contractual: la transmisión

---

[52] V. los arts. 973 d) y ss. del Código Suizo de las Obligaciones, introducidos por la Ley de 25 de septiembre de 2020 sobre la adaptación del derecho federal a los desarrollos de la tecnología de registros electrónicos distribuidos. En Alemania, primero se admitió la representación de valores de deuda y de participaciones de instituciones de inversión colectiva a través de TRD en la *Gesetz über elektronische Wertpapiere* (eWpG), en vigor desde junio de 2021. La *Gesetz zur Finanzierung von zukunftssichernden Investitionen* (ZuFinG) de diciembre de 2023 modifica la eWpG para admitir la emisión de acciones en TRD; habrá de existir una entidad financiera autorizada que asumirá la gestión del registro distribuido. Un listado de las 80 emisiones de *Kryptowertpapiere* registradas en la BaFIN hasta el 14 de marzo de 2024, en https://www.bafin.de/DE/PublikationenDaten/Datenbanken/Kryptowertpapiere/kryptowerte_node.html.
En el Derecho italiano, v. el *Decreto-legge de* 17 marzo 2023 sobre *disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech*. En el Derecho francés, el Decreto 2018-1226 de 24 de diciembre permitió la inscripción de valores de deuda a través de la TRD (*dispositif d'enregistrement électronique partagé*). La reforma del *Code Monetaire et Financier* por la Ley de 9 de marzo de 2023 prevé la posibilidad de inscripción de los valores negociables (*titres financiers*) en un dispositivo de registro electrónico compartido siempre que no se trate de valores sobre los que opera un depositario central de valores (v. art. L211-7 CMF y el Decreto 2023-421 de 31 de mayo de desarrollo reglamentario del CMF).

[53] Además de a otras muy concretas referencias en el art. 40 respecto a emisiones de deuda exentas de folleto objeto de una OPV o de admisión a negociación en un SMN, en el art. 80 (intervención de una entidad de contrapartida central en la liquidación de valores mediante TRD con remisión de su régimen –no producida– al legislador reglamentario, y en los arts. 279 y ss. LMV en relación con las infracciones y sanciones previstas en caso de incumplimiento de determinadas obligaciones incluidas en los arts. 5 a 15 LMV.

de un derecho de crédito toquenizado en una obligación o cualquier otro valor de deuda –transcripciones criptográficas en un registro electrónico–, quedará sometida a las reglas generales del derecho privado al no ser aplicable el régimen de transmisión previsto para los valores emitidos en TRD al amparo del reglamento sobre un régimen piloto en el art. 11 LMV ("La inscripción o registro de la transmisión en el sistema de anotaciones en cuenta o en el sistema basado en tecnología de registros distribuidos, según corresponda, a favor del adquirente, producirá los mismos efectos que la entrega de los títulos"). No creemos extensible, sin expreso reconocimiento legal, el régimen de la protección jurídica del tercer adquirente a estos valores negociables toquenizados fuera del ámbito del reglamento europeo[54]. Dicho en otros términos: no puede extenderse el régimen de los valores anotados a los criptovalores sin expresa previsión legal.

En nuestra opinión, debe realizarse una interpretación prudente de la normativa vigente y negar la posibilidad de emitir acciones directamente en TRD al margen del reglamento europeo. Y ello por varias razones adicionales desde la perspectiva del derecho privado. En primer lugar, la modificación de la LSC por la LMV no ha alterado la redacción del artículo 92.1 LSC ("Las acciones podrán estar representadas por medio de títulos o por medio de anotaciones en cuenta. En uno y otro caso tendrán la consideración de valores mobiliarios") ni del 412 LSC ("Las obligaciones podrán representarse por medio de títulos o por medio de anotaciones en cuenta"). Esto es, en la norma societaria no se contempla con carácter general esta tercera posibilidad de representación de las acciones y de

---

[54] Los principios de legitimación y autonomía en la teoría general clásica sobre los títulos valores, que el legislador extendió a los valores representados mediante anotaciones en cuenta y, respecto a los representados mediante TRD únicamente a los efectos del reglamento sobre un régimen piloto, se recogen en los tres primeros apartados del art. 11 LMV: "1. (...). La transmisión de los valores representados mediante sistemas basados en tecnología de registros distribuidos tendrá lugar mediante la transferencia registrada en el registro distribuido. La inscripción o registro de la transmisión en el sistema de anotaciones en cuenta o en el sistema basado en tecnología de registros distribuidos, según corresponda, a favor del adquirente, producirá los mismos efectos que la entrega de los títulos. 2. La transmisión será oponible a terceros desde el momento en que se haya practicado la inscripción en el sistema de anotaciones en cuenta o en el sistema basado en tecnología de registros distribuidos, según el caso. 3. El tercero que adquiera a título oneroso valores negociables representados por medio de anotaciones en cuenta o por medio de sistemas basados en tecnología de registros distribuidos, de persona que, según los asientos del registro contable o el sistema basado en tecnología de registros distribuidos, aparezca legitimada para transmitirlos, no estará sujeto a reivindicación, a no ser que en el momento de la adquisición haya obrado de mala fe o con culpa grave".

las obligaciones mediante TRD. La modificación del art. 23 d) LSC en relación con el contenido de los estatutos sociales ["Si la sociedad fuera anónima expresará las clases de acciones (...) y si las acciones están representadas por medio de títulos, o por medio de anotaciones en cuenta o mediante sistemas basados en tecnología de registros distribuidos"], debe interpretarse conjuntamente con el artículo 6.2 de la LMV, que permite la representación de los valores negociables mediante sistemas basados en TRD "en el marco del Reglamento UE 2022/858 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022". Insistimos en que ello no implica que no puedan ser toquenizados los derechos que incorporan las acciones y las obligaciones para poder circular a través de TRD[55]; pero no gozarán de la protección del régimen previsto para las anotaciones en cuenta en la LMV al que se remite el artículo 118 LSC. A diferencia de lo que sucede con los valores anotados, no se ha incluido expresamente la remisión con carácter general en la LSC a la normativa reguladora del mercado de valores en los casos de representación de las acciones mediante TRD.

El régimen de las criptoacciones y cripto-obligaciones, más allá de la mención en los estatutos sociales o en la escritura de emisión [art. 417.2 c)], no está previsto en la LSC. Que el artículo 5 LMV permita al emisor someterse a esta ley si en el documento de emisión así se ha establecido expresamente o, en su defecto, si el emisor tiene su domicilio social en territorio español o ha designado a una única entidad con domicilio social en España como responsable de la administración de la inscripción y registro de los valores en el sistema, no permite concluir el reconocimiento legal de criptoacciones y cripto-obligaciones emitidas por sociedades españolas con carácter general, sino que ha de entenderse referido a la admisión y negociación de esos valores en el marco del reglamento sobre un

---

[55] Parece que a estas dos posibilidades se refiere el reglamento sobre un régimen piloto cuando en su considerando 3 se refiere a "la representación digital de instrumentos financieros mediante sistemas basados en tecnología de registro descentralizado o la emisión de activos de tipo tradicional en forma de autenticación por tóquenes para que puedan ser emitidos, almacenados y transferidos empleando un registro descentralizado". Indica Herrero Morant que para las acciones de las sociedades cotizadas "este proceso de *tokenización* sería un paso previo obligatorio ya que al menos hasta el momento la normativa obliga a su representación por medio de anotaciones en cuenta (art. 496 LSC) y no habría acciones creadas dentro de la propia red". Por esta razón, los toquens solo podrán representar los derechos vinculados a la tenencia de las acciones y no la acción misma. Herrero Morant, R. (2020). "La tecnología DLT en el mercado de valores, en especial respecto de las acciones de las sociedades cotizadas. Aspectos generales y análisis de una posible desintermediación del mercado", *RDMV*, 26, p. 4 de la versión digital.

régimen piloto. El art. 496 LSC –inalterado por la LMV– obliga a representar las acciones en anotaciones en cuenta "que pretendan acceder o permanecer admitidas a cotización en un mercado regulado que esté domiciliado o que opere en España", previsión extendida a las acciones negociadas en un sistema multilateral de negociación por la disposición adicional decimotercera de la LSC.

Pero si hablamos de la toquenización de los derechos del socio, permaneciendo la acción instrumentada o representada en papel o en una anotación en cuenta, ahí la autonomía privada juega con mayor libertad. Tampoco estamos ante nada nuevo: la práctica creó los certificados de depósito de las acciones y de las obligaciones, certificados que se negocian, por ejemplo, en mercados estadounidenses bajo la denominación de *american depository receipts* o ADR para valores extranjeros[56]. Nuestro legislador los reconoce asimismo como valores mobiliarios, pero sólo los emitidos por emisores no residentes; se refiere a ellos como "recibos de depositario representativos de las acciones y de las obligaciones" [art. 2.1. a) LMV], y los somete, al considerarlos valores negociables y por tanto, instrumentos financieros, a la LMV[57]. En el Derecho estadounidense, estos ADR circulan al margen de la acción, que queda depositada en una entidad financiera y es este depositario quien figura como titular nominal de las acciones. Su ley de circulación será la que establezca el organismo rector del mercado en el que se negocian.

De la misma forma, es posible toquenizar los derechos económicos derivados de la acción y no la parte alícuota del capital social en sí misma considerada; pero si esa toquenización implica la creación de un mercado secundario en el que se negocien esos toquens y se considera que esos derechos representados por un toquen son valores negociables –dada la amplitud de la definición recogida en el artículo 2

---

[56] Algunas sociedades españolas han dado el salto al Nasdaq a través de esta figura, valga el caso casi experimental de Turbo Energy.

[57] Es en el art. 3.1. a) del Real Decreto 814/2023 sobre instrumentos financieros en donde se definen estos valores: "A efectos de lo dispuesto en este real decreto se entenderá por recibos de depositario los valores negociables en el mercado de capitales, que representan la propiedad de los valores de un emisor no residente, y pueden ser admitidos a negociación en un centro de negociación y negociados con independencia de los valores del emisor no residente". Llama la atención que en régimen del reglamento sobre un régimen piloto sí estén contemplados los *depository receipts* para las obligaciones, pero no para las acciones, quizá por las dudas que ha albergado siempre el supervisor europeo acerca de la consideración como instrumentos financieros no complejos de los segundos (v. CESR, *MiFID complex and non-complex financial instruments for the purposes of the Directive's appropriateness requirements*, 3 de noviembre de 2009).

de la LMV–, podría entrar en juego el derecho administrativo sancionador del mercado de valores, desde el momento en el que se está creando un mercado de instrumentos financieros sin la pertinente autorización administrativa. El concepto de criptovalor negociable a efectos de la aplicación de la normativa del mercado de valores –y de la exclusión de la aplicación del régimen del MiCA– es una de las cuestiones más difíciles en el derecho de los mercados financieros –europeo y español–. Al respecto, se espera que la Autoridad Europea de los Mercados de Valores (ESMA) aclare qué se entiende por valor negociable, al menos para su deslinde respecto a los toquens referenciados a activos (*asset referenced tokens*) e incluso para los conocidos como toques de servicio (*utility tokens)*. Sin perjuicio de que determinados capítulos del MiCA estén directamente inspirados en la normativa europea de los mercados de valores (la MiFID II, el Reglamento de folletos o el de abuso de mercado por citar las principales normas), estamos ante un régimen más laxo en el MiCA si atendemos a la tutela del inversor.

3.3. Los toquens como nueva forma de representación de los derechos-valor emitidos por la sociedad

La pregunta que ahora procede es, si en el caso de que se toquenicen las acciones y las obligaciones al amparo del reglamento sobre un régimen piloto estamos ante un *tertium genus* en la categoría de los derechos-valor. La respuesta, para las que sí es posible hacerlo, es, en nuestra opinión, afirmativa. Porque se predican de ellas las notas caracterizadoras de los títulos valores –y podemos realizar las mismas críticas a la concepción clásica de estos derechos incorporados en un documento–[58]. A la clasificación tradicional de los valores mobiliarios en función del medio elegido para su representación (títulos o anotaciones en cuenta) se añade ahora una tercera forma de representación: la que tiene lugar a través de la TRD (art. 6 LMV).

Así, en lo que respecta a su constitución, de la misma manera que los valores anotados se constituyen como tales en virtud de su inscripción en el correspondiente registro de la entidad encargada del registro contable, los criptovalores negociables se constituirán como tales en el momento de su registro en el

[58] Como indicara Jesús Rubio, en un planteamiento general, a propósito de la configuración y el desarrollo de los títulos-valores, se ha llegado a "exageraciones constructivistas" (Rubio, J., *Derecho cambiario*, cit. p. 10).

sistema en favor del emisor o directamente en favor de los suscriptores (art. 10 LMV). Igualmente, la constitución de derechos reales limitados y otros gravámenes deberá registrarse en el registro correspondiente a cargo de la entidad de crédito o de la sociedad de valores, entendiéndose que la "constitución del gravamen será oponible a terceros desde el momento en que se haya practicado la correspondiente inscripción" (art. 12.2 LMV). La nota de la autonomía prevista para las anotaciones en cuenta se traslada como hemos indicado en el art. 11. 3 LMV a los criptovalores. Respecto a la legitimación, *mutatis mutandis* con los valores anotados (el art. 13. 1), la persona que aparezca legitimada en el sistema basado en tecnología de registros distribuidos se presumirá titular legítimo y, en consecuencia, podrá exigir de la entidad emisora que realice en su favor las prestaciones a que dé derecho el valor negociable[59].

La legitimación activa no necesariamente va a instrumentarse a través de los certificados de legitimación (el art. 14 LMV, utiliza la expresión "podrá instrumentarse"). Será el propio sistema el que establezca cómo acreditar la titularidad de los derechos. Sin embargo, a la vista del modelo escogido por el legislador español, son las entidades responsables de la administración de la inscripción y registro de los valores en el sistema y de la gestión de la identificación de los titulares –incluido el emisor–, quienes asumen la función de emitir los justificantes o certificados en materia de legitimación del socio o bonista. Por lo que respecta a la legitimación pasiva, se mantiene el principio previsto para las anotaciones en cuenta de liberación de la entidad emisora que realice de buena fe y sin culpa grave la prestación en favor del legitimado según el registro, aunque este no sea el titular del valor negociable (art. 13.2 LMV). También a imagen de los valores representados mediante anotaciones en cuenta en cuenta se recoge el principio de tracto sucesivo en el artículo 13.3 de la LMV, aunque la TRD está basada precisamente en el tracto

[59] Las normas que permiten la corporeización del derecho en un papel o la incorporación del derecho en el documento, en la teoría clásica de los títulos-valores, la digitalización del derecho en una anotación en cuenta o la toquenización del derecho para posibilitar su circulación a través de la TRD, hacen posible la mobilización de los derechos y su circulación a través de la entrega (art. 120.2 LSC), la transferencia contable de los valores anotados (art. 11 LMV), o el registro en una red de TRD (art. 11 LMV) por medio de la ejecución del *smart contract* vinculado al toquen.

sucesivo (en el sistema *bitcoin*, la validación de la transacción en el bloque sobre el que se creará un nuevo bloque de la cadena)[60].

3.4. La financiación a través de préstamos toquenizados

El recurso a la TRD para la sociedad como nueva técnica de instrumentación de sus necesidades de financiación no se limita a la emisión de criptoacciones, cripto-obligaciones u otros instrumentos financieros representados mediante TRD. Ha de contarse también con la posibilidad de concesión de préstamos (*crypto-lending*)[61], materia en la actualidad carente de regulación en el Reglamento MiCA[62]. Pero sí contamos en España con un régimen de control por la CNMV de la publicidad sobre criptoactivos con objeto de inversión (sean o no criptovalores mobiliarios).

Como es sabido, el préstamo entre particulares no es una actividad regulada; aquí lo prestado no es dinero sino criptomonedas, que no tienen la naturaleza de moneda de curso legal. La sociedad de capitales puede solicitar préstamos a través de plataformas TRD. Se trata de una actividad que no puede subsumirse en la normativa reguladora de las plataformas de financiación participativa puesto que en el modelo legal de *crowdfunding* y *crowdlending* la plataforma realiza labores de intermediación entre el prestamista y el titular del proyecto, actividad que no casa con la naturaleza desintermediada de la concesión de préstamos

---

[60] En algunos sistemas de TRD, no necesariamente el envío de la orden de transacción al sistema implica la prioridad temporal en la validación de esa transacción; por ejemplo, en el ámbito de las finanzas descentralizadas (DeFI), si el usuario no protege su orden con determinados programas informáticos, la transacción se envía a una *memory pool* pública antes de ser incluida en la cadena de bloques, lo que propicia actuaciones ilícitas de terceros (abuso de mercado) en este espacio virtual para alterar el orden en el que se incluyen las transacciones en la cadena de bloques para su validación (v. Alonso, Ch., "Cómo evitar los bots de Blockchain que se llevan tus beneficios: protección MEV", https://www.elladodelmal.com/2024/02/como-evitar-los-bots-de-blockchain-que.html, 15 de febrero de 2024.

[61] A la posibilidad de toquenizar préstamos participativos para la adquisición de inmuebles se refieren, entre otros autores, Villanueva Redondo, J. y Vecino Bécares, V. (2023), "Tokenización: Una nueva forma de inversión en activos inmobiliarios", en AA. VV., *Nuevas tecnologías*, Ortega Burgos, E. (dir.), Tirant lo Blanch, Valencia, pp. 567-590, pp. 583-584.

[62] Ello sin perjuicio de que el art. 142 del MiCA prevea, en el informe que la Comisión Europea ha de presentar al Parlamento y al Consejo a más tardar el 30 de diciembre de 2024 sobre los últimos desarrollos en materia de criptoactivos, la evaluación por la Comisión de la necesidad y viabilidad de regular la concesión de préstamos de criptoactivos y las finanzas descentralizadas en los mercados de criptoactivos.

entre particulares al margen de la financiación bancaria a través de sistemas de registro distribuido[63]. Sólo dejamos planteada aquí esta cuestión, merecedora de un estudio detallado que no podemos abordar en el presente trabajo.

4. CONCLUSIONES

Las tecnologías de registro distribuido han irrumpido en los mercados financieros desde la creación del *bitcoin* en 2008. La principal ventaja que aportaron en origen, la desintermediación en la operativa financiera, se ha visto perjudicada por los evidentes riesgos que presentan para los mercados de capitales: el blanqueo y la financiación del terrorismo, las estafas en red y los constantes ataques informáticos a estos sistemas basados en TRD. De ahí que las primeras regulaciones en la Unión Europea se centraran en la lucha contra el blanqueo a través de criptoactivos y al establecimiento del régimen de acceso y funcionamiento de los mercados de criptoactivos financieros, con especial atención a la regulación de los proveedores de determinados servicios sobre estos activos digitales; el principio de equivalencia funcional llevó a realizar unas mínimas modificaciones en la legislación de los mercados de valores (MiFID II), puesto que los toquens representativos de las acciones y las obligaciones tienen la consideración de valores negociables. Cuando ello no ha sido posible por la peculiaridad en el funcionamiento de los mercados basados en registros distribuidos, se ha aprobado normativa específica como el reglamento sobre un régimen piloto de infraestructuras de mercado basadas en la TRD.

La constante evolución de estas tecnologías permite adaptarlas a las necesidades de los empresarios en el desarrollo de su actividad. Pueden contribuir a la ágil llevanza de los registros societarios al menos en las grandes sociedades anónimas y a la identificación del socio –beneficiario último– de la cotizada. Ello precisa, bien la toquenización de algunos derechos del socio o de la acción, bien la emisión de acciones y obligaciones directamente representadas mediante sistemas basados en la TRD. En el caso de las sociedades cerradas, la implicación de los registradores mercantiles parece esencial para la llevanza del registro de socios mediante toquens.

---

[63] A propósito, no sólo del *crowdlending* sino también del *crowdfunding* en relación con las *initial token offerings*, en este sentido ya Álvarez Royo-Villanova, S. (2018), "Las ICOs como nueva forma de crowdfunding", *El notario del siglo XXI*, 81, disponible en https://www.elnotario.es/hemeroteca/revista-81/8908-las-icos-como-nueva-forma-de-crowdfunding

El legislador español del mercado de valores ha reconocido esta tercera forma de representación de los valores negociables y la posibilidad de crear mercados en los que se negocien estos cripto-instrumentos financieros. Sin embargo, estamos aún lejos de la generalización de los toquens-valores mobiliarios en el derecho societario y financiero. Será necesario esperar al desarrollo de los sistemas multilaterales de negociación en el marco del reglamento sobre un régimen piloto; por otra parte, el fracasado sistema de compensación y liquidación con tecnología de registro distribuido en la bolsa australiana[64], hace que debamos ser cautos a la hora de generar expectativas sobre el éxito de esta clase de mercados valores.

BIBLIOGRAFÍA

Alonso Ureba, A. (2023). "Derecho de sociedades y función económico social de la gran empresa ("interés social" vs "interés de empresa": Una cuestión abierta)", AA. VV., *Derecho de sociedades y sostenibilidad,* C. Chamorro y J. A. Viera (coords.), La Ley, Madrid, pp. 27-92.

Álvarez Royo-Villanova, S. (2018). "Las ICOs como nueva forma de crowdfunding", *El notario del siglo XXI*, 81, disponible en https://www.elnotario.es/hemeroteca/revista-81/8908-las-icos-como-nueva-forma-de-crowdfunding

Ascarell, I. T. (1940). Voz "Titoli di crédito", *Nuovo Digesto Italiano,* vol. XII, Turín.

Bech, M. y Garrat, R. (2017). "Central Bank Cryptocurrencies", *BIS Quaterly Review*, septiembre, pp. 55-70.

Bednarz, Z. (2020). "El uso de la tecnología Blockchain para el ejercicio del derecho de voto por los socios", *Derecho de sociedades: los derechos del socio*B. González Fernández y A. Cohen Benchetrit (dirs.), Tirant lo blanch, Valencia, pp. 523-544.

Bednarz, Z. (2020). "El uso de la tecnología *blockchain* en las sociedades cotizadas: la implicación de los accionistas", *Revista de Derecho de Sociedades,* 58, versión digital.

[64] V. el comunicado de los supervisores financieros australianos de 17 de noviembre de 2022, *ASIC-RBA joint statement on ASX CHESS replacement program*, disponible en https://download.asic.gov.au/media/sypbow5u/22-320mr-asic-rba-letter-to-asx-board.pdf

Daniels, A. (2018). "Blockchain & shareholder voting: a hard fork for 21st-century corporate governance", *University of Pennsylvania Journal of Business Law*, 405, pp. 405-441.

Díaz Moreno, A. (2000). "Consejos de administración virtuales y adopción de acuerdos por escrito y sin sesión durante el estado de alarma", *Análisis GA-P*, 17 de marzo.

Gallego Corcoles, A. (2019). "El *blockchain* en la junta general", en AA. VV.: *Revolución digital, Derecho mercantil y token* economía, A. Muñoz Pérez (dir.), Tecnos, Madrid, pp. 306-339.

Gallego Lanau, M. (2021). "El funcionamiento virtual de la junta general de las sociedades de capital y *blockchain*", AA. VV. *El sistema jurídico ante la digitalización. Estudios de Derecho privado,* M. Paniagua Zurera (dir.), Tirant lo Blanch, Valencia, pp. 441-462.

Gállego Lanau, M. (2022). *La junta exclusivamente telemática en las sociedades de capital cerradas,* Aranzadi.

García Mandalóniz, M. (2020). *Una sociedad mercantil simplificada y digitalizada. Un ecosistema emprendedor innovador, inclusivo y sostenible*, Dykinson.

Garrido, J. (2023). "Digital Tokens: A Legal Perspective", *IMF wp/23/151*, julio.

Gónzalez Vázquez, J. C., entrada "Píldoras mercantiles: aprobación de la Ley 6/2023, de 17 de marzo, de los mercados de valores y de los servicios de inversión: aspectos relevantes (III)", 3 de marzo de 2023, disponible en https://www.linkedin.com/pulse/pildoras-mercantiles-aprobaci%25C3%25B3n-de-la-ley-62023-17-y-jos%25C3%25A9-carlos-1e/?trackingId=Gt8JTPdiQwqkdgL8c3M2Ag%3D%3D

Hernández Sáinz, E. (2020). "La asistencia virtual al consejo en las sociedades cotizadas", *Revista de Derecho del Mercado de Valores*, 27, versión digital.

Herrero Morant, R. (2019). *Los inversores institucionales en las sociedades cotizadas españolas: caracterización y activismo accionarial*, Marcial Pons, Madrid.

Herrero Morant, R. (2020). "La tecnología DLT en el mercado de valores, en especial respecto de las acciones de las sociedades cotizadas. Aspectos

generales y análisis de una posible desintermediación del mercado", *Revista de Derecho del Mercado de Valores*, 26, versión digital.

Ibáñez Jiménez, J. W. (2021). "Financiación digital distribuida", AA. VV., *Digitalización de sociedades,* C. Alonso Ledesma y A.F. Muñoz Pérez (coords.), *Cuadernos de Derecho para Ingenieros*, 54, pp. 22-48.

Ibáñez Jiménez, J. W. (2018). *Blockchain, primeras cuestiones en el ordenamiento español,* Dykinson, Madrid.

Ibáñez Jiménez, J. W. e Ibáñez Jiménez, E. M. (2023). "NFT Legal and Market Challenges in Permissioned Blockchain Networks" AA. VV., *Blockchain Applications: Transforming Industries, Enhancing Security, and Addressing Ethical Consideration,s* V. Chernyshenko y V. Mkrttchian (dirs.), DOI: 10.5772/intechopen.106460.

Jiménez Gómez, B. S. (2022). "El derecho de voto en las sociedades cotizadas a través de la tecnología *blockchain*", *Revista de Derecho Bancario y Bursátil,* 168, pp. 141-170.

Lafarre, A. y Van der ELTS, C. (2021). "Shareholder Voice in Complex Intermediated Proxy Systems: Blockchain Technology as a Solution?", *The Stanford Journal of Blockchain Law and Policy*, 4, versión digital.

Lafarre, A. y Van der ELST, C. (2023). "The Viability of Blockchain in Corporate Governance", *ECGI Law Working Paper* 712/2023, junio, disponible en https://ssrn.com/abstract=4483621

León Sanz, F. (2022). "Comentario al artículo 179", AA. VV. *La junta general de las sociedades de capital: Comentario de los artículos 159 a 208 LSC,* J. Juste y A. Recalde (coords.), Cívitas, Madrid, cit. pp. 357-380.

Muñoz García, A. (2024). "La tokenización de instrumentos financieros en la Ley de los Mercados de Valores y de los Servicios de Inversión", *Revista de Derecho Bancario y Bursátil,* 170, pp. 117-134.

Muñoz Pérez, A. F. (2024). "Tokenizaciones. Caracterización de las Criptomonedas, los Criptoactivos y los Instrumentos financieros", *Revista de Derecho Bancario y Bursátil,* 170, pp. 119-210.

Noval Pato, J. (2022). "Sociedades mercantiles y digitalización de la actuación de los órganos", AA. VV. *Blockchain: aspectos jurídicos de su* utilización, E. Valpuesta y J. C. Hernández Peña (dirs.), La Ley, Madrid, pp. 205-237.

Palá Laguna, R. (2021). "Digitalización de registros societarios", *Cuadernos de Derecho para Ingenieros*, 54, pp. 88-110.

Palá Laguna, R. y Canalejas Merín, J. C. (2023). "A qué criptoactivos no se aplicará el Reglamento MiCA", *Análisis GA_P*, 20 de junio.

Panisi, F., Buckley, R. y Arner, D. (2019). "Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance?", 2 *Stanford Journal of Blockchain Law and Policy*.

Peinado, J. I. y Bednardz, Z. (2021). "Cuestionando las bondades de la "blockchain" en las juntas generales", *Revista de Derecho de Sociedades,* 61, versión digital.

Perdices Huetos, A. (2016). "Estructura del accionariado e intervención de intermediarios financieros: ejercicio del voto y otorgamiento de delegaciones de voto por parte de entidades intermediarias titulares de los registros contables", AA. VV., *Junta general y consejo de administración en la sociedad cotizada,* F. Rodríguez Artigas et al. (dir.), Tomo I, Aranzadi, pp. 803-814.

Portellano Díez (2021). "Repercusión de la tecnología *blockchain* sobre el órgano de administración", *Cuadernos de Derecho para Ingenieros* 54, pp. 131-148.

Recalde Castells, A. (2022). "Comentario al artículo 189", AA. VV., *La junta general de las sociedades de capital: Comentario de los artículos 159 a 208 LSC,* cit. Madrid, pp. 501-513.

Ripert, G. (1950). *Aspectos jurídicos del capitalismo moderno*, Bosch y cía. eds., Buenos Aires.

Romero Ugarte, J. L. (2018). "Tecnología de registros distribuidos (DLT): una introducción", *Boletín Económico del Banco de España,* octubre.

Rubio García-Mina, J. (1973). *Derecho cambiario,* Madrid.

Sanjuan y Muñoz, E. (2021). "Aplicación de la tecnología *blockchain* al funcionamiento de las sociedades de capital y los medios judiciales de control", *Estudios sobre Derecho digital*, R. Perea Ortega (coord.), Aranzadi, pp. 757-616.

Sanz Bayón, P. (2021). "Emisión y regulación del dinero público digital: análisis de las monedas digitales de Banco Central", *Revista de Derecho del Mercado de Valores*, 29, versión digital.

Trías Sagnier, M. (1998). *Los Inversores Institucionales y el Gobierno de las Grandes Sociedades*, McGraw Hill, Madrid.

Takahashi, K. (2021). "Blockchain-based Negotiable Instruments (with Particular Reference to Bills of Lading and Investment Securities)", octubre, disponible en https://ssrn.com/abstract=3937664

Villanueva Redondo, J. y Vecino Bécares, V. (2023). "Tokenización: una nueva forma de inversión en activos inmobiliarios", AA.VV., *Nuevas tecnologías,* E. Ortega Burgos (dir.), Tirant lo Blanch, Valencia, pp. 567-590.

Quinta Parte
ESTUDIOS SOBRE EL METAVERSO

Capítulo 13
METAVERSO, BLOCKCHAIN Y EL REGISTRO DE LA PROPIEDAD

Rocío Perteguer Prieto
Directora de Medio Ambiente, Consumidores y Usuarios
Colegio de Registradores de España

1. INTRODUCCIÓN

La sociedad actual se encuentra inmersa en la cuarta revolución industrial, caracterizada por una convergencia de tecnologías que están transformando el mundo tal y como lo conocemos, la forma de relacionarnos, de trabajar y de hacer negocios.

El impacto de la innovación tecnológica en los registros ha sido creciente e intensa en los últimos años. En concreto, tras la Ley 11/2023, de 8 de mayo (publicada en el BOE de 9 de mayo), se ha traspuesto en nuestro ordenamiento, entre otras, la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del derecho de sociedades, introduciendo cambios significativos en la Ley del Notariado, Código de Comercio, Ley Hipotecaria y Ley 24/2001, de 27 de diciembre, de Medidas fiscales, administrativas y del orden social, para posibilitar la realización de determinadas actuaciones notariales y registrales de manera telemática, sin que sea necesaria la presencia física de los otorgantes o interesados.

Esta novedosa regulación conlleva un nuevo paradigma de relación de la sociedad con el Registro de la Propiedad, Mercantil y de Bienes Muebles llegando a establecer en su articulado el derecho de los ciudadanos a "*relacionarse directamente con el Registro de la Propiedad y con el Registro Mercantil y de Bienes Muebles por medios electrónicos y así podrán presentar documentos, obtener informaciones y certificaciones, realizar consultas, formular solicitudes, manifestar*

consentimientos, efectuar pagos, y recurrir los actos registrales de acuerdo con lo dispuesto en esta ley"[1].

En nuestras relaciones con la sociedad, se amplían los canales telemáticos del Registro haciendo ahora un Registro más abierto a la sociedad y a la digitalización de los procesos, a la identidad digital y al fomento de las relaciones electrónicas, agilizando procesos y reduciendo trámites, tanto de entrada y acceso de documentación de todo tipo, como de salida de información: de publicidad, pero conservando las características esenciales de una publicidad fiable, transparente, que garantiza la inexistencia de asimetrías en la información.

Finalmente, el impacto de la tecnología en nuestra sociedad está haciendo surgir nuevas realidades, para las que, como cualificados profesionales jurídicos, los Registradores de la Propiedad, Mercantiles y de Bienes Muebles demuestran estar preparados, con una hoja de ruta exacta, para crear nuevos servicios y ofrecer nuevas soluciones y estructuras jurídicas.

En un mundo conectado, en el que desaparecen los límites entre lo físico y digital, la Institución Registral se encuentra en una posición única para actuar de nexo de unión, conectando ambas realidades. Vínculo que será esencial si las transacciones que se realicen en el mundo virtual pretenden celebrarse con plenos efectos jurídicos y con repercusión en el mundo físico.

Tecnologías como blockchain, una nueva forma digital de reflejar transacciones, la tokenización de activos, o los NFT-tokens no fungibles, podrán encontrar acomodo en el Registro –de la propiedad, mercantil o bienes muebles, según la naturaleza del derecho que representen–, para beneficiarse de las presunciones jurídicas que proporciona la inscripción en nuestros registros de derechos. Igualmente, la posible personalidad jurídica de los robots, a través de su inscripción registral, o fórmulas para identificar la responsabilidad por los daños causados.

Las actuaciones telemáticas, sin presencia física, requerirán garantizar la identificación de los intervinientes. Tratándose de personas jurídicas y sus

---

[1] DA Primera 2.a. introducida por Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos.

representantes, el Registro Mercantil juega un papel clave en proporcionar, con total garantía y seguridad, el enlace entre su identidad digital y real.

Así el Registro de la Propiedad, Mercantil y de Bienes Muebles se revela como una estructura esencial para hacer una arquitectura jurídica en la transmisión onchain igual a la offchain. Las plataformas de tokenización son una nueva forma de acreditar una transmisión digital y privada. "*Las plataformas blockchain inmobiliarias no sustituirán al registro de la propiedad. Lo podemos decir tras varios años de investigación. Las plataformas de tokenización tienen un importante ámbito de acción como un marketplace privado para hacer una venta entre ausentes. La vinculación puede hacerse a través del Registro de la Propiedad. Es voluntario y se puede hacer hoy. El propietario decidirá si lo transmite de forma offchain u onchain*"[2].

2. METAVERSO

2.1. Concepto y descripción

El metaverso es un mundo virtual al que nos conectamos utilizando una serie de dispositivos que nos hacen sentir como si estuviéramos dentro de él, interactuando con todos sus elementos. La situación transporta al usuario de la experiencia a un mundo completamente nuevo a través de gafas de realidad virtual y otros complementos que le permiten interactuar con este entorno.

A diferencia de los mundos de fantasía en los videojuegos, el metaverso no busca ser un lugar irreal. Más bien, es una realidad alternativa en la que podemos realizar las mismas actividades que hacemos fuera de casa, pero sin movernos de la habitación. El término "metaverso" proviene de la novela de 1992 llamada "Snow Crash" y se ha asentado para describir visiones de espacios de trabajo tridimensionales o virtuales. En esencia, el metaverso es un mundo virtual en el que podemos interactuar y que se asemeja a una realidad externa.

La clave del metaverso es su inmersión total, la cual se practica a través de un avatar. En informática, un avatar es la representación gráfica que se asocia a un usuario en el mundo virtual. Puede ser una fotografía, un dibujo o incluso una representación tridimensional. Los avatares no solo se utilizan en el metaverso,

---

[2] Sieira Gil, J. (2021). *III Jornada Blockchain Economía realizada con el Campus de la Universidad de Navarra*, Madrid, 25 de octubre.

también en redes sociales, programas informáticos, foros de discusión, mensajería instantánea y otras plataformas de interacción en línea.

En el metaverso, un avatar es una representación digital de uno mismo que puede ser personalizada a gusto del usuario. Se puede elegir su apariencia, ropa, cabello, altura, forma y mucho más. En esencia, el avatar es el alter ego virtual dentro de los mundos digitales.

Aunque se utilizan gafas especiales de realidad virtual para sumergirnos en él, también habrá sensores que registren nuestros movimientos físicos para que nuestro avatar dentro del metaverso se comporte de manera realista. Incluso podríamos expresar emociones a través de nuestros dispositivos para que otros usuarios puedan entender cómo nos sentimos.

En resumen, el metaverso es una visión futurista de una internet inmersiva y virtual, donde las personas pueden conectarse, crear, socializar e incluso experimentar mundos virtuales. Es un concepto emocionante que está siendo explorado por empresas como Facebook (ahora Meta), Google, Nvidia y Microsoft. Aunque aún falta tiempo para que se convierta en una realidad cotidiana, el metaverso promete abrir nuevas posibilidades y experiencias.

2.2. Elementos necesarios para su creación y ejemplos

La construcción de un metaverso es un proceso complejo que involucra múltiples aspectos tecnológicos, creativos y sociales. A continuación, podemos señalar algunos pasos clave en la creación de un metaverso:

Se requiere una fuerte Infraestructura Tecnológica material para poder soportar toda la maquetación, actividad y transacciones del mundo virtual, dependiendo también de la complejidad de este.

Se necesita una infraestructura robusta para alojar y conectar a los usuarios en el metaverso. Esto incluye servidores, redes de alta velocidad y sistemas de almacenamiento.

Hardware: los dispositivos de acceso al metaverso, como gafas de realidad virtual (VR), auriculares y sensores de movimiento, son esenciales para la inmersión de los usuarios.

Para la *creación de contenido* se necesita una gran capacidad de talento innovador y creativo tanto en diseño gráfico e informático como en los entornos en los que se desarrollará el metaverso en cuestión.

Mundos Virtuales: los desarrolladores crean entornos virtuales dentro del metaverso. Estos pueden ser réplicas de lugares reales o completamente imaginarios. Además se utiliza modelado 3D, se diseñan objetos, edificios, paisajes y avatares en formato 3D. Los cuales serán enriquecidos con texturas y animaciones: Se agregan detalles visuales y movimientos realistas a los elementos del metaverso. Así la comunidad de desarrolladores, artistas y creativos contribuye activamente al metaverso.

En la planificación y generación de la *Interacción y Experiencia del Usuario* será fundamental que esta sea de características sencillas y de aprendizaje sencillo. La Interfaz de Usuario (UI) ha de ser diseñada como una interfaz intuitiva para que los usuarios naveguen por el metaverso. Esta interfaz está pensada para realizar una interacción social: Se implementan funciones para que los usuarios se comuniquen, colaboren y compartan experiencias.

Esta interrelación se completa con la posibilidad de transaccionar a través de una economía virtual que se crea dentro del metaverso, con monedas virtuales y transacciones.

En relación con la *Seguridad y Privacidad*, cobra gran relevancia los datos que aportemos en nuestro mundo virtual respecto del mundo real, de tal modo que la protección de datos y la prevención de abusos han de ser básicas para garantizar a los usuarios una experiencia confiable y cómoda de uso. Se deben establecer medidas de seguridad para proteger la privacidad de los usuarios y sus datos personales e implementar sistemas para evitar el acoso, el fraude y otros comportamientos perjudiciales.

Otro elemento clave para el éxito de un mundo en el metaverso es la necesidad de implementar estándares abiertos acordados por la comunidad para la interoperabilidad entre diferentes mundos virtuales y plataformas. De igual modo se deben de definir protocolos de comunicación lo más homogéneos para que los servidores y dispositivos se comuniquen eficientemente.

Y por fin el elemento final, determinante y más necesario en el éxito del nacimiento de un metaverso son los usuarios, ya que la participación activa de los usuarios es fundamental para el éxito del metaverso.

En resumen, la construcción de un metaverso es un esfuerzo colaborativo que combina tecnología, creatividad y comunidad. A medida que avanza la tecnología y más personas se suman a esta visión, el metaverso continuará evolucionando y expandiéndose.

El metaverso es un concepto emocionante que está ganando terreno rápidamente. Aunque aún no es una realidad cotidiana y ciertamente parece que el ímpetu con el que comenzó el metaverso ha sufrido una cierta no ya ralentización sino especificación en su uso, ya sea para juegos, visitas turísticas, recreaciones de museos, de entornos de pruebas para prototipos de vehículos, de visitas de inmuebles variando sus entornos y posibilidades, conciertos o eventos en directo en un metaverso... ya existen varios ejemplos de metaversos en producción definitiva. Mostraremos aquí algunos:

- *Horizon Worlds* (de Meta): anteriormente conocido como Facebook Horizon, este metaverso ha sido desarrollado por Meta (anteriormente Facebook). Ofrece un espacio virtual donde los usuarios pueden interactuar, crear contenido y socializar. Su acceso es gratuito, si bien ofrece compras y transacciones. Veremos que esta configuración con relación a los costes es la más común a todas las plataformas con los efectos en ocasiones perniciosos que ello conlleva en relación con la adicción al juego online o a los videojuegos, así como los riesgos de los juegos de azar y las apuestas deportivas[3].
- *Fortnite*: aunque es ampliamente conocido como un popular videojuego de batalla real, Fortnite también se considera un metaverso. Para acceder hay que descargar el juego en la plataforma elegida por el usuario (ordenador, consola o dispositivo móvil). Una vez dentro del juego, se puede participar en eventos en vivo y explorar los modos creativos. Los eventos en el juego atraen a millones de jugadores y espectadores, y la colaboración con marcas y artistas es común. Su uso es gratuito para jugar en todas las plataformas, sin embargo, se puede gastar dinero en compras dentro del juego, como skins, bailes y pases de batalla.
- *Roblox*: Roblox es una plataforma de creación de juegos que permite a los usuarios diseñar sus propios mundos virtuales y experiencias. Es especialmente popular entre los jóvenes y ha visto un crecimiento significativo en los últimos años. Para utilizarla hay que visitar el sitio web de Roblox y crear una cuenta, una vez creada se puede descargar el cliente de Roblox en el ordenador o dispositivo móvil y explorar los miles de juegos y mundos

[3] Cuesta Cano, L. (2023). *Crecer con Pantallas. Como enseñar a tus hijos a usar y disfrutar de la tecnología de forma segura y saludable*, Amat, Madrid, capítulo 7.

creados por la comunidad. Roblox es gratuito para descargar y jugar. Los usuarios pueden comprar Robux (la moneda virtual de Roblox) para personalizar sus avatares o comprar artículos en el juego.

- *Cryptovoxels*: este metaverso descentralizado utiliza tecnología blockchain y tokens no fungibles (NFT) para crear un mundo virtual donde los usuarios pueden comprar, vender y construir propiedades virtuales. Para participar hay que visitar su sitio web y obliga a crear una cuenta. Cryptovoxels permite la entrada gratuita al mundo virtual. Sin embargo, si se desea comprar parcelas de tierra virtual, hay que adquirir MANA (su criptomoneda nativa).
- *The Sandbox*: similar a Roblox, The Sandbox permite a los usuarios crear y compartir sus propios juegos y mundos virtuales. También utiliza NFT para representar activos digitales. Para acceder hay que registrarse en The Sandbox y descargar su cliente, una vez realizada esta alta se pueden crear juegos y mundos virtuales utilizando su plataforma de creación. The Sandbox también ofrece acceso gratuito. Los usuarios pueden crear y explorar mundos virtuales sin coste aparente, sin embargo, hay opciones premium para aquellos que deseen más funcionalidades
- *Decentraland*: otra plataforma descentralizada basada en blockchain, Decentraland permite a los usuarios comprar parcelas de tierra virtual y construir en ellas. Es un ejemplo de cómo la propiedad virtual puede ser transmitida. Requiere también crear una cuenta en el sitio web. Decentraland permite la entrada gratuita a su mundo virtual. Al igual que Cryptovoxels, se puede comprar parcelas de tierra virtual utilizando MANA.

Estos ejemplos muestran la diversidad de enfoques en la creación de metaversos, desde los desarrollados por grandes empresas hasta los impulsados por la comunidad y la tecnología descentralizada. En resumen, muchos metaversos ofrecen acceso básico sin coste aparente, pero algunos elementos dentro de ellos pueden requerir compras o transacciones, por lo que resulta más que recomendable investigar previamente a su uso cada plataforma específica para comprender mejor sus modelos de negocio y opciones de acceso.

Una pregunta necesaria que tenemos que realizarnos a la hora de acceder a un metaverso es la relativa a las precauciones de seguridad que se deben tener en cuenta al acceder a estos mundos virtuales. Los metaversos son emocionantes y prometedores, pero también presentan riesgos de seguridad. Podemos

así enumerar algunas precauciones que debemos de tener en cuenta al acceder a estos mundos virtuales:

- Robo de identidad y secuestro de cuentas: similar a lo que ocurre en las redes sociales y los juegos multijugador, los metaversos también enfrentan amenazas de robo de identidad y secuestro de cuentas. Es necesario proteger las credenciales y considerar seriamente la autenticación de dos factores.
- Ingeniería social: al igual que en las aplicaciones de citas, en los metaversos los usuarios pueden no ser quienes dicen ser. Se debe de ser cauteloso al interactuar con otros avatares y evitar compartir información personal sensible.
- Problemas de privacidad: los metaversos son como redes sociales en una realidad virtual. Es necesario proteger la información personal, como datos de pasaporte o números de billetes, de manera similar a como lo hacemos en línea.
- Perfilado extensivo y pérdida de autonomía personal: la tecnología en el metaverso puede generar un perfil detallado sobre el usuario el cual debe de considerar cómo esto podría afectar a su privacidad y autonomía personal. Incluyendo los sesgos en las ofertas y repeticiones de conductas detectando vulnerabilidades en su persona.
- Discriminación y fraude: el metaverso puede dar lugar a discriminación en los servicios ofrecidos y posibles esquemas de fraude. Los usuarios deben de permanecer siempre alerta y proteger sus activos virtuales.
- Interoperabilidad y uso indebido de datos: la interoperabilidad entre diferentes metaversos puede exponer los datos a riesgos. Es completamente necesario que el usuario comprenda cómo se comparten sus datos entre plataformas.

La Comisión Europea ha propuesto regulaciones sobre Digital Services Act (DSA) y Digital Market Act (DMA) para abordar los conflictos y vulneraciones de derechos en los metaversos. Están diseñadas para reforzar la capacidad de las plataformas para resolver disputas e imponer determinados requisitos de transparencia en sus términos y condiciones, obligándolas a proporcionar términos y condiciones claros para cada metaverso específico. Estos deben informar sobre restricciones de uso, políticas de moderación de contenidos y cuestiones relacionadas con propiedad intelectual y datos personales. Igualmente, las empresas que operan en el metaverso deben ofrecer políticas de privacidad claras. Los

usuarios deben saber si el "uso gratuito" implica compartir información personal y con qué fines se utilizará esa información.

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea también se aplica al metaverso. Las futuras regulaciones, como la Data Act y la Data Governance Act, también serán relevantes para proteger la privacidad de los usuarios. Si bien como veremos posteriormente pueden resultar insuficientes e ineficaces si no se articulan correctamente con las políticas consumeristas europeas.

3. BLOCKCHAIN

3.1. Concepto de blockchain, activos digitales, NFTs y smart contracts

El blockchain es un libro de contabilidad inmodificable y compartido que facilita el proceso de registro de transacciones y seguimiento de activos en una red empresarial. Así pues, el blockchain es un registro distribuido que almacena información de manera segura y transparente. Cada bloque de datos contiene detalles de transacciones y se encadena de forma segura con otros bloques.

La mecánica de funcionamiento de una red de blockchain se basa en que las transacciones se registran solo una vez en la cadena eliminando la duplicación de esfuerzos, de tal modo que ningún participante de la red blockchain puede cambiar o alterar una transacción una vez registrada y de esta forma los bloques confirman el tiempo y la secuencia exacta de las transacciones.

Cuando tratamos de entender la diferencia principal entre una cadena de bloques pública y una privada debemos de resaltar las siguientes diferencias: la cadena de bloques pública es una cadena sin permiso, cualquiera puede unirse a la red de bloques, lo que significa que puede leer, escribir o participar con un bloque público; además es de estructura descentralizada: nadie tiene control sobre la red. Y los datos no se pueden cambiar una vez validados en el blockchain. Ejemplos de blockchain públicas son Bitcoin, Ethereum y Litecoin.

En cambio, la cadena de Bloques Privada es una cadena de bloques autorizada, de tal manera que las redes autorizadas imponen restricciones sobre quién puede participar en la red y en qué transacciones. Los miembros son conocidos entre sí y las transacciones suelen ser confidenciales entre los participantes involucrados.

En resumen, la principal diferencia radica en el acceso y la privacidad. Las cadenas de bloques públicas son abiertas, mientras que las privadas tienen acceso restringido y pueden tener diferentes niveles de privacidad.

Llegados a este punto conviene destacar pues la diferencia entre blockchain y metaverso que radica básicamente en su naturaleza y función:

- Blockchain es una tecnología descentralizada que permite el registro seguro y transparente de transacciones en una red distribuida cuyas características son las siguientes:
- Es un registro inmutable, ya que las transacciones se registran en bloques y se enlazan en una cadena, lo que garantiza que no se puedan modificar retroactivamente.
- Es un registro descentralizado porque no está controlado por una entidad central, sino por una red de nodos distribuidos.
- Es un registro abierto porque cualquier persona puede verificar las transacciones en la cadena de bloques y utiliza algoritmos criptográficos para proteger la integridad de los datos.

Las aplicaciones principales de blockchain las encontramos en los siguientes ámbitos:

- Criptomonedas, como Bitcoin y otras criptomonedas que utilizan blockchain como base para sus transacciones.
- Contratos inteligentes ya que permite la automatización de acuerdos y transacciones.
- Registro de activos digitales: los NFT (tokens no fungibles) se crean en blockchain.

En cambio, el metaverso como hemos visto es un espacio virtual tridimensional donde las personas pueden interactuar, crear, comerciar y socializar. Sus características son: Desarrollo en un entorno virtual, con interacción social, con economía virtual, en diversidad de aplicaciones. En cuanto a su relación con blockchain podemos distinguir:

- Metaverso sin blockchain: incluye mundos virtuales como Minecraft o Roblox, pero no están basados en blockchain.
- Metaverso con blockchain, que a su vez pueden ser:
  - Centralizados porque están controlados por una entidad central (por ejemplo, Earth).
  - Descentralizados (blockchain abierto) basados en blockchain, como Decentraland, donde los usuarios pueden poseer tierras y activos digitales.

En resumen, blockchain es la tecnología subyacente que permite la confianza del grupo y las transacciones en los metaversos, mientras que el metaverso es el espacio virtual donde ocurren las interacciones y las transacciones digitales.

Los activos digitales son recursos de carácter intangible, ya que se basan en una construcción mediante datos informáticos. Estos datos, según se den, tendrán una serie de características que harán que se diferencien entre sí, tales como el formato en el que se apilen los datos, la forma de visualizarlos o su utilidad, entre otros factores. Algunas de las características propias de los activos digitales son las siguientes:

Están compuestos por datos y, por tanto, son de carácter digital. Únicamente pueden participar en su percepción sensorial como máximo dos sentidos de forma directa: vista y oído. Aunque se trate de un activo intangible o no físico, se almacena de forma física. Por ejemplo, una patente es un activo intangible, pero si está digitalizada, se considera un activo digital.

Tipos de activos digitales:

- Activos con un precio de mercado fijado: poseen un valor establecido al comercializarse.
- Activos sin un precio de mercado fijado: no tienen un valor asignado y pueden o no comercializarse puntualmente.
- Activos con desfase tecnológico: necesitan actualizarse continuamente para no quedar obsoletos.
- Activos sin desfase tecnológico: son piezas únicas que no requieren actualización o solo en una forma ínfima.

Como ejemplos más relevantes de activos digitales podemos destacar:

- Las criptomonedas que son divisas digitales con un rango de precio establecido.
- Los videojuegos son considerados activos digitales con precio fijado y desfase tecnológico limitado.
- Fotografía: archivos digitales que pueden ser un activo si se les puede sacar algún tipo de rendimiento.
- Los NFT (siglas de Non-Fungible Token, que se traduce como Token no fungible) son activos digitales únicos.

Centrándonos en los FNT y para comprenderlos primero debemos entender que existen bienes fungibles y bienes no fungibles en nuestro sistema jurídico.

Los bienes fungibles son aquellos que pueden intercambiarse y tienen un valor basado en su cantidad, medida o peso. Por ejemplo, el dinero es un bien fungible. En contraste, los bienes no fungibles no son sustituibles. Un ejemplo sería una obra de arte: cada cuadro es único y no puede intercambiarse directamente por otro.

Los NFT se basan en esta idea de unicidad. De tal modo que los NFT son tokens no fungibles que representan bienes digitales únicos, como obras de arte, ilustraciones o archivos digitales. Los cuales se crean y se comercializan a través de la tecnología blockchain, la misma que se utiliza para las criptomonedas.

Aunque tecnológicamente opuestos, los NFT y las criptomonedas comparten similitudes. Mientras que un Bitcoin es un bien fungible,un NFT es un bien no fungible.

Así las características principales de los NFT es que son activos únicos que no se pueden modificar ni intercambiar por otro con el mismo valor. Al igual que una obra de arte o un objeto hecho de oro, los NFT tienen un valor especial debido a su unicidad.

En resumen, los NFT son como certificados digitales de autenticidad asociados a archivos digitales únicos.

Los NFTs (tokens no fungibles) y las DAOs (Organizaciones Autónomas Descentralizadas) desempeñan un papel clave en los metaversos basados en blockchain. Por ello pasamos a explicarlos.

Así pues, para crear un NFT (Token no fungible) nos enfrentamos a un proceso que combina tecnología blockchain y creatividad. Los pasos básicos para crear uno serían los siguientes:

1º) Conceptualización del activo digital: implica la toma de decisión sobre qué tipo de activo digital deseamos convertir en un NFT. Puede ser una obra de arte, una ilustración, un video, una música, un juego, o incluso un tweet. En este punto hay que tener seguridad con relación a que el activo tenga valor único y sea auténtico.

2º) Una vez comprobado estos extremos el siguiente paso consiste en elegir una plataforma NFT (hay varias plataformas populares para crear

y vender NFTs, como OpenSea, Rarible, Foundation, SuperRare, entre otras). Después de registrarse en la plataforma hay que crear una billetera de criptomonedas. Dicha billetera digital debe de ser compatible con una cadena de bloques que admita NFTs, el primer paso será el pago de los costes de las tarifas de creación del NFT, para a continuación subir el activo a la plataforma. Estos serían los pasos para subir el activo:

- En la plataforma NFT, buscaremos la opción para subir el archivo. Puede ser una imagen, un vídeo o cualquier otro formato digital.
- Proporcionaremos una descripción detallada del activo, incluyendo su historia y contexto.
- Configuraremos los detalles del NFT: definir si el NFT será subastado o si tendrá un precio fijo. Estableceremos beneficios para el creador (porcentaje que recibiremos cada vez que se revenda el NFT). Mintear el NFT: El proceso de "minting" crea una representación única del activo en la cadena de bloques. Hay que seguir las instrucciones de la plataforma para mintear un NFT. Esto generará un contrato inteligente único para el activo. Se procede al pago de las tarifas de minteo y se confirma la transacción.

3º) Una vez minteado, el NFT estará disponible en la cadena de bloques y el usuario podrá verlo en su billetera. El siguiente paso sería promocionar el NFT, compartiéndolo en redes sociales, comunidades y grupos relacionados con criptomonedas y arte o aforos de interés según el tema del que se trate.

Una Organización Autónoma Descentralizada (DAO, por sus siglas en inglés) es un software que se ejecuta en una blockchain y ofrece a los usuarios un modelo integrado para gestionar su código de forma colectiva. A diferencia de las organizaciones tradicionales, que están dirigidas por juntas, comités y ejecutivos, las DAO operan de manera autónoma y descentralizada.

Imaginemos una máquina expendedora que no solo nos quita dinero y nos da un bocadillo a cambio, sino que también utiliza ese dinero para reordenar automáticamente los productos. Esta máquina también ordena servicios de limpieza y paga el alquiler por sí misma. Además, a medida que invertimos dinero en esa máquina, tanto nosotros como otros usuarios tenemos voz y voto en cuanto a qué bocadillos ordenará y con qué frecuencia deberá limpiarse.

No tiene administradores; todos esos procesos fueron preescritos en un código. Así es, a grandes rasgos, como funciona una DAO[4]:

- Con reglas preprogramadas: una DAO tiene un conjunto de reglas codificadas como un contrato inteligente. Este contrato es esencialmente un programa de computadora que existe autónomamente en Internet pero requiere que las personas reales realicen tareas que no puede hacer por sí mismo.
- Con financiación y propiedad interna: durante la fase de financiación, una DAO debe obtener propiedad interna, que generalmente se representa mediante tokens. Estos tokens pueden gastarse dentro de la organización o utilizarse para recompensar actividades específicas.
- Con derechos de voto y participación: al invertir en una DAO, los usuarios obtienen derechos de voto y la posibilidad de influir en su funcionamiento. Una vez desplegada, la DAO se convierte en un organismo totalmente autónomo e independiente de sus creadores y cualquier otra persona.

En resumen, las DAO son una combinación de tecnología blockchain y gestión descentralizada, donde las decisiones se toman colectivamente y sin intermediarios.

De este modo las Organizaciones Autónomas Descentralizadas (DAO) son estructuras digitales que operan de manera autónoma mediante contratos inteligentes en una blockchain. Aunque no tienen una autoridad central, su gobernanza es fundamental para su funcionamiento eficiente. Estas serían las directrices esenciales sobre cómo se gobiernan las DAO:

- El *poder de voto* en una DAO está determinado por la propiedad confirmada de NFT (Tokens no fungibles). Los propietarios de NFT se convierten automáticamente en parte del proceso de toma de decisiones. Estos derechos de voto también otorgan acceso a la gobernabilidad dentro de la DAO.
- Además de los derechos de voto, las DAO utilizan *tokens de gobernanza*. Estos tokens permiten a los participantes influir en las decisiones y en la dirección de la organización. Los titulares de estos tokens pueden

[4] https://es.cointelegraph.com/learn/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work

proponer cambios, votar en propuestas y participar activamente en la toma de decisiones.

- Para abordar el problema de los titulares inactivos, algunas DAOs implementan *delegados con derecho a voto*. Estos delegados representan a otros titulares y pueden votar en su nombre. Si se utilizan delegados con derecho a voto, hay que asegurarse de que sean responsables y rindan cuentas.

En resumen, la gobernanza de una DAO se basa en la participación activa de los miembros, la propiedad de tokens y la toma de decisiones descentralizada. Así pues, en una Organización Autónoma Descentralizada (DAO), prevenir el abuso de poder es crucial para su funcionamiento justo y equitativo. Hay algunas estrategias para evitarlo:

- La transparencia y participación se debe de fomentar en las decisiones y operaciones de la DAO. La información debe estar disponible para todos los miembros.
- Para ello hay que involucrar a los miembros en la toma de decisiones. Los mecanismos de votaciones abiertas y discusiones públicas ayudan a evitar concentraciones de poder.
- La utilización de reglas claras en el contrato inteligente de la DAO para definir cómo se toman las decisiones y cómo se asignan los recursos es un elemento esencial para su correcto funcionamiento. Los tokens de gobernanza deben distribuirse de manera justa y reflejar la participación real de los miembros.
- Es necesario realizar auditorías periódicas para verificar la integridad del código y la gestión financiera, así como evaluar regularmente el funcionamiento de la DAO y ajustar las reglas según sea necesario.

En resumen, la prevención del abuso de poder en una DAO requiere una combinación de estructuras sólidas, participación activa y una cultura de confianza y cooperación.

Un Smart contract o contrato inteligente es un acuerdo entre dos personas o entidades expresado en código informático y programado para ejecutarse automáticamente. La idea de los contratos inteligentes fue propuesta por Nick Szabo en los años 90. Él los definió como un conjunto de promesas virtuales con protocolos asociados para hacer que se cumplan. En esencia, un contrato

inteligente es una versión digital y automatizada de un contrato tradicional. Los aspectos esenciales que caracterizan a los smart contracts podemos resumirlos en los siguientes:

- Goza de ejecución automática: un contrato inteligente se ejecuta automáticamente una vez que se cumplen ciertas condiciones preprogramadas. Está escrito en un lenguaje virtual y tiene la facultad de ejecutarse y hacerse cumplir por sí mismo, sin necesidad de intermediarios.
- Necesita tecnología blockchain: los contratos inteligentes se ejecutan en blockchain, lo que garantiza que los términos del contrato se almacenen en una base de datos distribuida y no puedan modificarse. Las transacciones también se procesan en blockchain, lo que automatiza pagos y contrapartidas.
- El funcionamiento lo podemos resumir del siguiente modo: un usuario inicia una transacción desde su monedero en blockchain. La transacción llega a la base de datos distribuida, donde se confirma la identidad. Se aprueba la transacción, que puede ser una transferencia de fondos. La transacción incluye el código que define qué tipo de transacción debe ejecutarse. Las transacciones se añaden como un bloque dentro del blockchain. Cualquier cambio en el estado del contrato sigue el mismo proceso para actualizarse.
- El proceso de creación de un Smart contract es su propia esencia ya que el smart contract (o contrato inteligente) es un código digital utilizado para intercambiar activos, como acciones, dinero o propiedades, sin necesidad de intermediarios. En términos técnicos, es un contrato automatizado o autoejecutable que establece un acuerdo entre dos partes mediante código. Así pues, para crear un smart contract se necesitan los siguientes elementos:
  - Un lenguaje de programación informática adecuado ya que el smart contract se crea mediante la programación de un conjunto de reglas y condiciones que deben cumplirse para que el contrato se active.
  - Un acuerdo digital por el cual todas las partes involucradas en el contrato acuerdan las condiciones y los términos del contrato, y estos se codifican en el smart contract. Es muy dudoso que los Smart contracts cumplan los requisitos de transparencia material en el sentido de la comprensión de los mismos por parte del consumidor en el

sentido y con las exigencias en materia de consumidores exigidos por la Unión Europea[5].

- Una vez programado, el contrato se despliega en una blockchain (como Ethereum). La cadena de bloques ejecutará automáticamente el contrato cuando se cumplan las condiciones predefinidas.

En definitiva, la creación de un smart contract implica programar las reglas, acordar los términos y desplegarlo en una blockchain.

Como vemos los smart contracts ofrecen muchas ventajas, pero también tienen algunas desventajas importantes, dejando aparte la gran laguna de la información previa y la transparencia material al consumidor podemos señalar las siguientes.

La creación y programación de smart contracts puede ser técnicamente muy compleja. Requiere conocimientos sólidos en programación y comprensión de la tecnología blockchain. Aunque la inmutabilidad es una ventaja en términos de seguridad, también puede ser una desventaja. Una vez que se despliega un smart contract en la blockchain, no se puede modificar. Si hay errores o cambios necesarios, puede ser complicado corregirlos. El despliegue de un smart contract en una blockchain puede requerir el pago de tarifas inciales o de entrada (llamadas "gas" en Ethereum). Estos costos iniciales pueden ser prohibitivos para algunos usuarios. Además, los smart contracts dependen de la infraestructura tecnológica, como la disponibilidad de nodos en la red blockchain. Si la red experimenta problemas o se vuelve inaccesible, los contratos pueden quedar en un estado incierto. Aunque los smart contracts automatizan procesos, no siempre se adaptan perfectamente a las complejidades legales. Algunos acuerdos requieren interpretación humana y flexibilidad, lo que no siempre es posible con los contratos inteligentes. Por otro lado, a medida que aumenta la adopción de blockchain y smart contracts, la escalabilidad se convierte en un desafío. Las redes pueden volverse congestionadas y ralentizar las transacciones.

En resumen, aunque los smart contracts ofrecen muchas ventajas, es importante considerar estas desventajas al utilizarlos en situaciones específicas.

---

[5] El control de transparencia de las cláusulas suscritas con consumidores, conforme a la jurisprudencia establecida por el Tribunal Supremo tras la famosa Sentencia 241/2013 de 9 de mayo y otras posteriores, tiene su justificación en el artículo 4.2 de la Directiva 93/13 CEE.

Por otro lado, en relación con el cumplimiento del principio de transparencia material en la contratación a través de un smart contract sería deseable que el legislador impusiera la inscripción del modelo algorítmico contenido en el mismo y de contenido de código fuera depositado en el Registro de Condiciones Generales de la Contratación. Hay voces que cuando hablan de Smart contract dicen que se trata de una herramienta informática ya que el código de programación lo que determina es lo que ocurre según las opciones o decisiones que se adopten. Pero hay que tener en cuenta que una herramienta que genera a través de la emisión de voluntad consecuencias que se traducen en obligaciones y/o derechos para las partes, es evidentemente un contrato y ha de cumplir con los requisitos esenciales de información al consumidor exigidos por la normativa europea. El mundo de las acciones colectivas ha sido nutrido por numerosos ámbitos del sector financiero, no solamente en materias más tradicionales como la hipoteca, sino también en numerosos mecanismos de activos financieros, como operaciones multidivisas, crédito revolving y acciones preferentes.

3.2. Especial consideración de la nueva regulación por la LNMV

La Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión, con 340 artículos, 9 Disposiciones Adicionales, 7 Disposiciones Transitorias y 15 disposiciones finales, modifica diversas leyes entre ellas el Texto Refundido de la Ley de Sociedades de Capital.

Se trata de una nueva «ley marco» de los mercados de valores, persiguiendo su transparencia, su eficiencia y en definitiva la seguridad jurídica de los inversores y el "correcto funcionamiento y desarrollo de los mercados de capitales".

La Ley 6/2023, de 17 de marzo, de los Mercados de Valores y de los Servicios de Inversión en España regula los criptoactivos. Esta ley afecta a cualquier instrumento financiero que sea un criptoactivo, es decir, que esté representado mediante tecnología de registro distribuido (blockchain). Además, las infracciones y sanciones permitirán a la Comisión Nacional del Mercado de Valores (CNMV) actuar cuando entre en vigor la normativa europea. La existencia de un mercado de valores transparente y eficiente es fundamental para la economía y la protección de los inversores. La normativa reguladora de los mercados de capitales se ha transformado en las últimas décadas debido al aumento de normas reglamentarias y la incorporación de normas de derecho de la Unión Europea. Así, la nueva ley del mercado de valores aborda la regulación de los

criptoactivos y busca garantizar la protección de los inversores y la estabilidad financiera en este ámbito.

Esta Ley modifica entre otros el artículo 23 de la LSC, relativo al contenido de los estatutos de las sociedades de capital.

La única modificación que se aprecia del estudio comparativo del anterior artículo y del nuevo, es una referencia a que en las sociedades anónimas debe constar en estatutos "si las acciones están representadas por medio de títulos, o por medio de anotaciones en cuenta o mediante sistemas basados en tecnología de registros distribuidos".

Es decir, una referencia a una nueva forma de representación de las acciones en la sociedad anónima.

Por tanto, a partir de ahora y para las sociedades anónimas, entendemos sólo las cotizadas pues para las normales, sobre todo en cuanto a su transmisión regirán las normas del Código de Comercio, podrá escogerse como sistema de representación de sus acciones la llamada "tecnologías de registro distribuido (distributed ledger technologies, en inglés) y, en particular, la tecnología de cadenas de bloques (o blockchain, en inglés)".

Como hemos explicado hasta ahora, estas tecnologías se apoyan en claves criptográficas que permiten la creación de un registro inalterable, gestionado de forma absolutamente descentralizada, que podrá ser utilizado no solo para la representación de las acciones sino también y quizás sea lo más importante para su transmisión, aunque respeto de esta última deberán coordinarse las técnicas del blockchain con las normas sobre prevención del blanqueo de capitales. En definitiva, se trataría de una nueva forma disruptiva introducida para facilitar la digitalización y las transferencias de las acciones, ya que como dicen autores como Swan la tecnología de cadenas de bloques viene a ser "como un protocolo de software y un libro de registro distribuido para registrar transacciones, que puede actuar como sustrato computacional a escala global para el procesamiento de cualquier tipo de actividad digitalizada". No obstante, ahora veremos que incluso aunque se utilice esta tecnología para la representación de las acciones, estas quedan sujetas al requisito de su control por una entidad externa.

En todo caso, esta novedosa forma de representación de las acciones debe ponerse en relación con los artículos 5 a 15 de la propia Ley en cuanto trata en general de los valores negociables.

De ellos y en forma muy extractada deducimos que la nueva ley en este punto casi se limita a trasladar a esta nueva forma de representación de las acciones de las cotizadas, las normas que antes existían para las anotaciones en cuenta. Es el capítulo 2 del Título I. En resumen:

- Se empieza diciendo que todo ese capítulo 2 se aplica también a los valores representados mediante sistemas basados en tecnología de registros distribuidos siempre que se prevea en el acuerdo de emisión.
- Aunque no se prevea también serán aplicables cuando el emisor tenga su domicilio social en territorio español o, cuando el emisor designe una única entidad responsable de la administración de la inscripción y registro de los valores en el sistema, cuando dicha entidad tenga su domicilio social en territorio español.
- Los valores negociables deberán representarse por medio de anotaciones en cuenta, títulos o sistemas basados en "tecnología de registros distribuidos".
- Si lo valores son negociables, la representación por anotaciones en cuenta o por tecnología de registros es obligatoria.
- Reglamentariamente podrá determinarse la forma en que si están representados por anotaciones en cuenta podrán cambiarse a registros distribuidos y viceversa.
- Si el sistema es de "tecnología de registros distribuidos" se deberá garantizar la integridad e inmutabilidad de las emisiones que en ellos se realicen, identificar de forma directa o indirecta a los titulares de los derechos sobre los valores negociables y determinar la naturaleza, características y número de los mismos.
- La representación requiere la elaboración por la entidad emisora de un documento en el que constará la información necesaria para la identificación de la entidad encargada del registro contable o la responsable de la administración de la inscripción y registro, Ese documento deberá estar a disposición de los titulares y del público interesado en general.
- El artículo siguiente trata de las entidades encargadas del registro contable y entidades responsables de los valores representados por medio de sistemas basados en tecnología de registros distribuidos.
- Si se trata de anotaciones en cuenta no hay grandes cambios y si se trata de valores negociables representados mediante sistemas basados en

tecnología de registros distribuidos se llevará a cabo en la forma prevista en el documento de la emisión debiendo designar una o varias entidades que serán responsables de la administración de la inscripción y registro de los valores en el sistema, debiendo ser entidades debidamente autorizadas.

- El sistema de registro y tenencia de valores negociables representados mediante anotaciones en cuentan es similar al actualmente existente.
- Los valores negociables representados por medio de anotaciones en cuenta, o por medio de sistemas basados en tecnología de registros distribuidos, se constituirán como tales en virtud de su inscripción en el correspondiente registro de la entidad encargada del registro contable.
- La transmisión de los valores negociables representados por medio de anotaciones en cuenta tendrá lugar por transferencia contable.
- La transmisión de los valores representados mediante sistemas basados en tecnología de registros distribuidos tendrá lugar mediante la transferencia registrada en el registro distribuido.
- La inscripción o registro de la transmisión producirá los mismos efectos que la entrega de los títulos.
- La transmisión será oponible a terceros desde el momento en que se haya practicado la inscripción en el sistema de anotaciones en cuenta o en el sistema basado en tecnología de registros distribuidos, según el caso. Se aplica en estos registros el sistema de fe pública.
- Se sigue estableciendo que la suscripción o transmisión de valores negociables sólo requerirá para su validez la intervención de notario cuando, no estando admitidos a negociación en un mercado regulado, estén representados mediante títulos al portador y dicha suscripción o transmisión no se efectúe con la participación o mediación de una sociedad o agencia de valores, o de una entidad de crédito.
- También deberán inscribirse en los registros contables o en el nuevo sistema de blockchain, la constitución de derechos reales limitados u otra clase de gravámenes sobre valores negociables, sea cual sea su representación.
- Los sistemas basados en "tecnología de registros distribuidos" deberán contar con los mecanismos necesarios para realizar la inscripción de cualesquiera actos y negocios jurídicos. La constitución del gravamen será oponible a terceros desde el momento en que se haya practicado la correspondiente inscripción.

- En ambos tipos de registros se aplica el principio de legitimación registral y de tracto sucesivo.
- La legitimación para el ejercicio de derechos se acredita mediante certificados expedidos por las entidades encargadas de los registros contables.
- Si se declara el concurso de la entidad encargada del registro, los titulares de valores negociables anotados o inscritos en dichos registros gozarán del derecho de separación respecto de los valores negociables inscritos a su favor y lo podrán ejercitar solicitando su traslado a otra entidad.

Así pues, la nueva Ley de lo que trata es de aplicar a la utilización de la tecnología blockchain los mismos principios que a los registros de anotaciones en cuenta, si bien existen diferencias en sus consecuencias a nuestro juicio que deben de salvarse como veremos a continuación.

4. CONTRIBUCIÓN DE LOS REGISTROS JURÍDICOS

4.1. Garantías necesarias del Registro de la Propiedad

Hemos visto como la tokenización puede ser una forma de transmisión que se emplea respecto de los activos digitales que son el objeto de la red blockchain (por ejemplo, bitcoin), o puede también utilizarse para activos existentes al margen de la red (por ejemplo, inmuebles). En este último caso es necesario atribuirle a ese activo físico una representación digital, esto es un token o ficha que lo representa. En general podemos decir que los tokens son la unidad de valor de la cadena de bloques.

Por lo tanto, la tokenización inmobiliaria es el negocio jurídico por el que se atribuye una representación digital a un inmueble físico en la cadena de bloques.

El token inmobiliario/mobiliario es la representación digital del derecho real; no supone la incorporación del derecho al token. El token no es un título valor que incorpore el derecho real inmobiliario. La simple tenencia del token (título) no legitima para el ejercicio del derecho, no representa la propiedad; del mismo modo que la escritura no es título que incorpore el derecho de propiedad. El equivocar esta cuestión supondría alterar todo el ordenamiento jurídico existente: si el token (título) incorpora el derecho: ya solo podrían realizarse transmisiones digitales, no en otras formas; y se acabaría con la teoría del título y modo para la transmisión del dominio. La simple transmisión del título (token) supondría la transmisión del derecho de propiedad. Estos tokens

de activos físicos, al contrario, son un símbolo, un símbolo digital que funciona y permite la traditio simbólica digital en las transacciones digitales.

Así en la relación de la tokenización de bienes inmuebles y el Registro de la Propiedad hay que tener en cuenta que el control de legalidad independiente y bajo la responsabilidad patrimonial del registrador, la protección que los principios hipotecarios atribuyen a los titulares de derechos resales inscritos, la transparencia del procedimiento registral y la publicidad de los derechos inscritos, convierten al Registro de la Propiedad en la institución jurídica necesaria para permitir la vinculación jurídica entre activos físicos y tokens y, consecuentemente, dotar de seguridad jurídica y transparencia a la tokenización de activos inmobiliarios.

Es imprescindible que el mundo digital (token) esté conectado y vinculado con el mundo físico (bien inmueble), y viceversa. Es necesario asegurar que el token está inseparablemente unido al activo inmobiliario y, consecuentemente, al derecho real inmobiliario existente sobre el mismo. Sin esta vinculación permanente la tokenización de activos inmobiliarios estará condenada a la intrascendencia jurídica y no aportará valor añadido alguno a los operadores del mercado inmobiliario.

La tokenización de bienes inmuebles implica la coexistencia simultánea del activo físico con su representación digital (token) que refleja a ese concreto bien inmueble o participación indivisa del mismo en la cadena de bloques. Los bienes inmuebles son bienes tangibles, con una existencia física y ubicación determinada, bienes no fungibles. Estos bienes inmuebles perfectamente individualizados e identificados constituyen el objeto de los denominados derechos reales inmobiliarios. Y estos derechos reales, si están inscritos en el Registro de la Propiedad, presentan tres efectos jurídicos esenciales, conforme a los artículos 32, 34 y 38 de la LH, consecuencia del control de legalidad registral de todos los actos y contratos relativos al dominio y demás derechos reales sobre bienes inmuebles que pretenden su acceso al Registro de la Propiedad, conforme al artículo 18 de la LH. Por un lado, los derechos reales inmobiliarios sólo serán oponibles a todo tercero, eficacia erga omnes, si están inscritos en el Registro de la Propiedad. Por otro lado, quien adquiere del titular registral e inscribe su derecho a título oneroso y de buena fe queda protegido, en todo caso, en su adquisición, aunque se anule o resuelva el derecho del transmitente por causas ajenas al Registro. Finalmente, y a todos los efectos legales, se presume que los derechos reales

inscritos en el Registro existen y pertenecen a su titular en la forma determinada por el asiento registral correspondiente.

Esta caracterización y efectos jurídicos de la institución del Registro de la Propiedad determinan que deba ser la institución que conecte y vincule el activo físico inmobiliario, el derecho real sobre el mismo, y su representación digital, el token, el mundo onchain y offchain, de manera indubitada, con plena seguridad jurídica y plena transparencia para el tráfico jurídico inmobiliario.

Ahora bien, nos preguntaremos ¿cómo es posible realizar, a través del Registro de la Propiedad, esta vinculación entre el mundo físico y el mundo digital?

En un primer momento, una vez creado un token en la plataforma, el mismo se puede asociar voluntariamente por el titular registral a una finca registral mediante su constancia en el Registro. Así se lograría la vinculación del token a la finca registral, reflejando la circunstancia de estar representado el derecho real en un token a través de una nota marginal[6].

En segundo lugar, la transmisión del derecho real de forma digital se podrá hacer en la plataforma mediante el desplazamiento del token, quedando acreditado el acuerdo de voluntades y la traditio simbólica digital (transmisión privada "cualificada").

En tercer lugar, estas transmisiones pueden acceder al Registro de la Propiedad para su control de legalidad y efectos erga omnes. El acceso se haría de forma telemática a través de los canales correspondientes[7].

Siempre teniendo en cuenta que la constancia de la tokenización en el Registro de la Propiedad, no excluye el que siga pudiendo transmitirse en forma no digital, transmisiones que seguirán accediendo al Registro de la Propiedad por los canales habituales. El registro compatibiliza transmisiones digitales y no digitales, como puerto natural de llegada de todas ellas, pero siempre con la aplicación de sus principios esenciales entre las mismas.

---

[6] Mediante el artículo 9.a del Decreto de 8 de febrero de 1946, por el que se aprueba la nueva redacción oficial de la Ley Hipotecaria: "*Cuando conste acreditada, se expresará por nota al margen la calificación urbanística, medioambiental o administrativa correspondiente, con expresión de la fecha a la que se refiera*".

[7] Véase https://sede.registradores.org/site/presentacion-telematica

De no practicarse esta conexión con el Registro de la Propiedad tendríamos las siguientes insuficiencias indeseables de las plataformas blockchain para operar como registro:

- Obligaría a que todas las transmisiones fueran digitales, no podrían admitirse transmisiones documentales, pues estas se realizan, necesariamente, al margen de la plataforma.
- No accederían transmisiones forzosas (embargos, ejecuciones, expropiaciones...) dado que el control del token que representa al activo se realiza a través del empleo de claves privadas, en manos siempre del titular. La plataforma no puede intervenir, desconoce las claves.
- Duplicidad de tokenizaciones (transmisiones del mismo inmueble/mueble) en múltiples plataformas. Al existir libertad de mercado, son muchas las plataformas existentes.
- Inviabilidad de obtener una publicidad registral cierta y de confianza, por no existir un único registro, sino múltiples plataformas.
- Imposibilidad de garantizar que el token represente al activo inmobiliario/mobiliario que se transmite. No sería posible vincular el activo físico y el token.
- El token operaría como título-valor, con el derecho real incorporado, por lo que la simple transmisión del token supondría la transmisión del dominio, lo que llevaría a la desaparición del sistema de título y modo como sistema de transmisión
- No existiría control de legalidad. En las plataformas blockchain los nodos pueden garantizar que una transmisión del token se ha producido, pero no que es cierta y legal, dado que realizan un control puramente algorítmico.
- Problema en caso de pérdida u olvido de las claves que conllevaría la imposibilidad de disponer del token, y por lo tanto del bien.
- Privatización del registro, en manos de plataformas tecnológicas.
- Imposibilidad de publicidad y eficacia frente a terceros de la información registral asociada.

La tokenización de bienes inmuebles tiene dos características diferenciadoras de otros supuestos de tokenización:

- Por la especialidad de su objeto, nos encontramos, por un lado, en presencia de derechos reales y no de derechos personales.

- Por otro lado, puede dar lugar a una nueva forma de contratación y transmisión de bienes inmuebles –adicional a las ya tradicionales– consecuencia de blockchainizar el proceso de contratación inmobiliaria. La tecnología blockchain permite constatar y acreditar con sus técnicas de encriptación y distribución o réplica de información en nodos, la existencia, potencialmente el contenido, la fecha y, en caso de utilización de certificados electrónicos eIDAS, las partes intervinientes de un determinado hecho, acto o negocio jurídico. De la misma manera que los hechos, actos o negocios jurídicos pueden reflejarse mediante una mera forma verbal o con una forma escrita –ya sea forma privada o pública–, esta nueva tecnología permite reflejar y formalizar, igualmente, hechos, actos o negocios jurídicos de una manera digital.
- Es la «forma digital»: la forma no es, con carácter general, requisito constitutivo para el nacimiento o transmisión de derechos reales inmobiliarios (arts. 1278 a 1280 del Código Civil), por lo que no existe ningún impedimento jurídico para que la transmisión de derechos reales se pueda realizar también a través de la «forma digital» mediante la utilización de la tecnología blockchain y, completarse, obteniendo su protección erga omnes, con la inscripción, previo control registral de su legalidad.
- La tecnología blockchain no puede configurarse como un registro jurídico de derechos porque como tecnología no puede realizar un control de legalidad independiente y responsable de los hechos, actos o negocios jurídicos que se reflejen en sus nodos.

Por todo ello, la inscripción registral de la tokenización implica (sin perjuicio de los mencionados efectos de oponibilidad, fe pública, legitimación y exactitud) la posibilidad de transmitir derechos reales en «forma digital» a través de la tecnología blockchain, y que dichas adquisiciones de derechos reales inscritos tokenizados, puedan, a su vez, inscribirse en el Registro de la Propiedad, previo su control de legalidad registral, para poder tener eficacia frente a terceros, erga omnes y estar protegidas por los principios hipotecarios. Si, por el contrario, el adquirente del token decide no inscribir su adquisición digital, como la «forma digital» es una forma privada de adquisición de derechos, sus efectos serán los mismos que los casos de adquisición de un derecho real mediante documento privado. El derecho real podrá haber sido adquirido, pero, en ningún caso, será oponible a terceros al no estar inscrito en el Registro de la Propiedad.

4.2. Papel del Registro de Bienes Muebles

La misma estructura jurídica para la tokenización de activos inmobiliarios a través del Registro de la Propiedad puede ser aplicada en el ámbito mobiliario, a través del Registro de Bienes Muebles, como auténtico registro de titularidades y cargas, en donde son de aplicación, igualmente, los principios hipotecarios mencionados[8].

En el ámbito de los bienes muebles identificables, la titularidad y gravámenes existentes sobre los mismos puede, con carácter general, obtenerse con eficacia erga omnes a través de su inscripción registral. La voluntaria decisión del titular de un bien mueble para poder transmitir la titularidad de su derecho real mobiliario o de constituir un derecho real limitado, además de mediante las demás formas existentes, en forma digital mediante la creación de un token en una plataforma con tecnología blockchain requerirá, en primer lugar, la previa vinculación entre el activo físico y el token representativo del mismo. Esta vinculación se realizará con plena transparencia y seguridad jurídica, en los mismos términos explicados anteriormente en materia inmobiliaria, mediante la inscripción de la identificación del token y de la plataforma objeto de circulación de este en el Registro de Bienes Muebles. Además, en segundo lugar, dadas las características físicas de los bienes muebles y su facilidad de desplazamiento y movilidad, parece recomendable, en su caso, que, si van a ser objeto de transmisión en forma digital o blockchainizada, el bien sea objeto de depósito o custodia ante una institución o entidad específica, de cara a asegurar su entrega material o posesión al adquirente de su token representativo.

Producida la transmisión del derecho real en la plataforma con tecnología blockchain, conforme a las reglas generales anteriormente comentadas, cumpliendo la teoría del título y del modo con la traditio simbólica de entrega del token como signo o símbolo representativo del bien mueble objeto de transmisión, el adquirente tendrá la posesión del token, pero sólo, al igual que en el ámbito inmobiliario, la plena propiedad del bien mueble interpartes y no con eficacia frente a terceros, erga omnes. Posesión y propiedad son conceptos jurídicos distintos. La posesión del token resulta de la tenencia de la clave privada, sin embargo, en la medida que la tokenización, bajo el principio de libertad de forma y neutralidad

---

[8] Jiménez Rubio, R. (2022). "La nueva regulación de los criptoactivos en España", Escuela de Práctica Jurídica de la Universidad Complutense, 8 de marzo.

tecnológica, es sólo una forma adicional y digital de representar un hecho, acto o negocio jurídico, nada impide que pueda el titular efectuar transmisiones en formas no digitales, que el bien mueble pudiera haberse transmitido también offchain (imaginemos una venta del bien mueble con traditio instrumental, en contrato privado). Por esta razón, también en el ámbito mobiliario, al igual que en el ámbito inmobiliario, para garantizar la seguridad jurídica y la transparencia en el mercado de bienes, la adquisición del token representativo del bien mueble debe inscribirse en el Registro de Bienes Muebles para que, previo control registral de su legalidad, el adquirente en forma digital pueda ser considerado propietario con plena eficacia frente a terceros, erga omnes, y obtener del custodio o depositante, mediante la certificación registral acreditativa de su derecho real de propiedad mobiliaria erga omnes, la entrega o posesión material del bien mueble adquirido de forma digital, al igual que en forma no digital, si finalmente, hubiese sido esta la forma de transmisión seleccionada.

Mención especial merecen los tokens no fungibles –Non-Fungible Tokens (NFT)– que han irrumpido recientemente en el mercado del arte alcanzando precios astronómicos.

Cada vez son más quienes crean, no sólo obras de arte, sino colecciones de moda u objetos o accesorios para los juegos virtuales, tokenizándolos a través de NFT.

Estos NFT, tokens únicos que no pueden ser replicados, no evitan la reproducción de la obra en sí, pues esta podrá seguir siendo copiada, al igual que cualquier otro archivo digital, pero sí logran atribuir una prueba de autenticidad, de ser el original. Es una idea similar a las fotografías, en las que no pudiendo evitar su réplica, se trataba de lograr la escasez mediante el lanzamiento de ediciones limitadas, acompañadas de certificados de autenticidad.

Adicionalmente, si se añaden smart contracts podría programarse de tal forma que en caso de venta del NFT un porcentaje de la transacción revierta en el artista, logrando así una remuneración para el autor en el caso de reventa. En definitiva, las bondades de los NFT residen en atribuir una prueba de originalidad y en facilitar que el artista obtenga una comisión en caso de reventa, pero no impiden la copia.

En todo caso, es imprescindible que estemos en presencia de activos nativamente digitales, los NFT mencionados se refieren a activos intangibles del mundo digital. En el caso que la obra de arte tenga una existencia física, tangible,

estos NFT no resuelven los problemas, expuestos a lo largo de todo el artículo, de cómo conseguir la vinculación entre el activo digital –NFT– y la obra de arte y como conseguir la necesaria compatibilidad entre la posible transmisión digital y la posible transmisión no digital, derivada de su propia existencia física, y que sólo pueden resolverse configurando jurídicamente los NFT sobre activos físicos en los términos anteriormente explicados.

4.3. Desde el Registro Mercantil

En el ámbito societario, las acciones de la sociedad anónima y las participaciones sociales de las sociedades de responsabilidad limitada tiene su régimen jurídico esencialmente regulado en el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, (en adelante, "TRLSC") siendo configuradas como partes alícuotas indivisibles y acumulables del capital social que atribuyen a los socios una serie de derechos políticos y económicos. Las acciones podrán estar representadas por medio de títulos o por medio de anotaciones en cuenta, teniendo en ambos casos la consideración de valores mobiliarios mientras que las participaciones sociales no podrán estar representadas por medio de títulos ni anotaciones en cuenta y, en ningún caso, tendrán el carácter de valores. Por esta razón, para analizar el alcance de una posible tokenización en materia de acciones y participaciones hemos de diferenciar la forma de representación de las acciones y participaciones sociales de los derechos políticos y económicos que las mismas conceden a sus titulares.

En las *sociedades limitadas*, empezando nuestro análisis por las participaciones sociales, el TRLSC, en su art. 104, establece que su titularidad original y las sucesivas transmisiones voluntarias o forzosas, así como la constitución de derechos reales sobre las mismas se harán constar en un libro registro de socios, reputando la sociedad sólo socio a quien se halle inscrito en dicho libro, que podrá ser examinado por cualquier socio. Las participaciones no pueden estar representadas ni por medio de títulos, ya sea físicos o digitales, ni por medio de anotaciones en cuenta y, en ningún caso, tener la consideración de valores, ex art. 92 TRLSC. Esto es, no podrán incorporar y atribuir derechos mediante un título susceptible de transmisión con su entrega material o electrónica. Sin embargo, las participaciones sociales atribuyen a sus titulares una serie de derechos políticos y económicos conforme al art. 93 TRLSC, que pueden, en su caso, ser objeto de transmisión a un tercero distinto del titular de la participación, como ocurre con el usufructo de participaciones, regulado en los arts. 127

y ss. del TRLSC, donde se atribuye al usufructuario el derecho en todo caso a los dividendos, manteniendo el nudo propietario la cualidad de socio.

Este derecho real limitado de usufructo podría ser objeto de representación digital por medio de un signo o símbolo representativo del mismo, por medio de un token, que no incorpora ni atribuye el derecho, sino que representa un derecho inscrito –al igual que los tokens representativos de derechos reales inmobiliarios mencionados– y cuya titularidad esta hoy determinada por el libro registro de socios. Este token habilitaría, como signo o símbolo representativo de carácter digital, la posibilidad de transmisión en forma digital –adicional y compatible con la transmisión no digital–, funcionando a modo de certificación del artículo 105 TRLSC, y no tendría la consideración de valor.

Esta misma estructura de tokenización podría ser empleada para la transmisión digital por medio de tokens representativos de derechos de copropiedad de participaciones, en los términos admitidos por el artículo 126 TRLSC, así como del propio derecho de propiedad de la participación social, en la medida que el token, como símbolo o signo representativo de un derecho real, a modo de certificación digital, no incorpora ni atribuye el mismo derecho ni habilita su transmisión por el mero desplazamiento digital, al no tener la consideración de valor. El token facilita su transmisión en forma digital –como una forma adicional y compatible con la forma no digital– creando un símbolo o signo representativo que permitirá acreditar y formalizar digitalmente el acuerdo de voluntades en la plataforma DLT y consultarse, en todo caso, el legítimo titular del derecho del transmitente, con plena transparencia, en el Registro Mercantil. Este acuerdo de voluntades podrá inscribirse, como hemos mencionado, en el Registro Mercantil y en el libro registro de socios siendo considerado, en todo caso, titular del derecho frente a la sociedad sólo quien conste inscrito en el libro registro de socios y, más transparentemente, en el Registro Mercantil.

Finalmente, la anterior estructura jurídica de tokenización podría parecer ser igualmente aplicable, en el ámbito de la *sociedad anónima*, a las acciones nominativas que deben figurar en el libro registro de acciones nominativas, mediante su transmisión en forma digital como signo o símbolo digital. No obstante las acciones, que tienen una naturaleza jurídica sustancialmente distinta de las participaciones, como valores mobiliarios que incorporan un derecho, art. 92 TRLSC –que si bien es algo ajeno a la figura del token representativo de derechos sobre activos físicos determinados, como símbolo o signo– tienen actualmente,

a diferencia de las participaciones, la posibilidad de ser representadas mediante esta tecnología tras la reforma comentada como hemos visto con anterioridad, permitiéndose su ámbito de circulación electrónica, como valores mobiliarios, a través de la representación de las mismas mediante anotaciones en cuenta con sujeción a lo dispuesto en la normativa reguladora del mercado de valores[9].

En otro orden de cuestiones, cabe destacar que la nueva regulación de la emisión de valores anteriormente expuesta tras la nueva reforma de la Ley del Mercado de valores adolece de algunas cuestiones de interés. La separación del Registro de bienes muebles de derechos reales como el usufructo, prenda o los posibles embargos o prohibiciones de disponer que se puedan establecer sobre los mismos habida consideración de su naturaleza mobiliaria pueden dar lugar a actuaciones fraudulentas y a opacidad en relación con los mismos. Del mismo modo al ser una tecnología DLT la clave privada no será suministrada por el titular de forma voluntaria para el embargo de sus valores. No se resuelven las garantías reales sobre los mismos de una forma satisfactoria.

Hay que señalar que las entidades encargadas del registro contable que crea la nueva ley son verdaderos administradores de la sociedad emisora matriz por lo que deberán de ser objeto de inscripción en el Registro Mercantil so pena de nulidad de los actos ejecutados por las mismas frente a terceros pudiendo conllevar la nulidad per se del acto de emisión en blockchain.

4.4. Registro de Condiciones Generales de la Contratación

El Registro de Condiciones Generales de la Contratación como «instrumento jurídico integrado» en el marco de armonización de la Directiva 93/13/CEE, con la finalidad de garantizar al consumidor un mayor nivel de protección (artículos 7.1 y 8 de la Directiva y 8 bis y 8 ter, tras su modificación por las Directivas 2011/83/ UE y 2019/216/UE) es el elemento necesario para dotar de trasparencia a las emisiones de valores digitales, no bastando el mero deposito del folleto manteniendo el legislador inexplicablemente un modelo obsoleto de publicidad al consumidor.

---

[9] González Hernández, I., "Informe Innovación y Tendencias 2023", fundación corporativa de Aranzadi La Ley.

Como hemos expresado, es pues, un registro público de carácter jurídico a cargo de los Registradores de la Propiedad y Mercantiles, en el que se anotan preventivamente las acciones colectivas de cesación, de retractación y declarativas previstas en la legislación para la Defensa de los Consumidores y Usuarios, así como el depósito de los modelos de contratos para la inscripción de las cláusulas de condiciones generales de la contratación.

En este Registro, muchas veces desconocido por quienes no lo utilizan, se depositan:

- Las cláusulas contractuales que tengan el carácter de condiciones generales de la contratación.
- Los formularios de los préstamos y créditos hipotecarios comprendidos en el ámbito de aplicación de la Ley 5/2019, reguladora de los contratos de crédito inmobiliario. deberán depositarse obligatoriamente por el prestamista en el Registro antes de empezar su comercialización.

También son objeto de anotación preventiva:

- La interposición de las demandas ordinarias de nulidad o de declaración de no incorporación de cláusulas generales.
- Las acciones colectivas de cesación, de retractación y declarativa previstas en el capítulo IV de la Ley.
- Las resoluciones judiciales que acuerden la suspensión cautelar de la eficacia de una condición general.

Este carácter sistémico de la Directiva 93/13 en orden al marco de armonización del espacio europeo de la contratación bajo condiciones generales, ha sido destacado, de forma muy reiterada, por la jurisprudencia del TJUE en atención a las notas de «transversalidad u horizontalidad» que caracterizan su ámbito de aplicación (entre otras, STJUE de 6 de julio de 2017 asunto C-290/16). De forma que, por una parte, la Directiva 93/13 resulta de aplicación, tanto de oficio como de modo general, en todo «el ámbito material del derecho de consumidores de la Unión Europea» (STJUE de 21 de abril de 2015, asunto C-377/14) y, por otra parte, resulta de aplicación a todos los contratos celebrados entre profesionales y consumidores en «todos los sectores de la actividad económica», como también, si es del caso, de forma concurrente con las otras disposiciones de la normativa europea en materia de protección de consumidores (STJUE de 16 de noviembre de 2010, asunto C- 76/10).

Por lo que la interrelación de la Directiva 93/13, como eje central de referencia conceptual para la aplicación de otros actos regulatorios de la Unión Europea, es cada vez «más extensa e intensa» conforme se van desarrollando o implementando los distintos sectores económicos del Mercado interior europeo; casos, entre otros muchos, del reciente Reglamento 2019/ 1150/UE, sobre Equidad y Transparencia en los servicios de interrelación en línea, así como de los Reglamentos 2022/1925/UE y 2022/2065/UE sobre Mercados y Servicios Digitales, respectivamente.

No es de extrañar, por tanto, que el citado Comunicado de la Comisión subraye este papel central que desempeña la Directiva 93/13 como instrumento normativo para lograr la equidad y el buen funcionamiento del Mercado interior europeo.

En este contexto es donde la Directiva 93/13 juega el papel de un «Código Europeo» de la contratación bajo condiciones generales, pues en la decantación de sus principios y directrices están las claves interpretativas que ordenan el Espacio Europeo de este importante sector: su régimen jurídico y los derechos de los consumidores[10].

En definitiva, la tokenización como medio de transmisión de activos inmobiliarios, mobiliarios o de valores no puede vivir al margen de los registros jurídicos de la Propiedad, Mercantil y de Bienes Muebles so pena de incurrir en una disminución de la seguridad jurídica y de la protección del consumidor, el legislador en aras del cumplimiento del principio de supremacía del derecho europeo debe tener muy en cuenta la protección de los consumidores y usuarios. Su importancia ha sido puesta de relieve por una reciente sentencia del TJUE en la que se destaca que los artículos 3, apartado 1, 6, apartado 1, 7, apartado 1, y 8 de la Directiva 93/13 deben interpretarse en el sentido de que, no se oponen a una jurisprudencia nacional según la cual la inscripción de la cláusula de un contrato en el registro nacional de cláusulas ilícitas supone que se considere abusiva dicha cláusula en todo procedimiento en el que intervenga un consumidor, incluso en relación con un profesional que no sea aquel contra el que se hubiera incoado el procedimiento de inscripción de dicha cláusula en ese registro nacional (eficacia

---

[10] Orduña Moreno, F. J. (2023). "El Anteproyecto de Ley de acciones de representación para la protección de los intereses colectivos de los consumidores: la innecesariedad de la creación de un nuevo registro público", Diario La Ley, núm. 10245, Sección Tribuna, 10 de marzo, La Ley.

erga omnes de la publicidad registral) y cuando la misma cláusula no presente un tenor idéntico al de la cláusula inscrita, pero tenga el mismo alcance y produzca los mismos efectos para el consumidor afectado (extensión de la eficacia erga omnes a cláusulas semejantes).

BIBLIOGRAFÍA

Akour, Iman A., Al-Maroof, Rana-Saeed, Alfaisa, Raghad y Salloum, Said A. (2022). "A conceptual framework form determining metaverse adoption in higher institutions of Gulf area: an empirical study using hybrid SEM-ANN approach". *Computers and education: artificial intelligence*, Vol. 3. https://doi.org/10.16/j.caeai.2022.100052

Ball, M. (2022). *El metaverso*. https://www.google.es/books/edition/El_metaverso/r896EAAAQBAJ?hl=es&gbpv =1&dq=Matthew+Ball++metaverso&printsec=frontcover

Cuesta Cano, L. (2023). *Crecer con Pantallas. Como enseñar a tus hijos a usar y disfrutar de la tecnología de forma segura y saludable*, Amat, Madrid, capítulo 7.

Díaz Vico, J. y Sánchez Aragó, A. (2024). *Bitcoin, una moneda criptográfica*. https://www.incibe.es/incibe-cert

González Hernández, I. "Informe Innovación & Tendencias 2023", fundación corporativa de Aranzadi-La Ley.

Jiménez Rubio, R. (2022). "La nueva regulación de los criptoactivos en España", Escuela de Práctica Jurídica de la Universidad Complutense, 8 de marzo.

Kaur, G. y Cornèr, K. L. (2024). *¿Qué es dao?*, febrero. https://es.cointelegraph.com/learn/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Orduña Moreno, F. J. (2023). "El Anteproyecto de Ley de acciones de representación para la protección de los intereses colectivos de los consumidores: la innecesariedad de la creación de un nuevo registro público", *Diario La Ley*, núm. 10245, Sección Tribuna, 10 de marzo, La Ley.

Sieira Gil, J. (2021). *III Jornada Blockchain Economía realizada con el Campus de la Universidad de Navarra*, Madrid, 25 de octubre.

STJUE (2023). *Los procedimientos simplificados de apreciación del carácter abusivo de una cláusula contractual*, ECLI:EU:C:2023:212, Asunto C-565/21, de 21 de septiembre.

Valero Fernández-Reyes, Á. *Comentario de la Sentencia del Tribunal Supremo de 9 de mayo de 2013 (1916/2013) consumidores: condiciones generales abusivas. Cláusula suelo en los préstamos hipotecarios. Efectos de su nulidad*. https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2013-9

Vidal-Tomás, D. (2022). "The new crypto niche: NFTs, play-to-earn, and metaverse tokens", *Finance research letters*, Vol. 47. https://doi.org/10.1016/j.frl.2022.102742

Capítulo 14
METAVERSO LABORAL: RIESGOS REALES EN MUNDOS VIRTUALES

Magdalena Nogueira Guastavino
Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad Autónoma de Madrid
https://orcid.org/0000-0002-3195-9332

1. AUGE Y CAÍDA DEL METAVERSO

Mucho se ha hablado y escrito ya sobre el Metaverso o multiverso (entendido este último como concurrencia de Metaversos interconectados entre sí)[1]. Solo recientemente la Comisión Europea ha ofrecido los elementos definitorios de las plataformas de Metaverso o mundos virtuales, definiéndolos como "entornos persistentes e inmersivos, basados en tecnologías como la reproducción tridimensional (3D) o la realidad expandida (XR), que permiten una fusión entre la realidad física y digital en tiempo real para múltiples propósitos tales como el diseño, la ejecución de simulaciones, la colaboración, la enseñanza, la socialización, la ejecución de transacciones o el mero entretenimiento"[2].

El metaverso sería así un "mundo tridimensional generado por ordenador "gemelo digital" de la realidad. Se trata de crear un "nuevo mundo dentro del mundo"[3], en el que se podrán reproducir todas las dinámicas sociales de la vida real. De este modo, se podrá estudiar, trabajar, tener ocio, realizar deportes, comprar todo tipo de bienes, incluidos inmuebles, viajar, acceder a la cultura,

---

[1] Para un resumen me permito remitir a mi trabajo "Metaverso y legislación aplicable al contrato de trabajo", *Revista de Trabajo y de Seguridad Social, CEF*, 471/2022, pp. 17-53.

[2] *An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition* Strasbourg, 11.7.2023 COM(2023) 442/final.

[3] Nisa Avila, J. A., "El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas, *El Derecho.com,* Lefebvre.

etc.[4]; pero también se podrán cometer infracciones y delitos, ya que se reproducirá la vida real. Como en el mundo real, el metaverso pretende ser un gran mercado de infinitas posibilidades, teniendo en cuenta que se trata de espacios sometidos a una economía propia, con moneda propia que se cambiará por dinero de curso legal. Pero, además, la realidad física y la realidad virtual estarán interconectadas. Podrás comprar un traje en Zara en el mundo virtual y ponérselo a tu avatar o representación virtual y pagar por tenerlo al mismo tiempo físicamente en tu casa. McDonald's ya se ha planteado abrir franquicias virtuales en el metaverso y servir simultáneamente a domicilio.

La clave de un metaverso futuro vendría determinada, sobre todo, por el carácter totalmente inmersivo en un entorno virtual. Es precisamente esta característica la que hace que, de momento, no se vislumbre como algo inmediato. Entre otras razones porque las experiencias inmersivas a fecha de hoy requieren aún un equipo poco accesible, física y económicamente hablando. Frente al apoteósico anuncio de Marck Zuckerberg en noviembre de 2021 de que procedía a cambiar el nombre de su compañía más conocida, Facebook, por el de Meta y que, a partir de ese momento los metaversos pasaban a ser parte fundamental de su proyecto empresarial, lo cierto es que, tan sólo dos años después, de lo que se habla es del estancamiento y debilitamiento que ha sufrido el metaverso en su inversión financiera y en su demanda por parte de los potenciales usuarios. Las dificultades técnicas actuales para reconstruir un mundo gemelo digital, el elevado coste de los dispositivos de realidad virtual impidiendo su acceso a un público más amplio, su falta de ergonomía suficiente, o los últimos escándalos acecidos en el mundo de las criptomonedas, han abocado al que se ha denominado el "invierno del metaverso"[5].

Al freno del metaverso totalmente virtual se añade el reciente lanzamiento de las gafas de Apple, denominadas *Vision Pro* que, en lugar de optar por un mundo completamente inmersivo, es decir exclusivamente basado en la realidad virtual, como las más populares de Meta[6], apuestan por la realidad mixta uniendo

---

[4] *Newzoo: Introduction to the Metaverse Report*. https://newzoo.com/insights/trend-reports/newzoointro-to-the-metaverse-report-2021-freeversion/

[5] Malaschini, A. (2023). "Metaverso e diritto: su alcune questioni giuridiche della realtà virtuale", *GiustAmm.it*, núm. 2, pp. 1-28.

[6] *Oculus Quest 2*. Sólo son de realidad mixta las "Meta Quest Pro" de alta gama orientado a profesionales y las Meta Quest 3 incorporando en 2023 ya la realidad mixta.

contenido digital con el espacio real físico[7]. La diferencia es que sirven para hacer lo mismo que haces con tu ordenador Mac o iPad, sin necesidad de concurrencia de usuarios, ni de evadirte del mundo físico, lo que, ya de por si resulta bastante menos peligroso para la integridad física. De momento lo que auguran es un mundo sin pantallas físicas, pero por ahora incurren en problemas semejantes a los del metaverso potenciado por Meta, en especial su elevado peso, la incomodidad de su uso prolongado y, sobre todo, su elevadísimo precio. La línea que apuesta por la realidad mixta frente a la únicamente virtual presenta, en todo caso, un menor compromiso financiero y menores problemas tecnológicos, lo que indica que el camino a transitar se mueve por el camino trazado por Apple y que tímidamente, incorporaba Meta en su último lanzamiento de gafas en octubre de 2023 (*Meta Quest 3*). Aunque como acertadamente se ha señalado, puede que en puridad al metaverso exclusivamente virtual le espere una nueva primavera pues, en sentido estricto, lo cierto es que la supuesta realidad mixta incorporada por Apple en la que se combina espacio físico real con virtual es ficticia ya que no hay una realidad aumentada, siendo también una realidad totalmente inmersiva ya que lo que se ve con *las Vision Pro* de Apple lo es a través de cámaras, en lugar de imágenes digitales superpuestas sobre una vista del mundo real[8].

En cualquier caso, tanto los metaversos de realidad virtual como los de realidad mixta plantean enormes retos jurídicos, muchos de ellos comunes para todas las ramas del Derecho. Aquí nos centraremos en algunos más transversales y, posteriormente, abordaremos algunos específicamente laborales.

2. RIESGOS TRANSVERSALES CON REPERCUSIÓN LABORAL

2.1. La gobernanza

Uno de los aspectos más relevantes cuando hablamos de metaversos es el de su gobernanza. Es decir, a quién pertenece. La configuración de los distintos tipos de metaversos presenta repercusiones específicas a la hora de abordar los

---

[7] Un excelente y predictivo artículo en Fairfield, J. A. T., "Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life" *Berkeley Technology Law Journal*, 2012, Vol. 27, núm. 1, pp. 55-116.

[8] McGee, P. (2023). "Hands on with Apple's Vision Pro: bringing the metaverse to life", *Financial Times*, June 6.

diversos problemas jurídicos que pueden aparecer en esta realidad inmersiva. En la actualidad los metaversos existentes pueden ser privados centralizados o privados descentralizados, con un sistema de gobernanza diferente.

Marginando aquí los metaversos públicos, por su actual irrelevancia[9], en los metaversos *centralizados privados* (como Facebook ahora Meta, Microsoft o Fortnite en juegos, por ejemplo) se entra tras consentir una serie de cláusulas apenas leídas, pero formalmente asumidas. Los términos de uso (TOUs) de los distintos metaversos imponen una ley privada aplicable y las personas usuarias aceptan todas las condiciones otorgando casi inmunidad al proveedor del metaverso. En esas condiciones de uso a las que el usuario prácticamente se adhiere, se regula la responsabilidad, la propiedad intelectual, los derechos sobre todo lo subido o creado, la responsabilidad de los menores, el legítimo interés sobre enormes cantidades de datos, incluidos los biométricos para la correcta ejecución del contrato de prestación del servicio del metaverso, la jurisdicción y los sistemas competentes de resolución extrajudicial de conflictos. Y cada plataforma de metaverso estipula sus propias condiciones de uso multiplicándose las leyes privadas. Unas condiciones que debieran ser claras, concisas, y comprensibles para poder otorgar un consentimiento informado, pero que se asumen sin más porque sin consentimiento no hay acceso.

Por su parte, los metaversos *privados descentralizados* (que típicamente pueden encontrarse en el mundo e-sport como *Decentraland*, *Sandbox*, *Axie Infinity* o *Webaverse*) se basan en cadenas de *blockchain* y la propiedad no recae en una corporación, sino en una distribución colectiva basada en las denominadas DAOs, Organizaciones Autónomas Descentralizadas[10]. Estas organizaciones permiten que todos los usuarios que participan con dinero virtual mediante la posesión de algún bien no fungible o token (NTFs) tomen decisiones a través de sus votos. Las reglas y los registros de las transacciones de una DAO se almacenan de forma transparente en la *blockchain* y las decisiones se inician por propuestas que deben

---

[9] De momento son pocos los metaversos públicos, y parece que se van creando para específicas finalidades, sobre todo turísticas. Sobre la necesidad de metaversos impulsados por las AAPP y las dudas de considerar creaciones autónomas digitales la reproducción de ciudades o museos sin revertir ganancias a las ciudades o museos reales. https://www.administracionpublica.com/un-metaverso-publico/

[10] Ercilla García, J. (2020). "Aproximación jurídica a las organizaciones autónomas descentralizadas", *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 52.

ser sometidas a un proceso de consulta, de modo que para cada decisión que se tome se debe obtener el voto de la mayoría de los tenedores de tokens o cumplir cualquier otra condición establecida en el protocolo de consenso de la organización. Con este sistema se "digitaliza la confianza" eliminándose los recelos que pudieran surgir entre los integrantes de la organización en tanto las reglas de funcionamiento y los escenarios a los que la DAO se puede enfrentar dentro de la misma están predefinidos[11]. Aunque el modelo DAO representa inicialmente una gobernanza asamblearia y más democrática, también revela inconvenientes porque existen muchas decisiones que hay que tomar de gestión diaria de la DAO[12] y su completa consulta resulta impracticable; asimismo, quienes poseen más tokens pueden inclinar la balanza de la decisión y además la ausencia de personalidad jurídica genera problemas de determinación de la responsabilidad –de hecho en EEUU ya se les está reconociendo como sociedades de responsabilidad limitada basadas en cadenas de *blockchain*[13].

La cuestión de la gobernanza y la naturaleza centralizada o descentralizada del metaverso tiene enormes consecuencias con reflejo en el ámbito laboral. Las relaciones en los metaversos privados centralizados introducen un intermediario en el trabajo realizado. Si mi empresa real me contrata para trabajar de modo presencial, desde el centro de trabajo, pero para ejecutar mi trabajo dentro del metaverso representando a la empresa en su sucursal virtual (terreno por el que mi empresa paga a la compañía propietaria del metaverso), ciertamente no se pierde la bilateralidad que caracteriza la relación laboral. Pero la realización del trabajo en el marco de un espacio que no pertenece a la empresa, regido por sus propias reglas privadas, consentidas por la empresa cuando compra la licencia o por la persona trabajadora para poder acceder a la plataforma del metaverso,

---

[11] Oulego, J. R., "DAO naturaleza e implicaciones jurídicas". https://adefinitivas.com/arbol-del-derecho/dao-naturaleza-e-implicaciones-juridicas-a-cargo-de-jose-ramon-oulego/

[12] Por ello *Decentraland* ha establecido una Fundación Decentraland sin fines de lucro que se encarga de la gestión diaria y ordinaria de su metaverso, lo que supone casi una distinción entre un poder legislativo generalizado, que interviene en cuestiones políticas importantes, y una estructura de gobierno ejecutiva para la operación diaria del negocio, afirmando algún autor que hay un espacio para un embrión de investigación sobre el "derecho público del "metaverso": Malaschini A., *cit*., pp. 27-28.

[13] *Blockchain-based LLC* (BBLLC): Weinstein G., Lofchie S. y Schwartz J. (2022), "A primer on DAOs", *Harvard Law School Forum on Corporate Governance*, posted on Saturday September 17.

pueden generar implicaciones no deseadas. La férrea intervención de un tercero ajeno que ejerce el control y vigilancia en tiempo real, que puede monitorizar y seguir el rastro de absolutamente todo lo que acaece dentro de su metaverso, se añade a la ya injerencia habitual que las normales tecnologías están poniendo de manifiesto en el marco de las relaciones laborales. El estándar de comportamiento, el juego y alcance de los derechos fundamentales se mueve en un doble marco contractual. El control del tiempo de trabajo, la posibilidad de que el registro lo gestione la plataforma del metaverso, los problemas de acoso a la persona trabajadora por parte de terceros usuarios virtuales imposibles de localizar para el empleador, los incumplimientos o comportamientos sancionables de la persona trabajadora respecto a otros usuarios, etc., constituyen cuestiones en las que se imbrican dudas y respuestas llevando con facilidad de la responsabilidad contractual a la extracontractual. Los problemas se plantean no solo para la persona trabajadora, doblemente observada y controlada, sino también para la parte empresarial que en muchos casos desconoce cómo actuar en el cumplimiento de su general deber de prevención y actuación diligente. Todas estas dudas se plantean igualmente si el trabajo se desarrolla para una empresa virtual por una persona trabajadora y el encuentro de la oferta y la demanda ha tenido lugar en el propio metaverso. Sobre todo, teniendo en cuenta que, a diferencia de otras realidades laborales, la que se genera en este espacio virtual constituye un espacio sin fronteras e ilimitado en tiempos y husos horarios. Básicamente porque para su resolución no se puede jugar siempre con los limitados parámetros nacionales que extrapolan conceptos, regulaciones y realidades propias a contextos ajenos en clara contradicción con las fronteras derivadas del Derecho internacional privado que van a determinar la jurisdicción y la ley aplicable. La complejidad de estas normas se agudiza en la necesidad de tener en cuenta la intervención de un tercero que puede verse involucrado en la responsabilidad civil o laboral. Ciertamente, los comportamientos de la persona trabajadora dentro del metaverso cuando suponen un mal uso del metaverso, en el sentido de contrariar los términos de uso, si han sido informados por parte del empleador a la persona trabajadora y terminan por generar una responsabilidad empresarial siendo la cuenta corporativa, podrán abocar a las generales reglas de responsabilidad civil (del tercero afectado frente a la empresa *ex* 1903 CC o del proveedor del metaverso frente a la empresa) y laboral (de la empresa frente al trabajador mediante el poder disciplinario y la repercusión posible de los daños patrimoniales). Por otro lado, el trabajador goza de todos los derechos laborales

en el marco del metaverso al representar a su empresa y es justamente en esta importante vertiente donde el respeto empresarial resulta complejo y difícilmente gobernable. Desde luego cualquier ataque, acoso, etc. que sufra la persona trabajadora dentro del metaverso, en la medida en que afecte a la persona real (y neurológicamente está demostrada la afectación directa en los mundos inmersivos[14]), debiera dar lugar a la protección jurídica del mundo real (IT, *ius resistentia*e, prevención de riesgos laborales, etc.). Pero hay otros derechos del trabajador difícilmente ejercitables en su plenitud al verse sometido a una *doble asimetría contractual* (la laboral y la de usuario de la plataforma frente al proveedor), como ocurre con la protección de datos, en tanto es el proveedor del metaverso quien recoge los datos del trabajador, no el empresario, lo que podrá hacer lícitamente desde que se aceptan los términos de uso mediante consentimiento informado, correspondiendo los principios de minimización, finalidad, conservación, derechos ARCO al proveedor que es quien actúa como responsable. Cuestión distinta sería la creación de un metaverso empresarial propio, elaborado específicamente por un determinado empleador para que se realice en él la actividad laboral o parte de esta (lo que es frecuente cuando su uso principal es la formación). En tal caso, el empleador será el responsable del tratamiento y el obligado al cumplimiento del art. 18.4 CE. Fuera de este supuesto, lo cierto es que los metaversos privados cerrados constituyen una "dictadura" de la empresa propietaria del metaverso, un tercero ajeno a la relación laboral, dejando en el ciberespacio la duda del cumplimiento efectivo de los derechos fundamentales del usuario. Pasar de una visión economicista de las plataformas a una centrada en el ejercicio de derechos fundamentales y libertades públicas de quienes las utilizan es un camino por andar, aunque los primeros pasos ya han comenzado de la mano de la UE. Además del deber de transparencia y prohibición de cláusulas abusivas[15] las plataformas de metaverso, como servicios de la sociedad de

---

[14] La neurociencia confirma la diferencia con las interfaces digitales hasta ahora conocidas. La realidad psicológica lleva a los usuarios de tecnologías inmersivas a responder fisiológicamente a las simulaciones virtuales de manera similar a su respuesta corporal a situaciones reales, creándose recuerdos igual que los que se crean en la vida real; la neurología confirma esta realidad: Brittan Heller, 6/12/2020, "Reimagining Reality: Human Rights and Immersive Technology", Harvard Kennedy School, *Carr Center Discussion Paper Series,* 2020, p. 9 con cita de Brown T. I. et altri *Prospective Representation of Navigational Goals in the Human Hippocampus*, Vol. 352 SCIENCE 1323 (2016).

[15] Como servicios de la sociedad de información, se someten a la Directiva 2000/31/CE, de 8 de junio, sobre comercio electrónico (modificada por la DSA) y traspuesta por la Ley 34/2002,

información, deben cumplir con dos importantes regulaciones: el Reglamento sobre mercados digitales (DMA D*igital Markets Act*) y el Reglamento de Servicios Digitales (DSA *Digital Services Act*).

El Reglamento de Servicios Digitales (DSA)[16] incrementa el deber de diligencia y transparencia de las plataformas lo que repercute en los términos y condiciones ofrecidos para acceder al metaverso, dando información sobre muchos aspectos, incluidas las decisiones algorítmicas y la revisión humana, debiendo establecer sistemas internos de reclamación sobre las decisiones adoptadas en relación con contenidos ilícitos o información incompatible con sus condiciones, colaboración con órganos certificados de resolución extrajudicial de conflictos para resolver cualquier diferencia con los usuarios de los servicios y otras cautelas, como la de proporcionar un sistema interno de tramitación de reclamaciones[17]. Se busca que lo que es ilegal en el mundo físico lo sea también en el mundo digital[18]. Por su parte el Reglamento de Mercados Digitales (DMA)[19] impone obligaciones a las plataformas denominadas *Gatekeepers* (guardianas de acceso) prohibiéndolas realizar actuaciones contrarias a sus competidoras o que les impidan acceder o permanecer en el metaverso y obligándolas a que las empresas usuarias accedan a los datos que generan al utilizar sus plataformas prohibiendo rastrear a los usuarios finales al margen del servicio de plataforma básica de los guardianes de acceso con fines de publicidad personalizada sin haber concedido un consentimiento efectivo. Como en la DSA, también

---

donde se prevé que en caso de atentar contra ciertos principios (entre ellos, la protección de los usuarios, la dignidad o la no discriminación) los órganos competentes podrán adoptar medidas para que se interrumpa la prestación o para retirar los datos que los vulneran.

[16] Reglamento UE 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales o DSA *Digital Services Act*).

[17] Su incumplimiento permite la apertura de un procedimiento de incumplimiento que puede abocar a elevadas sanciones. La comisión ha abierto un procedimiento formal por incumplimiento de la DSA contra *AliExpress* –designada plataforma en línea de muy gran tamaño *Very Large Online Platforms* (VLOP) el 25 de abril de 2023–.

[18] Raso Delgue, J. (2022). "Metaverso y Derecho del Trabajo", *Informática y Derecho. Revista Iberoamericana de Derecho Informático,* 2ª época, núm. 12, p. 139.

[19] Reglamento UE 2022/1925 del PE y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

la DMA contempla sanciones duras en caso de incumplimientos[20]. Con estos Reglamentos no sólo se logran derechos procesales accionables ante las plataformas privadas que operan en el ecosistema digital, sino que las autoridades de la UE y de los EM obtienen herramientas para supervisar el cumplimiento de la nueva regulación y la sociedad civil conquista vías específicas para hacer valer mejor sus derechos a escala[21].

Frente a los metaversos centralizados privados, se encuentran los metaversos con estructura descentralizada en los que la toma de decisiones está distribuida y no depende de una sola autoridad, pero cuyos retos se encuentran en el polo contrario a los expuestos del modelo centralizado: dificultad de coordinación y creación de consenso, escalabilidad y difícil identificación de las leyes aplicables y por la dificultad para atribuir responsabilidades. Frente a la gobernanza centralizada, la descentralizada no resuelve todos los problemas, sino que, en algún caso, puede incluso amplificarlos a la hora de determinar el juego y la influencia de un tercero en el correcto cumplimiento de la relación laboral. Aunque la productividad y cumplimiento de la relación laboral en el metaverso dentro de la empresa virtual del empleador en estos casos es perfectamente trazable, así como la realización de trabajos extra, también en estos metaversos concurren los retos suscitados por las tecnologías emergentes relativos a la privacidad, protección de datos, ejercicio de derechos fundamentales, protección de datos y ciberseguridad, ejercicio de derechos laborales, protección de colectivos vulnerables, etc. Y todas estas cuestiones se reclaman frente multitud de nódulos y en un contexto donde la democracia del voto en función de la propiedad de tokens permite a la mayoría determinar el concepto de lo ilegal y de lo aceptable. Además de la dificultad de determinar la norma aplicable, si esta logra acotarse la dificultad reside en la imputación de responsabilidades, por ejemplo, por vulneración de derechos debidos a un *bug* o error del sistema. Por ello los

---

[20] La Comisión abre investigación contra Alphabet, Apple y Meta por incumplimiento de la Ley de Mercados Digitales. A Meta por el ofrecimiento binario "paga o consentimiento" contrario al art. 5.2 DMA que exige que los guardianes obtengan el consentimiento de los usuarios cuando intentan combinar o utilizar de forma cruzada sus datos personales en diferentes servicios de plataformas principales porque la elección binaria impide una alternativa real en caso de que los usuarios no den su consentimiento, frustrando así el objetivo de impedir la acumulación de datos personales por parte de los guardianes.

[21] Como resume Barrio Andrés, M. (2023), "El metaverso y su impacto en el Estado y la soberanía", *Revista de Derecho Político,* UNED, núm. 117, mayo-agosto, pp. 197-220.

principales desafíos para los responsables de la formulación de políticas en este modelo incluyen el desarrollo de un sistema ágil de controles y equilibrios que distribuya el poder y la responsabilidad a través de una comunidad de usuarios y partes interesadas, así como el establecimiento de formas de hacer cumplir la ley y permitir la supervisión humana[22]. Las responsabilidades y criterios de comportamiento (ley privada del metaverso descentralizado) podrían incorporarse en la fase de elaboración de la DAO, restando democracia participativa (al ser *ex ante*), pero permitiendo que solo quienes convergen éticamente, por ejemplo, respecto al trabajo decente, puedan incorporarse al protocolo. Las dificultades de la gobernanza en estos casos han llevado a algunos países a regular las DAOs como corporaciones, precisamente, para otorgarles personalidad jurídica, responsabilidad y fiscalidad[23].

Por todo lo expuesto, comienza a extenderse la idea de una *estructura híbrida* que combine elementos descentralizados y centralizados como el enfoque más realista para la gobernanza de los mundos virtuales. Ambos modelos en sus versiones perfectas tienen fortalezas y debilidades y la combinación de ellos podría ser utilizada estratégicamente, dependiendo del contexto y las necesidades. Así, el empoderamiento de los usuarios, la identidad digital y los futuros derechos digitales podrían beneficiarse enormemente de una arquitectura generalmente descentralizada, pero aspectos como la aplicación de la ley o las políticas específicas, pueden abordarse de manera más eficaz a través de las estructuras centralizadas[24]. Siendo poco probable que exista un único y uniforme estilo de gobernanza para los mundos virtuales a escala global, lo normal es que los gobiernos, a escala nacional, regional o internacional, terminen por establecer marcos de gobierno que reflejen el mundo real y adapten las actuales normativas a las particularidades del virtual. La interoperabilidad, o no, de los sistemas permitirá un ámbito mayor de gobernanza y alianzas estratégicas entre metaversos. Lograr, al menos en la Unión Europea, que cualquiera que sea la estructura desarrollada

---

[22] https://publications.jrc.ec.europa.eu/repository/handle/JRC133757

[23] Muy interesante sobre las posibilidades regulatorias de las DAOs. https://www.derechoyfinanzas.org/naturaleza-juridica-de-las-organizaciones-autonomas-descentralizadas-daos-segunda-parte/

[24] Como pone de manifiesto el informe AA. VV. (2023), *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU*, Publications Office of the EU, Luxembourg.

se permita el ejercicio de los derechos del mundo real, su coercibilidad y ejecutividad, es el reto más inmediato lo que obliga a la adaptación paulatina de las actuales normas a un mundo en constante movimiento y desarrollo. Esos pasos de la UE, aunque paulatinos, se van dando como lo demuestra no sólo la aprobación del paquete digital DMA y DSA, sino la aprobación reciente del Reglamento de Inteligencia Artificial[25] (RIA) o la Directiva para la mejora de las condiciones laborales en plataformas digitales, así como la aprobación el 18 de enero de 2023 por el Parlamento Europeo de un informe para proteger a los jugadores de videojuegos donde, entre otras cuestiones, se advierte sobre el "gold-farming" (producción de oro) como sistema con el que los jugadores que adquieren monedas en el juego pueden venderlas luego por dinero en el mundo real y que deben controlar si fomentan el trabajo forzoso y la explotación infantil en los países en desarrollo.

2.2. La identidad digital

Otro de los problemas relevantes que plantea el metaverso es el de la identidad digital[26]. La potencialidad del metaverso consiste, entre otras cosas, en la posibilidad infinita de ser quien y como quieras ser (animal, cosa, sexo, orientación, etc.). Ello, en principio, puede eliminar muchos de los problemas derivados de las discriminaciones en todos los ámbitos y resultar más igualatorio que el mundo real. Pero la ductilidad que ofrecen los metaversos para proyectarse como avatar genera relevantes interrogantes laborales en tanto, a fecha de hoy, basta para ser usuario de uno de estos espacios virtuales actuales con una cuenta de correo, que puede ser inventada y que, a lo sumo, requiere de un móvil para cotejar una existencia medianamente real. Las complejas implicaciones que la ductilidad del avatar presenta sobre la identidad digital se manifiestan en todos los ámbitos, pero en el laboral se potencian al constituir la relación laboral una prestación esencialmente *intuitu personae* en el que las titulaciones, competencias y aptitudes personales y profesionales de la persona determinan el encuadramiento profesional y, con ello, las funciones, obligaciones, derechos y, sobre todo, la retribución.

---

[25] P9_TA(2024)0138 Reglamento de Inteligencia Artificial Resolución legislativa del PE de 13-3-2024.

[26] Sobre esta materia puede verse el profundo estudio de Llaneza González, P. (2021), *Identidad Digital*, Bosch-Wolter Kluwer.

La empresa que contrata directamente dentro del metaverso a un avatar, detrás del cual hay una persona, necesita saber exactamente a quien contrata a efectos, por ejemplo, de acciones positivas, compromisos convencionales en selección de determinados colectivos, o el cumplimiento de obligaciones legales en materia de igualdad por razón de sexo. Asimismo, en muchos casos existen incentivos a la contratación de colectivos vulnerables que requieren el conocimiento de la identidad real de la persona contratada. En la vida real se podría saber si la empresa está cumpliendo sus obligaciones, lo que tiene efectos legales (ausencia de sanciones) y reputacionales (en caso de cumplimiento de códigos de conducta o RSC). Pero resulta que las personas candidatas al empleo dentro de un metaverso pueden conocer dichas normas y desarrollar una caracterización estratégica para conseguir el empleo manifestándose en el avatar de conformidad con los requerimientos empresariales objetivos. Solo cuando se realice el contrato final podrá saberse, si acaso –porque la posibilidad de suplantación no puede descartarse–, si se cumplen los requisitos (en tanto tendrán que realizarse actos concretos para la formalización del contrato y la cobertura social de la persona trabajadora).

En definitiva, en el ámbito del metaverso no cabe duda de que resultará de especial relevancia la construcción de una "identidad digital persistente"[27] para poder certificar que el avatar posee activos únicos y personalizados (vehículos, coches, casas, vestidos, arte) pero, sobre todo, que permita que los usuarios puedan operar en cualquier plataforma (*Self Sovereign Identity* SSI), con independencia del uso de múltiples avatares y que cumplen los requisitos para el desempeño de ciertas profesiones cualificadas o reguladas. En el ámbito europeo existen ya propuestas regulatorias, como la reciente resolución legislativa del Parlamento Europeo, de 29 de febrero de 2024, sobre la propuesta de modificación del Reglamento (UE) núm. 910/2014, para el establecimiento del marco europeo de identidad digital[28], por la que las partes usuarias deben facilitar la

---

[27] NEWZOO, *Introduction to the Metaverse Report*., *cit.,* pp. 15-17.

[28] El 3 de junio de 2021 se hizo pública la Propuesta de modificación del Reglamento (UE) núm. 910/2014 para establecer un marco para la Identidad Digital Europea (COM(2021) 281 final), que dota de validez jurídica plena a la identidad digital autosoberana (SSI) y a los libros mayores electrónicos, incluyendo aquellos basados en Blockchain (eIDAS). El texto aprobado en el Parlamento Europeo en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_ES.html#title1

información necesaria para permitir su identificación y autenticación en línea sin tener que recurrir a los proveedores de servicios. De este modo, "nuestro avatar en el metaverso podría identificarse a través de un *wallet* de identidad y permitir a su contraparte comprobar, por ejemplo, que es mayor de edad o que dispone de permiso de conducir" permitiendo, a la vez, al individuo un "mejor control de sus datos personales y el uso de los mismos (incluso de forma anónima)", facilitando el desarrollo de la economía del dato pero permitiendo, al mismo tiempo, la libertad individual y, sobre todo, habilitando la posibilidad de vincular nuestra actividad en el metaverso con las estructuras tradicionales de administración de justicia en caso de conflicto[29]. Pero, incluso, con todas las seguridades ofrecidas por el futuro nuevo sistema que se prevé que entre en vigor en el año 2025, lo cierto es que la erradicación total de la suplantación de la personalidad no puede asegurarse, como tampoco es posible erradicarla en el mundo real. Pero ni los metaversos descentralizados basados en el *blockchain* impedirán la exigencia de responsabilidad por actos derivados de la suplantación de personalidad dentro del metaverso si alguien distinto al titular logra usar su cuenta y sus credenciales. Así, un trabajador podría dejar su avatar a otra persona para que realizara las funciones encargadas (a modo de subcontratación, o por vínculos de amistad, haciéndole un favor al titular del avatar, por ejemplo). Ello mismo ocurriría en la vida real cuando el trabajo se hace por remoto, salvo que estuviera controlado por un dato biométrico no reproducible o, al menos, de menor posibilidad fungible. En ambos casos, mundo real y mundo virtual, la cuestión residirá en demostrar la suplantación a fin de determinar eventuales responsabilidades respecto del empleado y deberían poder activarse mecanismos parecidos a los del mundo real (denuncia, anulación, renovación). En este sentido, la protección de los ciudadanos europeos "frente al uso no autorizado o fraudulento" de las carteras digitales se prevé de modo específico en la futura Identidad digital europea (art. 10.bis). En cualquier caso, los interrogantes no se cierran al limitarse los *wallets* de identidad al ámbito europeo.

---

[29] Mata Muñoz, A. (2022). "Metaversos: *blockchain* y seguridad jurídica", *Diario La Ley sección ciberderecho*, núm. 60, de abril, Wolters Kluwer, versión digital.

2.3. La protección de datos

En el mundo digital si no pagas por un producto o servicio, entonces no eres el cliente, sino que tú eres el producto. La célebre frase atribuida a un profesor de Harvard (Andrew Lewis), no puede ser más cierta cuando se habla del metaverso. Las redes sociales y las plataformas son el mejor ejemplo, perfilando a los usuarios para mostrarles anuncios sorprendentemente precisos. Estas capacidades predictivas se desarrollan exponencialmente en el metaverso donde el uso de la IA es imprescindible y el hambre de datos es constante para lograr experiencias más personalizadas y realistas. A diferencia de lo hasta ahora conocido, el metaverso accede a infinidad de datos biométricos únicos e irremplazables de cada sujeto. Se recogen a través de *wereables* o interfaces neuronales y se extrae información sobre las variaciones del iris y cambios posturales, permitiendo analizar la respuesta emocional y emplear con gran precisión novedosas técnicas de neuromarketing[30], o usar para la manipulación o extorsión del consumidor sobre el plano comercial, político o personal. Todos esos datos trascienden más allá de la UE y además de afectar a la persona trabajadora en el metaverso, también pueden afectar a la persona empleadora, revelando en el metaverso sus intereses comerciales, las conversaciones privadas o los secretos comerciales. Injerencias y riesgos que ya actualmente son reales, pero que en el metaverso alcanzan una palpable y nueva dimensión. En el marco de un sistema de gobernanza centralizado el poder del metaverso se incrementa alimentado de suculentos datos que constantemente le permiten gobernar y chantajear para hacer callar. En los sistemas descentralizados, aunque el poder se diluye, si los datos no están suficientemente protegidos, se distribuyen en múltiples ordenadores y bloques, permitiendo una mayor difusión en caso de fuga cibernética o quiebra de seguridad.

Hablar de perfilados sin consentimiento ni información, de datos extraídos e inducidos, de datos exportados más allá de la UE y usados para finalidades que sobrepasan las inicialmente previstas y advertidas o el manejo de datos biométricos a un nivel de nano precisión nunca visto, plantea intensas contradicciones con el Reglamento europeo de Protección de Datos (RGPD)[31]. En la protección

---

[30] AEPD, "Metaverso y privacidad", 19-9-2022.

[31] Reglamento (UE) núm. 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos - RGPD).

de datos la cuestión neurálgica reside en si la cesión de todos esos datos y su tratamiento encuentran un fundamento de legitimidad en el consentimiento que el usuario otorga al acceder al metaverso y si expresa una voluntad libre, específica, informada, e inequívoca como base legitima (o si es necesario el acceso para el desempeño de un contrato como el de trabajo). En el marco de una relación asimétrica y de adhesión debiera hacerse un esfuerzo legislativo mayor para clarificar el consentimiento al acceder a las plataformas digitales con clara asimetría informativa[32]. Como plataformas digitales con capacidad de inferencia y de obtención de información de salida (recomendaciones, predicciones, decisiones que pueden influir en entornos físicos y virtuales) deben ser consideradas sistemas de IA de alto riesgo (art. 6 RIA) ya que pueden tener un efecto perjudicial importante en la salud, la seguridad y los derechos fundamentales de las personas de la Unión –cuando no en algún supuesto directamente de sistemas de IA prohibidos[33]–. Tal calificación lleva consigo garantías como la transparencia y explicabilidad algorítmica, el principio de gobernanza de los datos y lucha contra los sesgos, la obligación de protección desde el diseño y por defecto, la solidez técnica, auditorías algorítmicas y el principio de humano al mando[34]. Ambas normas (RGPD y RIA), con independencia de que enmarcan el derecho a la información en el derecho del consumo lo que impide suponer que se cierra la brecha del conocimiento y la asimetría informativa, al menos, ofrecen un marco normativo cuando los usuarios residen en la Unión Europea, dado su carácter "extraterritorial", en el sentido de que exigen su cumplimiento a todas las entidades que, con independencia de su ubicación o nacionalidad, lleven a cabo actividades empresariales en la UE con acceso y tratamiento de datos personales de ciudadanos de la UE (art. 3 RGPD, art. 2.1 RIA). El carácter multinacional del metaverso hará, no obstante, difícil aplicarlas a personas y trabajadores ubicados en otras latitudes y que desempeñan su actividad fuera de su ámbito de

---

[32] Nogueira Guastavino, M. y Mangan, D., "The metaverse matrix of labour law", *Italian Labour Law e-journal*, Vol. 16, núm. 1, pp. 13-277.

[33] Si se detectan prácticas que tienen gran potencial para manipular a las personas mediante técnicas subliminales que trascienden su conciencia o aprovechan las vulnerabilidades de grupos como menores o personas con discapacidad para alterar su comportamiento de un modo que resulte probable que les provoque perjuicios físicos o psicológico (art. 5).

[34] Estos principios y su alcance laboral *vid.* Mercader Uguina, J. R. (2024), "El Reglamento de inteligencia artificial entra en la recta final: una primera lectura en clave laboral", *Iustel*, *RGDTSS*, núm. 67, pp. 328 y ss.

aplicación. De ahí que las empresas que utilicen el metaverso deberán cumplir con normativas de múltiples jurisdicciones.

A los problemas de los datos se añade el de la obligación de dotarlos de sistemas seguros y evitar fugas. En el metaverso la cuantía de datos se multiplica exponencialmente con el correlativo incremento de las amenazas de seguridad al concurrir más usuarios y ciberdelincuentes[35]. Corresponde al responsable de la base de datos la obligación de adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personas, evitando su adulteración, su pérdida, la consulta no autorizada, detectar desviaciones de información ya sean automáticas o por causa humana. La cuestión reside en la adjudicación de roles de responsable (que es quien dispone los medios y decide la finalidad del tratamiento) o encargado (quienes brindan el servicio de tratamiento de datos personales por cuenta del responsable) y en la transferencia de datos más allá de la UE. Todo ello además se complica en caso de metaversos gestionados por DAOs donde es difícil distinguir entre una gobernanza y una estructura asamblearia impidiendo la identificación de la persona a la que atribuir la responsabilidad en caso de violación de la protección de datos[36].

El deber empresarial de evitar una vigilancia invasiva se topa de frente con espacios multiversianos. El uso del metaverso ofrece la revelación de datos biométricos del trabajador más allá de los generales para el control razonable y proporcionado de su actividad pudiendo anticipar enfermedades y la evolución de su salud. El ejercicio del poder de dirección y control del empleador, sometido a condicionantes europeos y nacionales cuando se trata de tratamiento de datos especialmente protegidos como los biométricos (que deben ser usados de modo excepcional y sólo con consentimiento, minimización y respetando estrictamente el consentimiento informado y el test de proporcionalidad) rebasa el ámbito de la relación laboral al ingresarse en un mundo virtual inmersivo en el que un tercer ojo panóptico vigila el ojo de tu empresa al mismo tiempo que el de sus trabajadores. El empresario laboral, hasta ahora considerada la gran empresa panóptica, cual gran hermano, pasa a ser también sometida y conducida por el nuevo "ojo del metaverso".

---

[35] Pietro, R. y Cresci, S. (2021). "Metaverse: Security and Privacy Issues", *Researchgate*.

[36] Como advierte Malaschini, A., *cit*. pp. 1-28.

3. EL META-DERECHO INDIVIDUAL DEL TRABAJO

3.1. Ley aplicable, mercado de trabajo y selección de personal

Las posibilidades de trabajar en un metaverso son variadas. Pueden ser relaciones laborales absolutamente presenciales en un centro de trabajo donde el objeto del contrato de trabajo sea el de prestar el servicio dentro del metaverso. Pero dicha prestación puede también realizarse desde otro lugar fuera de la empresa, a modo de teletrabajo nacional, trasnacional o internacional, ya sea contratado presencialmente, electrónicamente fuera del metaverso o, incluso, virtualmente dentro del metaverso. Asimismo, en cualquiera de estos supuestos se puede desplazar temporalmente a la persona trabajadora dentro de la UE o fuera de ella. La realización e, incluso, la contratación resulta global, como global es cualquiera de los metaversos existentes. De ahí que uno de los problemas nucleares para establecer las condiciones de trabajo venga determinado por la previa delimitación de la legislación aplicable. En la medida en que esta cuestión ya la he analizado profusamente en otro artículo[37], de momento y mientras no se adopten normas específicas tendentes a evitar el *dumping* social, baste señalar que habrá que estar a las normas de conflicto laboral reguladas en el reglamento conocido como Roma I, para las obligaciones contractuales (Reglamento 593/2008) aplicable al contrato individual de trabajo[38] y que coincidirá con la del lugar de ejecución habitual del trabajo, entendida por tal el lugar en el que se ponen las gafas y reside físicamente la persona que maneja el avatar.

El examen de algunos de las cuestiones laborales que pueden surgir en el metaverso se aborda a partir de ahora sobre la base de que el *metaworker* fuera contratado en el metaverso y el trabajo con el equipo inmersivo se llevara a cabo habitualmente en España, con independencia de donde estuviera ubicado el empleador. Comenzando por el *meta mercado de trabajo*, no cabe duda de que los metaversos ya están generando empleo. Este empleo puede crearse y ser "exógeno" o "endógeno" al propio metaverso. Exógeno será, por un lado, el empleo que crea todo metaverso y plataforma para su diseño, mantenimiento, actualización y correcto funcionamiento (programadores de realidades extendidas,

---

[37] Nogueira Guastavino, M. (2022). "Metaverso y legislación aplicable al contrato de trabajo", *RTSS. CEF,* núm. 71, pp. 17-53.

[38] Para las obligaciones extracontractuales (relevante en materia de conflictos colectivos o huelgas que ocasionen daños) se estará al Reglamento Roma II (Reglamento 863/2007).

modeladores de entornos virtuales, ingenieros de software y de computación gráfica y animadores, entre otros muchos, que poco a poco construirán este nuevo mundo para lograr que sea una parte cotidiana de nuestras vías)[39]. Asimismo, el metaverso genera un empleo indirecto exógeno por la necesidad de profesionales dedicados a la formación de trabajadores desempleados o que estén ocupados y necesiten cursos de reciclaje digital específicamente conectados con el metaverso. Finalmente, en la medida en que el metaverso persigue construir un mundo gemelar y es posible una interacción entre el mundo digital y el real puede augurarse el incremento de empleos en profesiones reales no vinculadas con la tecnología, pero cuyas tareas se vean incrementadas cuando la empresa resulta exitosa en sede virtual. Si una nueva empresa se crea en el metaverso y se pone de moda, lo predecible es que necesite más trabajadores, vendedores, diseñadores, contables, gestores, transportistas, etc., cuando, además del mundo virtual, sus servicios se hagan efectivos también en el mundo real. Si compro una hamburguesa en el metaverso, puedo quererla también en el mundo real y me llegará a casa gracias a un repartidor y al personal de cocina que la ha elaborado en una empresa real.

Dentro ya del metaverso la cuestión es si en su seno se puede crear empleo, qué empleo y cómo funciona. Y es en este punto donde, frente a las oportunidades internas que ofrece este nuevo mercado, se detectan unos mayores riesgos de precariedad y dumping social. De un lado, el metaverso funciona con avatares. En principio y dejando fuera los chatbots, detrás de cada avatar hay una persona y si se trata de un mundo gemelo digital, hace falta trabajadores prestando sus servicios, aunque sea a través de un avatar (*metaworker*). Se necesitarán trabajadores reales para cubrir esas posibilidades infinitas de monetización que ofrece el nuevo mundo virtual como personal de bienvenida, personal de márquetin, proveedores, reponedores de nuevos NTFs, vendedores, etc., de tratarse de tiendas y comercios. Pero también se necesitarán arquitectos, abogados, psicólogos, médicos, personal de enfermería, payasos, artistas de todo tipo, representantes de comercio, paisajistas, expertos en decoración, clérigos de las distintas religiones y otras nuevas virtuales y así, hasta el infinito y más allá. Sus avatares prestarán sus servicios dentro del mundo virtual (cobrando por ello

[39] Meneses, N. (2021). "El metaverso: nuevas oportunidades laborales y retos en el futuro de las redes sociales", *El País,* Madrid, 25 de noviembre.

como en el mundo real) de modo exclusivo, de forma mixta o sólo como inicial mecanismo de contacto profesional para desarrollar la actividad de que se trate fuera del metaverso. En el metaverso de *Second Life* ya hay estudios que ponen de manifiesto la importancia de estos nuevos mercados virtuales como mecanismo para la captación de clientes en el mundo real, por ejemplo, con Despachos de abogados[40]; o, con gran éxito, para atender servicios de telemedicina[41] creando un entorno virtual de consultas en el metaverso igual que se hace ya de modo generalizado mediante aplicaciones en el móvil.

De momento perspectivas de empleo existen. En un futuro no muy lejano, no obstante, serán posibles dentro del metaverso (e, incluso fuera) empresas de "gestión automatizada" o IA Business que no usan personas físicas, sino exclusivamente *roboworkers* sintéticos o no biológicos, avatares automatizados, que gestionen íntegramente los bienes o servicios ofrecidos por la empresa a los clientes sin necesidad de intervención humana. Con ellas la creación de empleo es cero, siempre y cuando, además, no destruyan el existente. En tales casos se ha propuesto que este tipo de empresas se vea sometida a una obligación de retorno social por el no uso de trabajadores biológicos[42].

Al margen de este extremo aún lejano, lo cierto es que la creación de empleo dentro del metaverso conecta con espinosas cuestiones como la regulación del trabajo de menores ante la incerteza de la identidad digital; la propia selección de personal en tanto el trabajo asalariado es *intuitu personae* con carácter general y en la época de pandemia y teletrabajo ya se detectaron fraudes en la contratación por parte de empleadores y/o de trabajadores que suplantaron su personalidad; posibilidad que se multiplica en un mundo de avatares imaginarios:¿con quién estoy contratando en el metaverso? ¿cómo saber si puedo recibir ayudas por la contratación? A estas preguntas responderá la identidad digital soberana en un inmediato futuro, ofreciendo los datos reales estrictamente necesarios para ajustar el mundo virtual al real. Junto a ello el reclutamiento tecnológico,

---

[40] *Vid*. Biurrun Abad, F. (2021). ¿Abrirías tu despacho en el netaverso?, *Actualidad Jurídica Aranzadi*, 22 de diciembre.

[41] Galindo Martes, E. (2022). "Las consultas médicas llegan al metaverso", *TICPymes*, 31-1-2022.

[42] Nisa Avila, J. A. (2022). "El Derecho del Trabajo Digital en el metaverso", *Francis Lefebvre*, 19-09-2022.

asistido con algoritmos que proporciona inicialmente una selección objetiva e imparcial plantea riesgos de sesgos de distinta base bien conocidos.

En la contratación llevada a cabo dentro del metaverso deben diferenciarse distintos supuestos pues el trabajo podría contratarse a través de intermediarios (una ETT virtual que actúa dentro del metaverso, contrata meta-trabajadores dentro del metaverso y los cede a empresas usuarias para realizar trabajos dentro del metaverso), o directamente con mano de obra autónoma (avatares por cuenta propia), o con trabajadores por cuenta ajena, incluso, a través de los servicios virtuales públicos de empleo.

Cuando de contratación directa de mano de obra se trata, surge el problema de quién es el empleador. La peculiaridad del metaverso es que la inmersión completa o híbrida se realiza a través de una plataforma concreta pero el contrato de trabajo se celebra dentro de ella entre avatares trabajadores y avatares representantes de una empresa ubicada en un concreto *land* en el que reproducen la empresa real o donde constituyen una nueva. Las plataformas de entrada (Meta, Apple) son consideradas *gatekeepers* en el sentido de guardianes de acceso sometidos a la DSA y en el ámbito laboral lo normal es que sean exclusivamente intermediarias. Por ello, salvo que la propia plataforma guardiana de acceso tenga una empresa o representante virtual que contrate avatares *metaworkers*, la relación laboral surgirá entre empresas "alojadas" en el metaverso y las personas (avatares) allí reclutadas virtualmente. A estas empresas virtuales del metaverso habría que aplicarles la recién aprobada Directiva para la mejora de las condiciones laborales en plataformas digitales de trabajo[43] cuando utilicen sistemas automatizados de supervisión o de toma de decisiones para organizar el trabajo realizado por personas físicas a petición del destinatario del servicio prestado por la plataforma (art. 2.1) con independencia de que se trate de una plataforma de reparto, o de cualquier otro tipo, y del lugar donde se encuentre establecida la plataforma digital o donde se preste el servicio al destinatario ya que esta Directiva proyecta sus ambiciosos objetivos a toda plataforma digital de trabajo cualquiera que sea el sector de actividad y el elemento decisivo para su aplicabilidad territorial es el lugar donde se realiza el trabajo en plataformas (art 1.3). Por el

[43] Aprobada el 11 de marzo de 2024 pero de momento no ha sido publicada en el DOUE. El texto aprobado puede verse https://data.consilium.europa.eu/doc/document/ST-7212-2024-ADD-1/es/pdf

contrario, si la empresa en el metaverso no organiza el trabajo, sino que se limita a proporcionar los medios a través de los cuales los proveedores de servicios pueden llegar al usuario final sin más participación en la plataforma, por ejemplo mediante la publicación de ofertas o solicitudes de servicios, o mediante la agregación y presentación de información sobre los proveedores de servicios disponibles en un ámbito específico, no deben considerarse plataformas digitales de trabajo (Considerando 21). En el metaverso pueden concurrir ambos supuestos, incluso empresas que organicen el trabajo de las personas, pero sin sistemas automatizados, a los que no será tampoco aplicable esta Directiva. Pero lo normal es que las empresas que deciden introducirse en el mercado virtual utilicen sistemas automatizados de toma de decisiones y de organización autónoma y predictiva del trabajo y que el trabajo se desarrolle a distancia por medios electrónicos (ordenador y aplicaciones incorporadas en las gafas virtuales), debiendo, en tal caso, cumplir una serie de obligaciones que deberían modificar la actual realidad inmersiva. Entre ellas, la obligación de consulta con los representantes de los trabajadores (¿los de la empresa real o los elegidos en el mundo virtual?, entendemos que los primeros pues debiera ser un cumplimiento *ex ante* a la contratación de *metaworkers* en el metaverso), la prohibición de tratamiento de algunos datos personales[44] o una serie de obligaciones de transparencia respecto al uso del algoritmo debiendo informar sobre una larga lista de aspectos a la persona trabajadora, pero también a sus representantes (art. 9). Se reconoce también expresamente el derecho de supervisión o de revisión humana de las decisiones automatizadas (arts. 10 y 11). Cómo proceder al cumplimiento de todas estas obligaciones por parte del empleador inmersivo supondrá, en muchos casos, la colaboración de las plataformas de acceso que sirven de intermediario y ofrecen el entorno de trabajo.

En fin, además de que el metaverso desdibujará la frontera entre el trabajo por cuenta ajena y el trabajo por cuenta propia y obligará a la adaptación de los

---

[44] Como el estado emocional o psicológico de la persona que realiza trabajos en la plataforma, los relacionados con conversaciones privadas, o los datos personales de la persona trabajadora mientras no ofrezca su servicio en esa plataforma; o el uso de datos que infieran origen, raza, afiliación, religión, sindicación, salud; o el tratamiento de datos biométricos para establecer su identidad mediante el cotejo de sus datos con los datos biométricos de personas físicas almacenados en una base de datos (art. 7).

conceptos tradicionales de trabajador y de empresario en el mundo digital[45] –lo que ya parece incorporar la Directiva de plataformas digitales de trabajo al menos en relación con las garantías de la gestión algorítmica–, la selección de personal en los mundos virtuales permitirá igualmente que se lleven a cabo entrevistas inmersivas y una selección más objetiva e inclusiva mientras los avatares permitan una proyección no necesariamente real de la persona que los maneja.

Realizada la contratación inmersiva –normalmente a través de un s*mart contract*– entre dos avatares (por ejemplo, entre el avatar de una empresa francesa y un *metaworker* que desarrolla su trabajo habitual en España), además de la información exigida por la Directiva de plataformas digitales de trabajo, el empleador deberá informar de los elementos esenciales del contrato en virtud de la Directiva (UE) 2019/1152, del Parlamento Europeo y del Consejo, relativa a unas condiciones laborales transparentes y previsibles en la Unión Europea, entre las que será especialmente relevante el de la legislación aplicable, el lugar (virtual y físico) de prestación del trabajo[46] y la fijación de las condiciones que necesariamente deben permitir que su trabajo sea "previsible"[47]. Esta Directiva, ofrece interesantes refuerzos informativos para las personas trabajadoras en un entorno muy propicio para variadas tareas "a demanda" o con "patrón imprevisible[48], además de la prohibición de que los empleadores virtuales prohíban a los/las avatares aceptar un empleo paralelo salvo causas objetivas como la salud y seguridad (por ejemplo, por sobreexposición a campos magnéticos o aspectos relacionados con salud en el metaverso) o por causas empresariales como la protección de la confidencialidad empresarial o la prevención de conflictos de intereses, entre ellos, la competencia desleal (art. 9).

---

[45] Sobre esta cuestión resulta muy interesante el estudio de Pérez Prado, D. (2023), "Los tradicionales conceptos de trabajador y empresario en un mundo digital", AA. VV., Mercader y Puebla (dirs.), *Cambio tecnológico y transformación de las fuentes laborales,* Tirant lo Blanch, pp. 91 y ss.

[46] Biasi, M. (2023). "Il decent work e la dimensione virtuale: spunti di rifessione sulla regulazione del lavoro nel metaverso", *Lavoro Diritti Europa*, núm. 1, pp. 1-12.

[47] En la materia, imprescindible, Miranda Boto, J. M. (2023). *Condiciones de trabajo transparentes y previsibles: desafíos para el Derecho español en la trasposición de la Directiva (UE) 2019/1152*, Tirant lo Blanch.

[48] Como la cantidad de horas pagadas garantizadas y la remuneración del trabajo realizado fuera de las horas garantizadas, las horas y los días de referencia en los cuales se puede exigir al trabajador que trabaje, el período mínimo de preaviso a que tiene derecho el trabajador antes del comienzo de la tarea y, en su caso, el plazo de preaviso en caso de cancelación indemnizada de la tarea previamente asignada (art. 4.2.m).

Por otro lado, el contrato de trabajo celebrado y desplegado en el metaverso constituye un trabajo a distancia[49], si la ley aplicable es la española deberá tenerse en cuenta la Ley 10/2021, de 9 de junio, de trabajo a distancia (LTAD) cuando se trata de trabajo a distancia regular. Entre cuyas exigencias, como es sabido, destaca la obligación empresarial de dotar y mantener los medios equipos y herramientas necesarios para la experiencia inmersiva y de hacerlos accesibles en caso de resultar necesario por la discapacidad de la persona trabajadora, debiendo atenderse además técnicamente al trabajador (art. 11), así como el derecho del *metaworker* a la compensación de gastos generados por los equipos y herramientas y medios vinculados al desarrollo de la prestación (en los términos previstos en el acuerdo de trabajo a distancia, convenio o cuerdo colectivo de aplicación[50]) lo que, en el caso del metaverso deberá tener en cuenta no sólo el hardware, sino el software y el equipamiento adicional requerido dentro del metaverso. Obligación de medios de especial relevancia para supuestos de "tele existencia" en los que la persona trabajadora realiza un trabajo totalmente desarrollado en el mundo físico real pero desde su casa a través de unas gafas virtuales y unos mandos que se conectan con un gemelo robot en el lugar físico de trabajo y cuyas tareas, funciones y movimientos, reproducirán en tiempo real las que desarrolle el trabajador en su propia casa, como muestra la publicidad de la empresa japonesa Telexistence Inc.

3.2. Formación con y para el metaverso y riesgos laborales

La formación "en" el metaverso exige la previa formación "para" el metaverso y la evaluación de riesgos que tal formación lleva consigo. El uso de las gafas y el hardware y software necesario hoy en día para manejarse en el metaverso no es sencillo. Pero es el uso del metaverso para recrear situaciones reales 100% seguras y ausentes de los riesgos inherentes al mundo real donde el metaverso está mostrando su crecimiento más exponencial[51]. En su seno se permite un entrenamiento

---

[49] Se ha afirmado que el metaverso es una versión avanzada del teletrabajo (Sagardoy De Simón, I. (2022), "El metaverso y los derechos laborales", *El confidencial,* 22-2-2022; Cavas Martínez, F. (2023), "Relaciones laborales en el metaverso", *Revista justicia y trabajo*, núm. 3, p. 59). Pero ello no siempre es así ya que puede realizarse presencialmente en un centro físico de la empresa.

[50] STS Social núm. 179/2023, de 8 de marzo, rec. 277/2021 confirmando la SAN, núm. 132/2021.

[51] La obligación de formar a las personas trabajadoras en materia preventiva (art. 19 LPRL) permite que la formación sea virtual práctica a distancia como complemento a la formación

preventivo y progresivo con una evaluación y control el trabajador por parte de sus supervisores en tiempo real, con posibilidad de obtener informes objetivos de la evolución de los trabajadores. Pero, sobre todo, la formación se realiza de modo gamificado, sin riesgos de daños para el trabajador, con la consiguiente reducción de accidentes, de costes de desplazamientos y la minimización de tasas de abandono, ofreciendo a los empleadores una más eficiente organización de las agendas para los cursos formativos, pues se puede diseñar un único curso válido para todos los trabajadores o varias sesiones sincrónicas o diacrónicas.

La formación inmersiva puede servir, incluso, para formarse específicamente en los propios riesgos laborales que el uso del metaverso puede llevar consigo (lo que sería muy útil en relación con la protección de datos o los sistemas IA). Unos riesgos para la salud con sesgo de género por el demostrado mayor nivel de ciberviolencia y ciberacoso sufrido[52], sino porque el diseño y tamaño de los dispositivos está pensado para usuarios masculinos potenciales[53]. En todo caso, junto a los riesgos físicos derivados de no disponer de espacios adecuados para manejarse con libertad en el metaverso, el sometimiento a campos electromagnéticos, la perturbación de los patrones del sueño, problemas musculoesqueléticos por el peso de las gafas sobre las cervicales, el incremento de la exigencia visual y de mareos, concurren también importantes riesgos psicosociales como el tecnoestrés, tecnofobia, tecnoadicción, fatiga cognitiva[54], la naturaleza adictiva de los diseños inmersivos y gamificados de trabajo, el estrés postraumático[55] o riesgos específicos no extrapolables a otras realidades como la pérdida del control de los aspectos locativos y de tiempo. También hay riesgos para la personalidad moral de la persona trabajadora como los acosos de superiores jerárquicos, bulismo, comentarios ofensivos que inciden sobre la dignidad de la persona[56].

---

presencial, si bien debe reunir las mismas condiciones y requisitos que la formación presencial: consulta de la DGE de 4-10-2017.

[52] Resolución PE 17-1-2024 sobre mundos virtuales: oportunidades, riesgos y repercusiones estratégicas para el mercado único [2022/2198(INI)].

[53] López Jiménez, J. M., Sebastián Castañares, L. y Sales Ibáñez, A. (2022). "El metaverso y las relaciones laborales. Una aproximación", *Revista Jurídica Valenciana*, núm. 40, pp. 103-119.

[54] Vallecillo Gámez, M. R. (2020). "El derecho a la desconexión digital: perspectiva comparada y riesgos asociados" *ADAPT,* núm. 1, p. 2.

[55] SJS 28 Barcelona núm. 13/2024, de 12 de enero considera IT derivada de accidente de trabajo los daños psicológicos provocados al moderador de contenido de una plataforma.

[56] Martone, M. (2022). "Prime riflessioni su lavoro e metaverso", *ADL,* núm. 6, p. 1135.

Sobre todos estos riesgos recae el deber de prevención del empleador y, pese a lo difícil que es su concreción, dicho deber debe regirse por los principios de precaución, proporcionalidad y acción preventiva. El mayor problema reside en que esta nueva combinación de tecnologías pueda abocar a calificar estos riesgos como "riesgos del desarrollo", es decir, riesgos que todavía no existen para el mundo científico y que terminan por exonerar de los deberes de prevención al empresario por no poder planificar su prevención. Pese a ello, como riesgo generado a causa de una actividad de naturaleza lucrativa, debieran ser asumidos por la empresa[57]. La importancia de la prevención de riesgos laborales en el metaverso (sobre todo, fuera del metaverso para que las personas que trabajan dentro de entornos virtuales puedan hacerlo en condiciones de seguridad razonables) se demuestra por la incorporación de obligaciones específicas en esta materia tanto en el Acuerdo Marco Europeo sobre digitalización de 2020[58], en la Directiva sobre condiciones laborales en plataformas digitales de trabajo[59] o en la LTAD, en especial en lo relativo a la fatiga informática en el teletrabajo (art. 18 L. 10/2021).

3.3. Salario, tiempo y lugar de trabajo

En materia retributiva, además de la licitud de los pactos en moneda extranjera[60], la cuestión que se plantea es la de si se puede pagar a las personas trabajadoras por los servicios realizados a través de *blockchain* mediante criptomonedas

---

[57] En caso de aplicación de la ley española: García Salas, A. I., "Responsabilidad de prevención de riesgos laborales ante la incidencia de la tecnología y la robótica" p. 239 quien analiza también si se debe atribuir personalidad jurídica al empleador algoritmo y los mecanismos para cubrir los daños provocados por los nuevos robots cuando sean capaces de actuar de un modo autónomo e imprevisible.

[58] Goerlich Peset, J. M. (2021). "El Acuerdo Marco Europeo sobre digitalización," *DL*, núm. 122, pp. 49-57; Sepulveda, M. (2021), "El acuerdo marco europeo sobre digitalización. El necesario protagonismo de la norma pactada", *TL,* núm. 158, pp. 213-244.

[59] Exigiendo una evaluación de los riesgos que entrañen los sistemas automatizados de supervisión o de toma de decisiones para la seguridad y salud, en particular los posibles riesgos psicosociales, ergonómicos y de accidente laboral, la evaluación de si las salvaguardias de dichos sistemas son adecuadas para los riesgos detectados en función de las características específicas del entorno laboral (art. 12.1), la prohibición del uso de sistemas automatizados de supervisión o toma de decisiones que ejerzan una presión indebida sobre los trabajadores de plataformas o se ponga en riesgo de algún otro modo la seguridad y la salud física y mental de los trabajadores de plataformas (art. 12.4), y la necesidad de canales de denuncia eficaces.

[60] Raso Delgue, J., *cit*., p. 140. Aunque en ausencia de una prohibición especifica, no debieran existir problemas si se trata de una moneda de curso legal sometida a cambio oficial.

convertibles en dinero real o, incluso, en tokens específicos solo utilizables dentro del metaverso a modo de "dinero del monopoly". Esta última opción no es viable y plantea reminiscencias del "truck system" hace ya tantos años prohibido por impedir que el trabajador pueda disponer con total libertad de su salario fuera del ámbito empresarial de acuerdo con sus intereses y necesidades. La duda se mantiene respecto a las criptomonedas convertibles en dinero de curso legal cuya característica principal es el riesgo inherente a su fluctuación ya que su valor depende de la oferta y de la demanda. Se trata de una posibilidad no meramente teórica, sino que parece que ya se está admitiendo en algunos países[61] aunque en puridad habría que estudiar exactamente qué alcance tiene este pago en cada uno de ellos pues, al menos en los Estados Unidos bajo la *Fair Labor Standars Act* (FLSA) se requiere que el pago sea hecho en dinero o cheque[62].

En España no podría pagarse con criptomonedas el salario base[63]. De momento las criptomonedas no pueden considerarse "moneda de curso legal" ni dinero electrónico[64]. La duda es si se pueden considerar salario en especie

---

[61] Como Japón, USA, Canadá, Australia, Singapur o Finlandia: https://www.welcometothejungle.com/es/articles/criptomonedas-bitcoin-salario-del-futuro

[62] https://www.trinet.com/insights/paying-employees-with-cryptocurrency-the-pros-and-cons

[63] El art. 26.1 TRET considera salario "la totalidad de las percepciones económicas de los trabajadores, en dinero o en especie, (...)" sin que el salario en especie pueda superar el 30% "de las percepciones salariales del trabajador ni dar lugar a una minoración de la cuantía integra en dinero del salario mínimo interprofesional" (art. 26.2 TRET) y el art. 29.4 TRET establece expresamente que "el salario, así como el pago delegado de las prestaciones de la Seguridad Social, podrá efectuarlo el empresario en *moneda de curso legal* o mediante cheque u otra modalidad de *pago similar a través de entidades de crédito*, previo informe al comité de empresa o delegados de personal".

[64] El TS, Penal, considera que el bitcoin se puede usar "como un activo inmaterial de contraprestación o de intercambio en cualquier transacción bilateral en la que los contratantes lo acepten, pero en modo alguno es dinero, o puede tener tal consideración legal, dado que la Ley 21/2011, de 26 de julio, de dinero electrónico, indica en su artículo 1.2 que por dinero electrónico se entiende solo el "valor monetario almacenado por medios electrónicos o magnéticos que represente un crédito sobre el emisor, que se emita al recibo de fondos con el propósito de efectuar operaciones de pago según se definen en el artículo 2.5 de la Ley 16/2009, de 13 de noviembre, de servicios de pago, y que sea aceptado por una persona física o jurídica distinta del emisor de dinero electrónico" (STS Penal núm. 356/2019, de 20 de junio de 2019 (rec. 998/2018). En el ámbito social los problemas de las criptomonedas, de momento, se ciñen a estafas de terceros ajenos a los trabajadores haciéndoles creer que son el empresario: por todas, TSJ Baleares 9-2-2024, rec 463/2023 y TSJ Cataluña17-1- 2024, rec. 4757/2023.

sometido a los máximos legales de porcentaje[65] o si constituyen parte del salario, pero como complemento salarial (a modo de lo que ocurre con las opciones sobre acciones o stock *options*, cuya naturaleza de complemento salarial en metálico parece asumir el Tribunal Supremo en STS 24 de octubre de 2001, rec. 4851/2000). La naturaleza de complemento salarial se ajusta mejor a las características de una moneda que no tiene representación física, pero cuyo valor económico es claro al convertirse en dinero efectivo de curso legal (como en el caso de las *stock options* en el momento de su venta). En un futuro, podría pagarse el salario, completo, en criptomonedas si este tipo de activos se reconocieran como estables mundialmente (Tokens referenciados a activos: *Stablecoins*[66]) soslayando así el riesgo de una excesiva fluctuación y el riesgo de que el trabajador se encuentre de pronto sin poder asumir los costes normales de su vida (hipoteca, colegios, manutención etc.) y siempre que tuvieran el respaldo de una entidad de crédito, pues no otra cosa parece permitir el art. 29.4 TRET cuando alude al cheque u "otra modalidad de pago similar a través de entidades de crédito". En esta línea comienza a andar el nuevo Reglamento MiCa (*markets in Cryptoassets*)[67] que permite el uso de "las fichas de dinero electrónico" (e-money tokens o EMT) (arts. 48-58). Se trata de un criptoactivo cuya principal finalidad es la de ser usado como medio de intercambio sustituto electrónico de las monedas y los billetes y que se emplea normalmente para efectuar pagos y que, a fin de mantener un valor estable, se referencia al valor de una moneda oficial de curso legal emitida por un banco central u otra autoridad monetaria (art. 3.1.7 y 8 MiCA). Al estar respaldado por una entidad de crédito podría ya reunir los requisitos exigidos por el TRET. De hecho, se considera ya dinero electrónico (art. 48.2 MiCa).

En materia retributiva cabe preguntarse si hay opción para los conceptos extrasalariales y, en concreto, para los suplidos. Los costes del metaverso en su

---

[65] En sentido positivo, López Cumbre, L. (2022). "Relaciones laborales "por", "para" y "en" el metaverso", *Diario La Ley*, núm. 100033, de 21 de marzo.

[66] Medina Jiménez, J. (2023). "Stablecoins. Riesgos y desafíos jurídicos: un análisis de la regulación contenida en el Reglamento MiCa", *Repositori Digital de la UPF,* Universitat Pompeu Fabra. https://repositori.upf.edu/bitstream/handle/10230/57688/TFGDRET2023MedinaRegimen.pdf?sequence=1&isAllowed=y

[67] Reglamento (UE) 2023/1114 del PE y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) núm. 1093/2010 y (UE) núm. 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937.

hardware y software no son menores. Cuando el contrato se ha celebrado en el metaverso lo normal es que los haya asumido inicialmente el trabajador, pero si la relación se considera de trabajo, lo cierto es que corresponde al empresario su asunción al no aceptarse con carácter general en nuestro país el BYOD (*bring your own device)* cunado supone un abuso o un intento de romper con la nota de ajenidad propia del contrato subordinado jurídicamente[68]. Idea que recepciona el art. 17.2 LTAD cuando prohíbe que la empresa "exija" la instalación de aplicaciones o programas en dispositivos propiedad de la persona trabajadora, ni su utilización en el desarrollo del trabajo a distancia. Aunque estos costes no siempre se podrán trasladar al empleador lo cierto es que el desarrollo de la actividad laboral para un empleador en el mundo inmersivo exige la construcción del avatar, esto es, vestirlo y dotarlo de elementos virtuales para poder desarrollar su trabajo. Si el empleador quiere que la persona trabajadora adquiera o diseñe un uniforme determinado (por ejemplo, empleado de McDonalds)[69] o use trajes de chaqueta con pañuelos de seda o corbatas para proyectar una buena imagen empresarial en una reunión virtual, el coste de estos activos debe ser asumido por el empleador[70] bien directamente o retribuyendo el coste a la persona trabajadora, en cuyo caso se trataría de una partida extrasalarial.

El tiempo de trabajo es un tema mucho más espinoso. En los trabajos en plataformas o aplicaciones la práctica demuestra que las zonas horarias no detienen a los trabajadores pues el cumplimiento de las tareas comprometidas depende, sobre todo, del huso horario del lugar de residencia del cliente y no del proveedor del servicio, pudiendo el trabajo realizarse en horas nocturnas y en cualquier momento del día, de la semana y del año. Los *click workers* terminan por estar

---

[68] SAN 6 -2-2019 (proc. 318/2018) confirmada por STS 8-2-2021 (rec. 84/2019).

[69] El derecho a la imagen puede ser abordado con los mismos parámetros que en el mundo real (López Cumbre, L., *cit*., p. 3). Es claro que si la apariencia que se pretende proyectar es la misma que la exigida en el mundo real y está directamente vinculada con la actividad realizada (por ejemplo, ropa representativa de la marca de la empresa usada en la vida real también) el empresario podrá exigir dicha proyección en tanto condición esencial de contratación. Pero si la proyección pretendida por el empleador en ese mundo virtual no tiene conexión con la actividad empresarial, la persona trabajadora podrá proyectarse con libertad en su avatar, siempre con límites de razonabilidad que no supongan un abuso de confianza o transgresión de la buena fe contractual (por ejemplo, por escoger proyecciones de avatar denigrantes o insultantes respecto a la empresa o lo que representa, como podría ser si se está un día cargado de trabajo, ese día manifestarse en el mundo virtual como una persona esclava atada con cadenas).

[70] Raso Delgue, J., *cit.,* p. 135.

sometidos a contratos a llamada o cero horas donde lo importante es la realización del trabajo sin tener en cuenta el tiempo empleado. La pregunta es si es admisible una relación laboral en la que la deuda de actividad se concreta en una obligación de resultado o trabajo por tareas, pero sin concreción horaria[71]. En el marco de la UE la respuesta viene dada por la Directiva relativa a unas condiciones transparentes y previsibles (Directiva 2019/1152) que establece la obligación de previsibilidad mínima del trabajo y medidas para los contratos a demanda, como ya hemos visto, especialmente pertinentes para prestaciones atípicas de servicios a través de plataformas, aunque no se gestionen ni tomen decisiones algorítmicas. Pero también por la Directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales las cuales, además de tener que cumplir con el deber de transparencia de las condiciones laborales básicas, deben también informar sobre el uso de algoritmos en el lugar de trabajo y en qué medida afectan a los trabajadores individuales. En todo caso no se puede olvidar en el marco europeo la Directiva sobre tiempo de trabajo (D. 2003/88/CE) donde se concretan los tiempos de trabajo y de descanso, así como su interpretación por el TJUE (TSJUE 21-2-2018, C-158/15, asunto *Matzac* y las que le siguen[72]) en relación con los tiempos de guardia calificados de trabajo efectivo cuando el trabajador ve limitadas considerablemente sus expectativas de realizar otras actividades. En España, a la espera de la trasposición de ambas Directivas, serian aplicables las normas generales en materia de tiempo de trabajo, así como la obligación de registro de la jornada laboral y no se permite el trabajo a llamada no previsible[73]. En el metaverso, como fuera de él, la jornada podrá realizarse en

---

[71] Aragón Gómez, C. (2023). "El tiempo de trabajo ante las nuevas formas de organización empresarial", AA. VV., *Cambio tecnológico y transformación de las fuentes laborales*, Tirant lo Blanch, pp. 125 y ss.

[72] https://almacendederecho.org/cronica-laboral-las-guardias-como-tiempo-de-trabajo

[73] El art. 26 TRET permite el salario por unidad de tiempo, pero también por unidad de obra. Pero se ha considerado que el sistema de trabajo por tareas incumple la normativa nacional y europea sobre la obligación de registro de jornada y supone un grave perjuicio al sistema legal y convencional de jornada cuando da lugar a jornadas superiores al máximo legal o convencional (STS 7-2-2024, rec. 214/2021). Además, en relación con el trabajo a distancia, nuestro ordenamiento establece la obligación de que en el acuerdo conste el horario de trabajo de la persona trabajadora y las reglas de disponibilidad (art. 7 LTAD), el derecho al horario flexible en los términos del acuerdo (art. 13 LTAD), el derecho a un registro horario adecuado (art. 14 LTAD) y la obligación de que en la evaluación de riesgos se tengan particularmente en cuenta la "distribución de la jornada, los tiempos de disponibilidad y la garantía de los descansos y desconexiones durante la jornada" (art. 16 LTAD).

horario nocturno (de la zona horaria de la persona trabajadora que está detrás del avatar) y podrán realizarse horas extra, pero siempre y cuando la empresa las autorice ya que en caso contrario el riesgo lo asumiría el trabajador sin derecho a percibir los complementos[74]. Solo delimitada la jornada se podrá dirimir el alcance del derecho a la desconexión digital del art. 88 LOPD cuyos problemas e interpretaciones (solo un derecho del trabajador, pero no obligación del empresario, o un derecho que genera un correlativo deber empresarial[75]) se convierten en un derecho con claro correlativo deber empresarial cuando se trata del trabajo a distancia ex art. 18 LTAD. Pero si no es aplicable nuestra norma, la ineficacia del derecho a la desconexión se hace más patente, profunda y líquida en un entorno como el metaverso donde las personas reales puede que no se conozcan nunca en la vida real perdiéndose en mayor grado la humanidad y aumentando la avaricia.

Junto al salario y al tiempo, la cuestión del "lugar" de trabajo ha generado un gran debate. Se afirma en general que el metaverso es el nuevo "lugar" de trabajo[76]. Pero en realidad el "lugar" en que se ejecuta el trabajo es un lugar estrictamente físico, que puede ser el centro de trabajo de una empresa, el domicilio del trabajador o una cafetería en tanto no exista una normativa universal para las relaciones laborales en el metaverso. En esta línea se mueve la Directiva sobre plataformas digitales que dota de unos derechos mínimos aplicables "a todas las personas que realizan trabajo en plataformas en la Unión" y se aplica "a las plataformas digitales de trabajo que organizan el trabajo en plataformas realizado en la Unión, independientemente de su lugar de establecimiento y de la legislación aplicable" (art. 1.3). Es decir, como en el RGPD, donde la clave es que el usuario resida en la UE, aquí lo importante es que el trabajo se desarrolle o desempeñe en la UE, aunque ello excluye a todos los trabajadores que prestan sus servicios en el metaverso en otros países, que será la regla general.

---

[74] Thibault Aranda, J. (2000). *El teletrabajo: análisis jurídico-laboral,* CES, p. 100.

[75] Sobre el debate, recientemente: Aragón Gómez, C., *cit*. sobre el derecho a la desconexión digital y su problemática Trujillo Pons, F. (2021). *La desconexión digital en el ámbito laboral*, Tirant lo Blanch.

[76] Sagardoy De Simón, I., *cit*.; Cavas Martínez, F., *cit*. p. 59.

3.4. Otras cuestiones laborales

En fin, cabe plantear numerosas cuestiones adicionales de carácter individual que sólo aquí se pueden apuntar, como las relativas a los derechos fundamentales del trabajador que está tras un avatar[77]: el derecho a la intimidad, la libertad de expresión, el derecho a la protección de datos, el derecho a la propia imagen del trabajador –debiendo valorarse si el aspecto del avatar lo decide el empleador o lo puede elegir libremente la persona que presta el servicio–, el secreto de comunicaciones de empleador y persona trabajadora, el derecho a la igualdad y a la no discriminación, a la integridad física y psíquica, al derecho de propiedad intelectual e industrial del empleador y trabajador, etc. Todos ellos de aplicación siempre que detrás esté una persona y no una IA[78].

Pero también otros estrictamente laborales como los derechos de ocupación efectiva, al pluriempleo, la posible modificación de condiciones de trabajo, la suspensión[79], o extinción del contrato[80] por causas empresariales –por introducir un avatar inteligente por IA para realizar las funciones que el avatar gemelar venía desarrollando[81]–, el despido del avatar y la consecuencia para el trabaja-

---

[77] Para el mayor riesgo que las tecnologías inmersivas presentan para los derechos humanos *vid*. Brittan Heller, 6/12/2020, "Reimagining Reality: Human Rights and Immersive Technology." Harvard Kennedy School, *Carr Center Discussion Paper Series,* 2020-008, alertando de que en este espacio existen nuevas convenciones sociales aun no asumidas: "pocas personas saben qué convenciones sociales son aplicables cuando interactúas con alguien que, tal vez, parece ser una tostadora voladora parlante".

[78] Al respecto *vid*. Guerini, M. (2022), *Robot ed effetto di sostituzione: alcune riflession,* LLI, Vol. 8, núm. 2, p. 34; Pérez del Prado, D. (2022), "Metaverso y Derechos fundamentales", *Foro de Labos,* 15-12-2022.

[79] Plantear si cabe la suspensión del contrato de trabajo por fuerza mayor (ERTE por ciberataque al *Land* empresarial situado en el metaverso o sufrido por el avatar profesional), o si es posible la extinción del contrato por estos mismos motivos (eliminación del propio metaverso), constituyen cuestiones que habría también que abordar, al haberse ya dado en el mundo gemelo real. La SAN 37/2022, de 14 de marzo de 2022, rec. 13/2022. Un comentario en Beltran Heredia, I., "ERTE por fuerza mayor derivado de un ciberataque mediante virus *ransomware*", *Una mirada crítica a las relaciones laborales,* 22-3-2022.

[80] Se ha planteado si es posible sancionar y despedir a un avatar, al existir también proyecciones en el mundo real de despidos por incumplimiento de órdenes empresariales del uso de la realidad virtual: STSJ Asturias 29-6-2021, rec. 1249/2021, confirmando la del JS núm. 4 de Gijón, 8-2-2021.

[81] Mercader Uguina, J. R. (2019). "Despido de una administrativa cuyo trabajo ha sido sustituido por un robot: ¿es posible poner puertas al campo?, *El Foro de Labos,* 1-10-2019, comentando la STSJ Galicia 19-7. De interés es también el caso de Alba Renai, una *influencer* virtual

dor gemelar, la cancelación o suspensión de la cuenta, las reglas de subcontratación, los efectos de los grupos laborales virtuales no gemelares en el mundo real, la transmisión de empresa virtual, etc. La regla general será la de, una vez determinada la ley aplicable, proyectar las reglas generales del mundo real adaptándolas en caso de presentar peculiaridad.

4. METAVERSO Y DERECHO COLECTIVO DEL TRABAJO

El metaverso presenta nuevas oportunidades para la organización sindical, especialmente para atraer a la conciencia de clase a los más jóvenes que son quienes inicialmente frecuentarán los mundos inmersivos. La inmersión de los sindicatos para cumplir con sus fines de defensa de los derechos de las personas trabajadoras, asesorando avatares, la utilización de las herramientas de *blockchain*[82] para realizar elecciones sindicales, percibir la cuota sindical, o utilizar el metaverso como mecanismo de comunicación y reunión, son cuestiones fácilmente imaginables. Asimismo, dado el carácter global del metaverso podrían realizarse Acuerdos Marcos Globales (IFAs) por federaciones internacionales de sindicatos como *Global Union*s como Confederación sindical internacional, o bien Acuerdos Marco Europeos (EFAs)[83] para la defensa y determinación de condiciones mínimas en el marco del trabajo decente para todos los trabajadores del metaverso[84]. En el marco nacional, la posibilidad de negociar un convenio colectivo específico para las personas que trabajan en entornos inmersivos y clarificar el convenio aplicable a los nómadas digitales constituyen algunas de las numerosas cuestiones futuras a dilucidar[85].

---

creada por inteligencia artificial que se ha unido al plantel de presentadores de Mediaset España para cubrir el *reality* de televisión *Supervivientes 2024.*

[82] Peruzzi, M. (2022). "Almeno tu nel metaverso. Il diritto del lavoro e la sfida dei nuovi spazi digitali", *LLI,* Vol. 8, núm. 2, p. 69 señala la existencia de la primera comunidad global que financia y apoya a los trabajadores en sus demandas y acciones colectivas: The Labor DAO.

[83] De interés es el Acuerdo Marco Europeo sobre digitalización de 2020.

[84] En la Directiva sobre plataformas digitales se prevé la obligación de las plataformas de posibilitar que los trabajadores se pongan en contacto y se comuniquen entre sí y de ser contactados por representantes a través de la infraestructura digital o por medios igualmente eficaces (art. 15), dada la "ausencia de un lugar de trabajo común" (Considerando 45).

[85] Sobre los problemas de determinación del convenio colectivo aplicable *vid.* Cruz Villalón, J. (2022). "Las especialidades del teletrabajo transnacional", ACDCT, Vol. XIV, p. 104.

Otras posibilidades y reflexiones futuras surgen en relación con la representación (interna/externa[86] de las personas trabajadoras del metaverso[87]); la generación de una nueva conciencia de clase inmersiva; la posibilidad de realizar elecciones dentro del metaverso e introducir un nuevo colegio electoral teniendo en cuenta las peculiaridades de la prestación del servicio; los derechos de los representantes dentro del metaverso, como el de un local o sala virtual en el metaverso para sus reuniones, por ejemplo[88]; o la posibilidad de constituir comités de empresa europeos para personas trabajadoras en entornos inmersivos en el marco de empresas multinacionales con sede en la UE. Pero también en relación con los derechos de información, consulta y participación como elementos clave del desarrollo social en entornos inmersivos. En este sentido, el RIA y las Directivas sobre condiciones transparentes y previsibles y la Directiva de mejora de las condiciones de trabajo en las plataformas digitales refuerzan la intervención colectiva en la toma de decisiones y debieran permitir una mayor participación de los trabajadores y de los representantes de los trabajadores, entre sí y cooperando en la vigilancia humana de los sistemas automatizados.

Finalmente, la posibilidad de huelgas y conflictos colectivos es todo menos virtual. Como en el trabajo en plataformas digitales, también elementos que resultan esenciales en la configuración tradicional del trabajo, como el tiempo y el lugar, pasan a un segundo plano y, frente a la necesidad de la concentración de los trabajadores en el espacio en un momento homogéneo, la realidad inmersiva permite la dispersión en la prestación de servicios[89]. Prueba de ello sería la huelga de Glovo en Barcelona. La famosa huelga por recortes salariales llevada a cabo en 2007 por los trabajadores de IBM en el seno de dicha empresa ubicada en el *land* del metaverso de *Second Life* pese a su impacto mediático, no puede calificarse como huelga legal –al menos en España[90]–. La digitalización y los sistemas de

---

[86] Incorporando a los trabajadores reales que ejecutan su trabajo en el seno del metaverso a los convenios y acuerdos generales, contemplando, en su caso, especialidades.

[87] Sobre estos temas *vid.* Cherry, M. A. (2009). "Working for (virtually) mínimum wage: aplplying the fair abor standards Act in cyberspace", *Alabama Law Review,* núm. 5, pp. 1077 y ss.

[88] Como sugiere Donini Novella (2022). *Il metaverso come luogo di lavoro LLI,* Vol. 8, núm. 2, p. 22.

[89] Goerlich Peset, J. M. (2020). "Digitalización y derecho de huelga", *TL,* núm. 155, p. 95.

[90] En España podría constituir una huelga abusiva por no suponer una cesación efectiva del trabajo pues los trabajadores de IBM siguieron en sus puestos y solo movieron sus avatares dentro del entorno virtual.

IA permiten nuevas formas de conflicto y amplifican su visibilidad, pero también la sustitución permanente de trabajo y el esquirolaje tecnológico por la extrema facilidad de encontrar personas disponibles para trabajar a través de sus propios avatares en el metaverso incluso si están físicamente ubicados en áreas geográficas distantes[91]. Los conflictos y huelgas, por lo demás, podrían también darse en el mundo real por conflictos laborales dentro del metaverso, baste recordar la huelga contra la IA y la por parte de los actores de Hollywood en 2017.

5. PODERES DEL ESTADO, INSTITUCIONES LABORALES PÚBLICAS Y METAVERSO

El metaverso genera una nueva dimensión también para las instituciones públicas laborales. En primer lugar, para la administración pública laboral dentro del metaverso, pudiendo constituirse un Ministerio de Trabajo en un *land* que dictara normas específicas para su cumplimiento dentro del metaverso, con composición decidida por la plataforma privada, o pública, o por la DAO, o bien conformado por normas internacionales exógenas al metaverso. También en relación con posibles órganos consultivos (a modo del CES), Institutos u organismos de servicios públicos que gestionen las particularidades de un mundo legislativo y jurisdiccional dispar mientras no se armonicen normas de contenido mínimo inderogable. La aplicación de los sistemas de seguridad social en las relaciones inmersivas abre enormes cuestiones que solo se pueden apuntar[92]. Fuera del metaverso, la normativa aplicable a los *metaworkers* se rige, en términos generales, por el principio de territorialidad, aunque en el trabajo transnacional europeo surge la duda (igual que en el marco del contrato de trabajo) de si la referencia para determinar en qué Estado se ejerce la actividad profesional es el lugar de residencia o donde radica el establecimiento para el que trabaja. Recientemente en Europa se prevé una excepción a la aplicación del principio de territorialidad en la coordinación de los sistemas de Seguridad Social pues un Acuerdo Marco de 2023[93] prevé la aplicación de la legislación del Estado en el que el empresario

---

[91] Donini Novella, *Il metaverso come luogo di lavoro*, cit., p. 22.

[92] Específicamente, Burriel Rodríguez, P. (2023). "Más allá del "zoom": la seguridad social y el metaverso", AA. VV., *Las transformaciones de la Seguridad Social ante los retos de la era digital. Por una salud y Seguridad Social digna e inclusiva*, Vol. 1, pp. 89-106.

[93] Acuerdo marco de 30-6-2023 (BOE 4 de agosto), relativo a la aplicación del apartado 1 del artículo 16 del Reglamento (CE) núm. 883/2004 en los casos de teletrabajo transfronterizo habitual.

tenga su sede o su domicilio, siempre que el teletrabajo transfronterizo realizado en el Estado de residencia sea inferior al 50% del tiempo de trabajo total. Aunque se prevén tantas excepciones que presenta poco recorrido[94]. Dentro del metaverso las cuestiones parecen más ficticias, pero habrá que interrogarse sobre si puede cotizar en el metaverso, si existen contingencias diversas, si se pueden cobrar las prestaciones en criptomonedas, si existen mínimos de subsistencia, etc. Por otro lado, el cumplimiento de las normas laborales positivas en el seno de las realidades inmersivas (por ejemplo, acoso cibernético) obliga a traer a colación el papel de la inspección de trabajo, o a pensar en la creación de un cuerpo especializado que permita la inmersión de avatares de la inspección gemelares, es decir, representando personas reales o la creación de inspectores robotizados para los que la IA haya programado para el cumplimiento de las normas aplicables fuera y dentro del entorno inmersivo. Podrían ser nuevos campos de actuación para la Autoridad Labotal Europea o la Agencia Europea de Inteligencia Artificial.

Finalmente, la administración de justicia y los mecanismos de solución extrajudicial de conflictos muestran nuevas posibilidades en la realidad inmersiva. Conflictos generados dentro del metaverso que se resuelven en tribunales reales[95], o casos reales que se resuelven en audiencias reales usando el metaverso[96] para evitar ausencias, ahorrando tiempo y costes de desplazamiento. Incluso, se podría contemplar una Meta jurisdicción y "tribunales metavérsicos" a cuyo sometimiento se pudiera quedar vinculado son algunas de las hipótesis por construir en su formulación y resolución jurídica. Lo mismo se puede decir de la configuración de sistemas de resolución extrajudicial de los conflictos laborales, pudiendo utilizar el metaverso como sistema de resolución de conflictos del mundo físico (en plataforma del SIMA o de la CC. AA., por ejemplo en caso de conflictos en España), resolviendo conflictos del metaverso en instituciones autónomas o heterónomas de conciliación, mediación y arbitraje o estableciendo mecanismos de solución extrajudicial autónomos y públicos y privados organizados por la propia plataforma en un *land* o consensuados en el marco *blockchkain.* En este sentido, aunque conviene recordar

---

[94] *Vid*. Cruz Villalón, J., "Las especialidades del teletrabajo transnacional", *cit.,* pp. 106 y ss.

[95] Juicio de los *Metabirkins*, unos NFTS que emulaban Bolsos Birking de Hermés quien interpuso demanda por uso no autorizado de marca con sentencia favorable para la casa de moda.

[96] El primer juicio en el metaverso se llevó a cabo en el Tribunal administrativo de Magdalena, en Colombia a través de *Horizon Workrooms*. Puede verse en https://www.youtube.com/watch?v=obtpftF2wcI

que en todas las plataformas el consentimiento para el acceso lleva consigo cláusulas de sumisión competencial[97], o que en los entornos de *blockchain* es difícil proyectar el Reglamento Bruselas I bis (R. 1215/2015) y los acuerdos atributivos de jurisdicción, los conflictos "laborales" que se puedan generar dentro del metaverso de momento debieran encontrar solución de la mano de la previa determinación del foro competente y de la norma aplicable, ya que exceden de las sumisiones aceptadas tendentes a canalizar responsabilidades derivadas del uso del programa.

6. CONCLUSIONES

Los metaversos ya existen y pueden ser de muy diferentes tipos. Pero el metaverso del futuro pretende ir más allá de los meros videojuegos y las plataformas para convertirse en totalmente inmersivo y en una proyección sensorial completa del mundo real. Como toda novedad presenta ventajas e inconvenientes. Los distintos modelos de gobernanza presentan consecuencias jurídicas relevantes al no ser lo mismo que se rijan por una ley privada, centralizada e impuesta por quien ha invertido y financiado el mundo gemelar, que por una gobernanza descentralizada basada en DAOs. En cualquiera de los supuestos, los gobiernos se topan con limitaciones derivadas del carácter global que caracteriza estos mundos virtuales y que exceden del ámbito jurídico para combinarse con complejos problemas técnicos. En cualquiera de los modelos de gobernanza surgen problemas cuyo embrión se gesta desde la propia naturaleza consensuada e inmersiva del metaverso. Por ello uno de los grandes retos jurídicos va a ser el de la protección general de los derechos humanos universales y, particularmente, el de la protección de los datos personales. La privacidad y protección de datos debe reforzarse en estas plataformas desde el diseño y por defecto, implicando en la medida de lo posible a los agentes sociales y a autoridades imparciales especializadas con capacidad para auditar el cumplimiento de unos mínimos estándares jurídicos. No debiera ser suficiente un consentimiento activo informado actualizado donde el usuario debe rechazar expresamente las injerencias no deseadas. Por el contrario, el modelo debiera ser el inverso, con la premisa del rechazo generalizado del uso

---

[97] Arribas Sánchez, B. (2022). "Régimen jurídico del metaverso: una aproximación europea", *Informática y Derecho. Revista Iberoamericana De Derecho Informático,* 2ª época, núm. 12, pp. 151-159, señala que en *Decentraland* los términos de uso señalan la ley panameña como derecho aplicable y arbitraje de la ICC como sistema ADRS; *Meta* el derecho del Estado de California y el arbitraje de la AAA; *Sandbox* ley y jurisdicción de los tribunales de Hong Kong.

desviado de datos y del perfilado, el comportamiento activo debiera dirigirse solo a confirmar todo aquello no técnicamente necesario. En general, debiera adaptarse la normativa europea para clarificar cómo garantizar en el metaverso la tutela de la privacidad, cómo garantizar el consentimiento previo necesario para que su uso sea informado y consciente, cómo se cumple el principio de minimización de datos, clarificar quién es el responsable y, en su caso, el encargado, cómo localizar y custodiar de modo seguro los datos y garantizar que las partes interesadas tengan derecho a visualizar, extraer, portar y, sobre todo, suprimir los datos (lo que parece especialmente complejo en cadenas de *blockchain*). En cualquier caso, el consentimiento debiera acompañarse con un sistema de control por parte del usuario sobre la recopilación y almacenamiento de los datos recogidos, lo que podría hacerse mediante sistemas que permitieran que los datos de categoría especial o sensibles se retuvieran en los dispositivos del usuario (gafas) pero no se enviasen ni almacenaran en archivos externos o servidores, reteniendo el usuario así el control.

En el marco del Derecho del Trabajo, todos los problemas generales del metaverso en materia de protección de datos se multiplican porque la dirección y control de las personas trabajadores no sólo se realiza por el empleador sino, en mayor medida incluso, por un tercero ajeno al mismo. El reto reside en el control empresarial de los datos y la cesión de estos por parte del tercero intermediario, lo que podría resolverse asegurando que en el marco del *land* virtual el control de datos fuera exclusivamente empresarial permitiéndole el acceso de los datos solo respecto del cumplimiento de la relación laboral, esto es, viabilizar y gestionar la intermediación de un tercero. Pero no sólo ello, sino que, para el cumplimiento del respeto de los derechos laborales, el principio de proporcionalidad, *a priori* incompatible con una recopilación de datos en tiempo real y permanente, debe ser respetado, de modo que los datos a los que el empresario o el tercero pueda tener acceso sean los estrictamente necesarios (por ejemplo, exclusivamente se le proporcionarían cuando demostrara el empleador indicios de incumplimiento). En este sentido, la autodeterminación de datos laborales (*IDW, Individual Data Work*) podría servir de pilar sobre el que sustentar el Derecho del Trabajo digital[98]. En definitiva, deberá examinarse en qué medida son suficientes los requisitos actuales contemplados en el RGPD y en el RIA para los metaversos.

---

[98] Su alcance y protección mediante bloques de *blockchain* en Nisa Avila, J. A, "El Derecho del Trabajo Digital en el metaverso", *cit.;* Nogueira Guastavino, M. y Mangan, D., "The metaverse matrix of labour law", *cit,* p. 20, en línea con el art. 40 RGPD.

Los problemas de gobernanza y normativa aplicable aconsejarían la instauración de un Metalaw específico para el Multiverso, a modo de Tratado Internacional sobre las realidades inmersivas o, incluso, específicamente sobre el trabajo desarrollado en su seno, conteniendo una serie de principios y derechos fundamentales que sirviera de guía general y de aglutinador, permitiendo superar la variedad de modelos de regulación del gobierno de internet que se trasladarían al metaverso. La cuestión reside, de nuevo, en la legitimidad para emanarlo. A la ONU le correspondería el establecimiento de criterios generales en la línea con los Principios Rectores de las Naciones Unidas para las Empresas y los Derechos Humanos (PRNU) de 2011 sobre los estándares de la responsabilidad de las empresas multinacionales en relación con los derechos humanos (deber de proteger, respetar y remediar), aunque convendría profundizar en el grado de coercibilidad. Un Tratado que no sólo valdría para los metaversos de estructura centralizada [incorporando el reconocimiento del cumplimiento en sus condiciones generales de uso (TOUs)], sino que sería aplicable a los metaversos descentralizados (introduciéndolo en el protocolo inicial o en los estatutos digitales de las DAOs). Para el ámbito específicamente laboral, sin duda, la OIT debiera tomar la iniciativa y los principios que configuran los mínimos de trabajo decente, servirían de referencia en un Convenio específico sobre los derechos laborales en el trabajo inmersivo, con la previsión de órganos tripartitos para la resolución de los conflictos que pudieran darse dentro del metaverso. En todo caso, la estela que debe guiar toda regulación debe ser la de centrar la IA en el ser humano y reforzar el respeto de los derechos humanos.

Por otro lado, para cuestiones más precisas, habría que abordar la competencia jurisdiccional y la norma aplicable, estableciendo criterios específicos de derecho internacional para los conflictos en el metaverso, clarificando para estas realidades cuál es el "lugar" en que "debe cumplirse la obligación" o, en materia laboral, el de "desarrollo habitual del trabajo". En este sentido, convendría que, cualquiera que fuera la jurisdicción aplicable, se pudiera establecer un bloque de derechos y condiciones laborales como mínimos indisponibles equiparables al del lugar de recepción del trabajo, a modo de lo que se prevé en el ámbito de la UE para el desplazamiento de trabajadores.

La nueva geopolítica del metaverso ya se está posicionando frente a la dictadura de las fuerzas del mercado. El liderazgo, sin duda, lo ha asumido la UE con la promulgación de normas específicas como las mencionadas en este artículo (DSA, DMA; RIA, RGPD; Directivas de plataformas digitales de trabajo, etc.);

normas que, a pesar de necesitar una adaptación a las especificidades del metaverso, constituyen todo menos pasos en falso cuando proclaman una filosofía centrada en el ser humano y en los valores de la UE, entre ellos, los derechos fundamentales, incluidos los de los trabajadores[99], o la defensa de la democracia.

A nivel internacional se sigue la estela europea iniciada con la reciente proclamación de la primera resolución de la asamblea general de las Naciones Unidas sobre inteligencia artificial (21-3-2024) en la que se insta a los Estados que se abstengan de utilizar sistemas de inteligencia artificial que no puedan funcionar de conformidad con las normas internacionales de derechos humanos o los pongan en riesgo, proclamando que los mismos derechos que tienen las personas fuera de línea deben protegerles también en línea, incluso durante todo el ciclo de vida de los sistemas de inteligencia artificial.

Junto a la gobernanza política, la gobernanza empresarial como forma de cumplimiento de las normas aplicables y de autogobierno tiene también un gran juego de actuación. Un código de conducta para la industria inmersiva regido por una política de transparencia que muestre los principios básicos que sostienen cada metaverso y que permita a los usuarios actuar de modo ético, sostenible y responsable y optar por una plataforma u otra resultaría imprescindible. Especificar si se acogen Objetivos de Desarrollo Sostenible (ODS), cuáles y cómo, o si optan por seguir estándares de conducta internacionales o buenas prácticas, permite al usuario una selección acorde con sus valores prioritarios. El valor reputacional en este sentido podría atraer un número mayor de usuarios a un concreto metaverso, expulsando del mercado aquellos otros carentes de principios generales y faltos de respeto por los derechos fundamentales. Un código de conducta permitiría a las empresas anticipar y abordar desafíos minimizando daños, pero, además, abordando las cuestiones sobre la base de un consenso de las diversas partes interesadas[100].

---

[99] La expresamente advierte de aplicación a estos entornos de los estándares laborales de la UE, incluyendo las normas relativas a seguridad y salud en el trabajo, o seguridad social, para evitar que este nuevo tipo de plataformas se convierta en un refugio de incumplimiento laboral: Iniciativa de la UE sobre la web 4.0 y los mundos virtuales: en la vanguardia hacia la próxima transición tecnológica.

[100] Brittan Heller, 6/12/2020, "Reimagining Reality: Human Rights and Immersive Technology", Harvard Kennedy School, *cit.*

BIBLIOGRAFÍA

AA. VV. (2023). *Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU*, Publications Office of the EU, Luxembourg.

Aragón Gómez, C. (2023). "El tiempo de trabajo ante las nuevas formas de organización empresarial", AA. VV., *Cambio tecnológico y transformación de las fuentes laborales*, Tirant lo Blanch, pp. 125-150.

Arribas Sánchez, B. (2022). "Régimen jurídico del metaverso: una aproximación europea", *Informática y Derecho. Revista Iberoamericana de Derecho Informático,* 2ª época, núm. 12, pp. 197-220.

Barrio Andrés, M. (2023). "El metaverso y su impacto en el Estado y la soberanía", UNED, *Revista de Derecho Político,* núm. 117, mayo-agosto, pp. 197-220.

Beltran Heredia, I. (2022). "ERTE por fuerza mayor derivado de un ciberataque mediante virus *ransomware*", *Una mirada crítica a las relaciones laborales,* 22-3-2022.

Biurrun Abad, F. (2021). ¿Abrirías tu despacho en el Metaverso?, *Actualidad Jurídica Aranzadi*, 22 diciembre.

Brittan Heller, (2020). "Reimagining Reality: Human Rights and Immersive Technology", Harvard Kennedy School, *Carr Center Discussion Paper Series,* p. 9, 6/12/2020.

Burriel Rodríguez, P. (2023). "Más allá del "zoom": la seguridad social y el metaverso", AA. VV., *Las transformaciones de la Seguridad Social ante los retos de la era digital. Por una salud y Seguridad Social digna e inclusiva*, Vol. 1, pp. 89-106.

Cherry, M. A. (2009). "Working for (virtually) minimum wage: applying the fair labor standards Act in cyberspace", *Alabama Law Review,* núm. 5, pp. 1077-1110.

Cruz Villalón, J. (2022). "Las especialidades del teletrabajo transnacional", *ACDCT*, Vol. XIV, pp. 93-107.

Donini Novella (2022). "Il metaverso come luogo di lavoro", *LLI,* Vol. 8, núm. 2.

Ercilla García, J. (2020). "Aproximación jurídica a las organizaciones autónomas descentralizadas", *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 52.

Fairfield, J. A. T. (2012). "Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life", *Berkeley Technology Law Journal*, Vol. 27, núm. 1, pp. 55-116.

Galindo Martes, E. (2022). "Las consultas médicas llegan al metaverso", *TICPyme*s, 31-1-2022.

García Salas, A. I. (2023). "Responsabilidad de prevención de riesgos laborales ante la incidencia de la tecnología y la robótica", AA. VV., *Cambio tecnológico y transformación de las fuentes laborales: ley y convenio colectivo ante la disrupción digital*, Tirant lo Blanch, pp. 223-246.

Goerlich Peset, J. M. (2021). "El Acuerdo Marco Europeo sobre digitalización", *DL*, 122/2021, pp. 49-57.

Goerlich Peset, J. M. "Digitalización y derecho de huelga", *Temas Laborales*, núm. 155, pp. 93-108.

Guerini, M. (2022). *Robot ed effetto di sostituzione: alcune riflessioni, LLI*, Vol. 8, núm. 2. https://labourlaw.unibo.it/article/view/15994

Llaneza González, P. (2021). *Identidad Digital*, Bosch-Wolter Kluwer.

López Cumbre, L. (2022). "Relaciones laborales "por", "para" y "en" el Metaverso", *Diario La Ley*, núm. 100033, de 21 de marzo.

López Jiménez, J. M., Sebastián Castañares, L. y Sales Ibáñez, A. (2022). "El Metaverso y las relaciones laborales. Una aproximación", *Revista Jurídica Valenciana*, núm. 40, pp. 103-109.

Malaschini, A. (2023). "Metaverso e diritto: su alcune questioni giuridiche della realtà virtuale", *GiustAmm.it*, núm. 2, pp 1-28.

Martone, M. (2022). "Prime riflessioni su lavoro e metaverso", *ADL,* núm. 6, pp. 1131-1146.

Mata Muñoz, A. (2022). "Metaversos: *blockchain* y seguridad jurídica", *Diario La Ley sección ciberderecho*, núm. 60, abril, Wolters Kluwer, versión digital.

McGee, P. (2023). "Hands on with Apple's Vision Pro: bringing the metaverse to life", *Financial Times*, June 6.

Medina Jiménez, J. (2023). "Stablecoins. Riesgos y desafíos jurídicos: un análisis de la regulación contenida en el Reglamento MiCa", *Repositori Digital de la UPF,* Universitat Pompeu Fabra.

Meneses, N. (2021). "El metaverso: nuevas oportunidades laborales y retos en el futuro de las redes sociales, *El País,* Madrid, 25-11-2021.

Mercader Uguina, J. R. (2019). "Despido de una administrativa cuyo trabajo ha sido sustituido por un robot: ¿es posible poner puertas al campo?, *El Foro de Labos,* 1-10-2019.

Mercader Uguina, J. R. (2024). "El Reglamento de inteligencia artificial entra en la recta final: una primera lectura en clave laboral", *Iustel*, *RGDTSS*, núm. 67, pp. 328 y ss.

Miranda Boto, J. M. (2023). *Condiciones de trabajo transparentes y previsibles: desafíos para el Derecho español en la trasposición de la Directiva (UE) 2019/1152*, Tirant lo Blanch.

NEWZOO, *Introduction to the Metaverse Report*. https://newzoo.com/insights/trend-reports/newzoointro-to-the-metaverse-report-2021-freeversion/

Nisa Avila, J. A. (2022). "El Derecho del Trabajo Digital en el Metaverso", *El Derecho.com Francis Lefebvre*, 19-09-2022.

Nisa Avila, J. A. (2021). "El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas, *El Derecho.com,* Lefebvre, 30-11-2021.

Nogueira Guastavino, M. "Metaverso y legislación aplicable al contrato de trabajo", *Revista de Trabajo y de Seguridad Social, CEF*, 471/2022, pp. 17-53. Puede encontrarse en italiano: *Metaverso e legislazione applicabile al contratto di lavoro*, *ADL*, núm. 3, 2023, pp. 445-470.

Nogueira Guastavino, M. y Mangan, D. "The metaverse matrix of labour law", *Italian Labour Law e-journal*, Vol. 16, núm. 1, pp 13-27.

Oulego, J. R. (2021). "DAO naturaleza e implicaciones jurídicas", AD núm. 180, blog *on line*.

Pérez del Prado, D. (2022). "Metaverso y Derechos fundamentales", *Foro de Labos* 15-12-2022.

Pérez del Prado, D. (2023). "Los tradicionales conceptos de trabajador y empresario en un mundo digital", AA. VV. Mercader y Puebla (dirs.), *Cambio tecnológico y transformación de las fuentes laborales,* Tirant lo Blanch, pp. 91-124.

Peruzzi, M. (2022). "Almeno tu nel metaverso. Il diritto del lavoro e la sfida dei nuovi spazi digitali", *LLI,* Vol. 8, núm. 2, on line.

Pietro, R. y Cresci, S. (2021). "Metaverse: Security and Privacy Issues", *Researchgate*.

Raso Delgue, J. (2022). "Metaverso y Derecho del Trabajo", *Informática y Derecho. Revista Iberoamericana de Derecho Informático,* 2ª época, núm. 12, pp. 127-150.

Sagardoy de Simón, I. (2022). "El metaverso y los derechos laborales", *El confidencial* 22-2-2022.

Sepúlveda, M. (2021). "El acuerdo marco europeo sobre digitalización. El necesario protagonismo de la norma pactada", *Temas Laborales,* núm. 158, pp. 213-244.

Thibault Aranda, J. (2000). *El teletrabajo: análisis jurídico-laboral,* CES.

Trujillo Pons, F. (2021). *La desconexión digital en el ámbito laboral*, Tirant lo Blanch.

Vallecillo Gámez, M. R. (2020). "El derecho a la desconexión digital: perspectiva comparada y riesgos asociados" *ADAPT,* núm. 1, pp. 210-238.

Weinstein, G., Lofchie, S. y Schwartz, J. (2022). "A primer on DAOs", *Harvard Law School Forum on Corporate Governanc*e, 17-09-2022.

Sexta Parte

ESTUDIOS SOBRE PLATAFORMAS

Capítulo 15
THE INDIVIDUAL EMPLOYMENT RELATIONSHIP THROUGH DIGITAL PLATFORMS

Adalberto Perulli
Full Professor of Labour Law
Ca' Foscari University of Venice
https://orcid.org/0000-0001-9202-498X

1. INTRODUCTION. WORK AND TECHNOLOGY WITHIN PLATFORM ECONOMY

According to economic sociology, the advent of digital technologies marks the shifts towards a new "platform capitalism", where companies result as virtual structures of interconnection between supply and demand of goods and services[1]. As a multifaceted entity, platforms tends to conceal their true nature as a business and their role as an employer, but they fail to hide the oppressive dimension of digital technology, with its scope of organisation, control and technical-strategic discipline.

This is not to say that every platform and every mechanism incorporated in the algorithm is necessarily the expression of an arbitrary and alienating imposition, a digital vector of a social reification that reduces interpersonal bonds to mere principles of instrumental rationality. Of course, according to a critical perspective, what has been defined as the "uberization" of society creates *app-driven* entities that perform *on-demand* services imparted and monitored by a superordinate provider within an oppressive re-edition of Taylorism. If this interpretation were correct, gig economy might be considered as the latest and radical manifestation of an economic rationality that exploits technology in order to use human work as an increasingly flexible production factor.

---

[1] Perulli, P. (2018). Dopo il capitalismo, in Perulli, A., a cura di, *Lavoro autonomo e capitalismo delle piattaforme*, Wolters Kluwer-Cedam, p. 147 ss.

However, there's a more problematic and detailed analysis to be opposed to this drastically negative vision. The former tends to verify the links between digital technology of platforms and human work, also considering the new economic challenges in terms of protection of social rights and of the person of the worker, without only applying the traditional regulatory framework and, above all, without losing sight of "the new, extraordinary possibilities for growth offered by the "second age of machines"[2].

In other words, faced with the surge of technology, the jurist, like any social scientist, must first of all listen to, distinguish and measure the distance between the regulatory system and the economic-social environment, which is always more complex than the former[3]. Most likely, as it happens in all phases of innovation and change in production paradigms, the "old" and the "new" coexist within platform neo-capitalism. Technology as a reproductive imposition of fragmentation and domination – *apps* as a tool for the neo-exploitation of intensive, abundant and low-cost work, where people are employed "*for short-term gigs as errand-runners*"[4] – goes along with innovative production techniques that unexpectedly make work more valued, being less oppressed by the constraints of hierarchical subordination.

The "old" is for sure the revival of the division of labour linked to increasingly "random" and precarious forms of activity, emblematically identified with the term gig *economy*. If the icon of work in the 20th century is the Taylor-Fordist factory, governed by the principles of the scientific organization of work, where the pre-eminent element is prescriptive direction[5], the emblem of the 21st century is the open and unlimited space of *crowd-working*, in which human work performed by an *app-driven* cyber-proletariat is once again reduced to simple,

---

[2] Barbera, M. (2016). L'idea di impresa. Un dialogo con la giovane dottrina giuslavorista, in Perulli, A., a cura di, *L'idea di diritto del lavoro, oggi. In ricordo di Giorgio Ghezzi*, Wolters Kluwer Cedam, Milano, p. 688.

[3] Cfr. Luhmann, N. (1973). Il senso come concetto fondamentale della sociologia, in Habermas-Luhmann, *Teoria della società o tecnologia sociale*, Etas Kompas, p. 14 ss.

[4] Avent, R. (2016). *The Wealth of Humans. Work and its Absence in the Twenty-First Century*, Allan Lane, UK, p. 51.

[5] Winslow Taylor, F. (1960). *L'organizzazione scientifica del lavoro*, Milano, Ediz. Comunità, p. 169 ss.

standardized and programmed movements[6]. The most significant example of this is Amazon's *Mechanical Turk*, whose name evokes the imaginative machine created in 1706 by Baron von Kempelen commissioned by Maria Theresa of Austria, which reproduces the idea of the fake chess-playing automaton, actually operated by a master hidden in its mechanical body. This "operational showcase" collects job advertisements for the performance of tasks that are generally very simple, mechanical and repetitive, although not achievable automatically by AI. Therefore, they are *crowdsourced* by anonymous clients to an equally anonymous *crowd* of operators who, thanks to the help of a virtual platform on the internet, are confined in an "indefinable condition between self-employment and servitude"[7]. If these workers are qualified – as it often happens – as self-employed, they are forced to carry out their activity without any type of protection in the event of illness or injury and without any social security coverage, accepting the rates recognized by the platform (generally under the parameters of a decent salary)[8]. Moreover, they are subjected to unquestionable judgments from customers, with the risk of undergoing a demotion of their position and earning opportunities, exposed to penalties and "deactivations" in case of refusal to carry out a job, or due to an unsatisfactory rating[9]. Some analyzes of the different – but connected – phenomenon of work on demand via apps lead to similar conclusions, especially in the transport and cleaning sectors, through platforms such as Uber, Taskrabbit, Handy, etc., even though they actively arrange service quality standards and in the selection of management and workforce[10].

---

[6] Cfr. Jolly-E. Prouet, C. (coord.) (2016). L'avenir du travail: quelles redéfinitions de l'emploi, des status et des protections? *WP, 4*, marzo, www.strategie.gouv.fr. p. 42.

[7] Mori, L. (2016). *Rivoluzione informatica e lavoro tra XX e XXI secolo, in Il lavoro dopo il novecento. Da produttori ad attori sociali*, a cura di Gramolati, A, and Mari, G., Firenze University Press, p. 139.

[8] American research shows that workers on the Amazon *Mechanical Turk* platform earn on average less than $5 per hour, which is below the *federal minimum wage*: cfr. Hitlin, P. (2016), *Research in the crowdsourcing age, a case study: How scholars, companies, and workers are using Mechanical Turk, a "gig economy" platform, for tasks computers can't handle*, Pew Research Center, July.

[9] Cfr. Dagnino, E. (2015). *Uber law: prospettive giuslavoristiche sulla sharing/on demand economy*, Adapt Labour Studies, giugno.

[10] Cfr. Stefano, V. di (2016). Introduction: Crowdsourcing, the Gig Economy and the Law, in *Comparative Labour Law & Policy Journal*, 37, p. 1 ss.

Faced with the expansion of these fungible particles of the on demand economy[11] and the new models of social regulation through algorithmic devices, labour law plays an essential role, because it expresses the fundamental ethical-social values that must be guaranteed to platform workers. The defensive reaction of labour law against yet another paradox of precariousness, dehumanization and commodification of work[12] is therefore completely natural. From this perspective, digital work may appear, depending on the operating methods of the platform, either as the extreme edge of work randomization, achieved through the *micro-parceling* of the activity leading to the payment of micro-salaries. Or as an unprecedented form of social Darwinism in which work, in its most professional forms, becomes a sort of prize lottery paid only to the *winners*, while the platform still remains the owner of the property rights on the intellectual work[13].

The defense of labour law has mainly focused on the field of qualification of work relationships. And this is completely understandable, given the tendency of platforms to classify workers as self-employed, thus denying them the fundamental protections of labour law. In this perspective, in the face of a truly complex and articulated jurisprudential scenario, the attention of the legislator and the commentator has focused on presumptions of employment relationship, as it happened in Spain with the Ley Riders, in the state of California with the ABC-test, and how a European Directive is willing to intervene, based on the provisions of ILO Recommendation no. 198/2006[14]. As an alternative to the legal presumption, various qualification mechanisms have operated so far, aimed, in general, at considering every activity that can be said to be to some extent "organised" by the platform as an employment relationship[15].

---

[11] Felstiner, A. (2011). Working the crowd: employment and labour law in the crowding industry, in *Berkley Journal of Employment and labour law*, 32, 1, p. 197.

[12] Cfr. Freedland, M. (2016). Le contrat de travail et les paradoxes de la précarité, in *Rev. Dr. Trav*., p. 289 ss.

[13] Cfr. Däubler, w. (2016). Challenges to Labour Law, in Perulli, A., a cura di, *L'idea di diritto del lavoro, oggi. In ricordo di Giorgio Ghezzi*, Wolters Kluwer Cedam, Milano, p. 503, il quale ricorda come, ai sensi del diritto tedesco, il *crowdworker* non è qualificato come un normale lavoratore subordinato.

[14] Cfr. Stefano, V. di (2016). The rise of the "just-in-time workforce: On demand work, crowdwork and labour protection in the "gig economy", *ILO*, p. 22.

[15] Cfr. Lyon-Caen, A. (2016). Plateforme, in *Rev. Dr. Trav*. p. 301.

2. LABOUR LAW'S REGULATIVE CHALLENGES

Digital revolution and platform economy require a deep reconsideration of the functions and classic "figures" of labour law: first of all, subordination vs autonomy. They should not only be understood as categories to measure the scope of traditional labour law, but also as categories that can be overcome by redefining the regulatory links between technology, work and personal protection. From this perspective, the EU Directive on platform work bears substantial relevance: on the one hand it puts forward – through the presumption of employment relationship – a traditional vision of the protections of labour law centered on the notion of direction and control; on the other hand, it relativizes the notion of subordination by extending the protections of algorithmic management to all "persons" who work through a platform, irrespective of the qualification of the employment relationship.

Secondly, and conversely, both the figure of the employer and the conditions of exercise of entrepreneurial powers are called into question: control and direction in particular, which are modified by the digital methods of coordination of the activity. Finally, the legal figures of the organization of work through algorithms call into question particularly important protection issues regarding platform workers, such as discrimination, health and safety and the risks associated with the division of work into micro-tasks, overworking, and risks related to the security features of the platforms[16].

From the first point of view, the development of platform economy – but even more so the digitalisation of the entire production system – is leading to new forms of work that are not consistent with the classic bipartition between subordination and autonomy. Platform workers are often placed in an indistinct archipelago of non-legally adjectivized activities, hybrid forms, which on the one hand, benefit from freedom due to direct contact with the customer, self-determination of working hours and the possibility of carrying out multiple activities also in favour of other subjects. However, they suffer from economic and/or organizational dependence on the platform. Even though workers are classified as self-employed, they are subject to ambiguous mechanisms of control and conditioning, through the general regulations which unilaterally establish

---

[16] Cfr. Dagnino, E., op. cit.; Weiss, M. (2016). Digitalizzazione: sfide e prospettive per il diritto del lavoro, in *Dir. Rel. Ind.* p. 651 ss.; W. Daubler.

the contractual conditions, (such as fixing the price of the service, control over execution, the acceptance clauses of the online activity, or deactivation).

Employers and workers as a category are also strongly under discussion. The *on demand economy* gave rise to economic activities based on the use of internet platforms that allow immediate matching between a user requesting a good or a service and another entity able to provide it by sharing the wealth of goods and skills. Therefore, we are faced with a substantial surge of "opportunistic" and transitory activities, such as the *digital corporation* and *crowdsourcing*, which replace the traditional job assignment within the company with an open call on platforms[17]. The latter, far from presenting themselves as employers, express a different organizational rationality, which does not so much concern – like in classical labour law – the organization of work for productive purposes, but rather the organization of service "markets", which connect customers and workers.

The figure of the employer seems to emerge more clearly in cases where the platform establishes the price of the service, or sets the contractual conditions for the suitor and the technical specifications or requirements of the offer[18]. The first question we need to ask ourselves is therefore whether the platform, under these specific profiles, is an "employer" or whether actually the "organization" functions are accessory to a primary intermediation function of a subject who – as Uber claims – provides to a smartphone user a "*user interface*", essentially a computerized program, as part of a service performance offered by the provider.

According to some, the platform does not limit itself to carrying out an intermediation function. Uber, in particular, claims that the drivers whose services it coordinates are independent providers, often falsifying a very different reality, in which providers are subject to much more penetrating direction and control that than that of Fordist-Taylorist factory workers.

Other analyses, more aware of the difficulties of *tout court* identifying the legal features of a traditional employer in the platform, adopt a functional vision, with the aim of selecting at least one employer's prerogative, exercised by the platform, which allows the employer's role to be attributed at least

---

[17] Dagnino, op. cit.
[18] P. Tullini, op. loc. cit.

partially to the platform[19]. From this perspective, given that the platform often determines the price of the service – typical function of the employer – the platform itself may be considered as an employer, but only in relation to the function of determining the price. For this reason, if the salary paid is below the minimum wage, the platform will be responsible for the violation. Likewise, the platform may be held accountable as a "functional" employer for the violation of anti-discrimination legislation if, for example, in determining the price of the service it systematically reduces the cost of female labour[20].

A completely opposite vision claims that the platform does not provide top down services: Uber, for example, would not offer a transport service[21] but would act as a technological "*enabler*", directly putting those in search in contact with those offering and becoming thus a vehicle of reputation, trust and belonging. Therefore, the platform may offer added value services by designing the environment in which interactions take place, without however influencing the actors who are *enabled*. Furthermore, the *assets* that generate value for the platforms (goods and skills) belong to the people and not to the platform, as it happens in traditional businesses. The actors themselves are interchangeable, in some cases presenting themselves as "those who offer" and in others as "those in search"[22]. It seems clear that the platform does not carry out any of the typical functions of the employer, not even that of fixing the price of the service (as it happens instead for some digital platforms, such as UberPop for example), while the user-operator cannot be classified as an employee, because there is no control/direction of work.

---

[19] The research of J. Prassl moves in this direction. He, on the basis of an original functional theory (J. Prassl, The Concept of the Employer, Oxford University Press, 2015), believes he can identify the employer in the entity, or combination of entities "playing a decisive role in the exericise of relational employing functions, and regulated or controlled as such in each particular domain of employment law"; cfr. Prassl, J. (2017), *Towards a Functional Concept of the Employer*, paper presentato a *The Annual Conference of the European Centre of Expertise (ECE) in the field of labour law, employment and labour market policies: The Personal Scope of labour law in Times of Atypical Employment and Digitalisation*, Frankfurt, April.

[20] https://www.bostonglobe.com/news/science/2013/08/08/the-pitfalls-crowdsourcing-online-ratings-vulnerable-bias/

[21] As is known, the issue is especially relevant from the perspective of European competition law and economic freedoms (freedom to provide services).

[22] Cfr. M. Mainieri, M., and V. Bucci, V. *Sharing Economy: la mappatura delle piattaforme italiane 2014.*

The thesis of the platform as a mere intermediary or technological *enabler* on the market has been widely proved to be wrong by jurisprudence. Since when the platform-work model has established itself as one of the new and emerging labour markets on a global scale, the doctrinal discussion and the (even supranational) decisions of jurisprudence no longer leave room for theses that identify the platform as a mere intermediary. Actually, the focus is on its typically entrepreneurial, productive function, and therefore as a user of the work of others (either as an employer, or as a client in the context of self-employed relationships). The same Court of Justice, in the *Elite Taxi* case, stated that the platform carries out an "intermediation service" based "on the selection of non-professional drivers using their own vehicle, to whom the company provides an application without which (i) those drivers would not be led to provide transport services and (ii) persons who wish to make an urban journey would not use the services provided by those drivers. In addition, Uber exercises decisive influence over the conditions under which that service is provided by those drivers. In fact, it appears that Uber determines at least the maximum fare – by means of the eponymous application, that the company receives that amount from the client before paying part of it to the non-professional driver of the vehicle, and that it exercises a certain control over the quality of the vehicles, the drivers and their conduct, which can, in some circumstances, result in their exclusion"[23].

The intermediation activity of the platform is, therefore, not at all neutral, but is exercised through the establishment of general conditions of sale for the customer, and the preparation of a contract (generally for the provision of services, work, or project-based work) between the platform and the provider, through which the former demonstrates its dominance in terms of contractual relationships, and consequently exercises broad and penetrating legal prerogatives related to the organization of services.

Finally, let's not forget that the legislator, in countries such as France and Italy, has defined the characteristic features of digital platforms as part of a regulation which concerns minimum levels of protection for self-employed workers who carry out delivery activities of goods on behalf of others, in urban areas. Pursuant to Italian law, for example, digital platforms are "the IT programs and

---

[23] ECJ, 20 December 2017, *Asociación Profesional Elite Taxi contro Uber Systems SpainSL*, C 434/15, punto 39.

procedures used by the client which, regardless of the place of establishment, are instrumental to the delivery activities of the goods, setting the compensation and determining the methods of execution of the performance" (art. 47 bis, co. 2, as introduced by art. 1, law no. 128/2019).

3. THE ISSUE RELATED TO THE QUALIFICATION OF THE EMPLOYMENT RELATIONSHIP

The issue of qualifying work relationships with digital platforms has been addressed by the European Commission as part of the European Agenda on collaborative economy[24]. The Commission deals with the issue of qualification as a "shift at a structural level" of the forms and methods on how a job is performed, often based on activities carried out *ad hoc* outside regular and predefined working hours. The Commission stated that "there are increasingly blurred boundaries between the self-employed and employees, there is an increase in temporary and part-time work and multiple job-holding", as also showed by the Eurostat data. In order to verify whether and how the traditional distinction between subordination and autonomy finds application in the collaborative economy, the Commission limits itself to referring to national laws, providing some elements with reference to EU labour law and to the jurisprudence of the Court of Justice. The rights guaranteed by the social chapter of the Union apply, in fact, only to those subjects who can be defined as "workers" pursuant to the jurisprudence of the Court of Justice, for which the essential characteristic of the work relationship is the circumstance that "it covers any person who undertakes genuine and effective work for which he is paid under the direction of someone else"[25].

Whether we are dealing with an employment relationship or not must therefore be verified on the basis of a case-by-case assessment, taking into account the factual circumstances that characterize the relationship between the platform and the underlying service provider and the execution of the related tasks, particularly analysing the three essential criteria consisting of the existence of a subordination link, the nature of work and the presence of remuneration. But what application would this general criterion for qualifying employment relationships have towards service providers who operate through

---

[24] COM (2016) 356 final.
[25] COM (2010) 373.

a digital platform? The answer is not very original. According to the European Commission, the criterion would be met if the service provider acts "*under the direction* of the collaborative platform, the latter determining the choice of the activity, remuneration and working conditions", with the clarification that if the platform merely processes the payment on the part of a user and transmits it to the underlying service provider, this does not imply that the platform determines the remuneration and so it is not to be considered as an employer.

This document does not explain, in fact, what the "direction" by the platform consists of. For this reason, we are faced with the issue relating to the actual specification of the technical characteristics of the direction power of the platform/employer. With reference to the internal legal system, we know that the subjection of the worker to external direction, which jurisprudence considers essential for the identification of the subordination link, can in fact take different forms, with significantly different effects for the purposes of qualification. According to some, the new forms of organization of employment entail an attenuation of the authoritative interventions and controls of the entrepreneur, so much so as to justify the recognition of the relative relationships as being employment relationships even in the face of a simple "hetero-organization" of the service[26]. In this perspective – and for qualifying purposes – the subjection of the worker to the control power of the employer – understood in the most rigorous sense – becomes, with the evolution of non-hierarchical organizational systems and with the extension of forms of outsourcing of entire phases of the production cycle, less and less significant than subordination. With reference to this new attitude of the socio-economic context, the obligation to make one's working energies available to others and to use them continuously according to the general directives given by the employer would take on a decisive value in order to pursue the company's objectives.

This reduction in the typological value of the directive power – affirmed by most commentators and found in the *modus operandi* of part of jurisprudence – guarantees a certain elasticity of the notion of subordination, which is not excluded by possible margins of autonomy, initiative and discretion which the provider actually can benefit from. On the other hand, however, this vision

---

[26] Cfr. Razzolini, O. (2014). La nozione di subordinazione alla prova delle nuove tecnologie, in *Dir. Rel. Ind.*, p. 974 ss.

risks excessively expanding the scope of subordination, which, in the absence of adequate mechanisms for selecting and modulating protections, would translate into an undifferentiated application of labour law in favour of individuals not in need of protection – or in need of protection in forms and measures other than those related to employment.

The Commission, stating that the existence of subordination does not necessarily depend on the effective exercise of "continuous control or supervision" of work, seems to confirm the direction requirement even in the face of an IT platform"predefining" the methods and conditions of work, thereby realizing the "direction" of work via the platform. It is not clear, however, whether, in this way, the Commission really opens up to a broader notion of subordination, of an "organizational" type, which will in any case have to be verified within the individual laws of the Member States based on the criteria in use by the national Courts. In France, for example, the jurisprudence has played a decisive role in broadening the concept of employee through a redevelopment of the *lien de subordination juridique*. The maximum extension of this expansive trend was achieved with the identification of a subordination link in the work performed in the framework of an "organized service" where the employer unilaterally determines the conditions of execution of the service by the client. *Mutatis mutandis*, paths for redefining subordination in an expansive sense are also known in common law countries, where formalistic approaches in terms of interpreting the notion of employee are replaced by a principle of reality – adopted by the UK Supreme Court – and by a "purposive approach" aimed at avoiding removing workers from the protections of labour law, and which part of the doctrine would like to push to the point of a "general presumption" of *employee status*[27].

4. THE QUALIFICATION OF WORK RELATIONSHIPS WITHIN PLATFORMS IN THE SINGLE LABOUR LAW SYSTEMS

The spread of new forms of economy linked to technological innovation and digital platforms therefore exacerbate the issues of qualifying relationships and raises new questions of value linked to the consequences of qualification. The boundary between subordination and autonomy – increasingly uncertain despite the methodological rigour with which the *summa divisio* can be traced

[27] Cfr. Davidov, G. (2016). *A purposive approach to labour law*, Oxford University Press, p. 116 s.

in apicibus – is getting more and more blurred. Consequently, these neighboring universe move, dragged by the factors of production, and it's the legislators task to find in this uncertain upheaval, a rational compass of regulation. However, the main role, up to now, has been played by the Courts, with very different outcomes from system to system.

At the basis of these processes there is a progressive change in the basic paradigm of labour law: the notion of employment. In some countries, such as Italy, the legislator has progressively moved away from the rigidly binary scheme (subordination and autonomy) to take on a more complex regulatory architecture, enriched with new cases, such as "collaborations organized by the client" pursuant to art. 2, co.1, d. lgs. n. 81/2015. In Italy, project-based contracts – pursuant to art. 409 n. 3 c.p.c. – are still being used, whereby the system looks at the qualification of relationships in a more complex perspective, in which employment protections also move "beyond" the case of subordination referred to in the art. 2094 c.c. In other systems, on the contrary, the response of labour law to the problem of qualification has focused on the use of interpretative devices that guarantee the reference of the concrete case to the area covered by labour law protections through the use of different techniques, converging in the aim of not leaving the provider without adequate protections and guarantees: a) use of tests aimed at adapting the protective ratio to the provider's situation of social vulnerability within platform work (such as the English control test, or the *service organisé* criterion adopted by French jurisprudence); b) the provision for presumptions of employment relationship, as it happens in the state of California through the ABC-test, the European Directive on platform work, and on the basis of the provisions of the ILO Recommendation no. 198/2006[28]; c) a teleological ("purposive") interpretation of the notion of subordination, to which the criteria of democratic deficit and economic dependence are added, although they are not referable to any type of digital platform[29]; e) a "remedial" approach, capable

[28] Cfr. V Stefano, V. di (2016). The rise of the "just-in-time workforce: On demand work, crowdwork and labour protection in the "gig economy", *ILO*, p. 22.

[29] Davidov, G. *Setting labour Law's Coverage: Between Universalism and Selectivity*, in questo volume.

of responding through jurisprudence to the needs of social protection even regardless of the use of the usual techniques for qualifying the case[30].

In some cases, along with the mobilization of interpretative techniques on the part of the doctrine and the judiciary, the legislator – aware of the uncertainties in the qualification of these peculiar relationships – intervened to provide a set of minimum protections to platform workers, effectively creating a selective and targeted protection system. The latter recognises, on the one hand, the difficulty of subsuming new forms of digital work within consolidated categories, and, on the other, the need to ensure some basic protections for platform workers even if they are autonomous. In France, the *Loi Travail* (l. n. 1088/2016) containing "*nouvelles libertés et de nouvelles protections pour les entreprises et les actifs*"[31], followed this direction by using the assimilation technique in a very weak and partial way, providing for the application of rules reserved for "self-employed workers who use one or more electronic networking platforms to carry out their professional activity". For this reason, if the platform determines the characteristics of the service performance or of the goods sold and fixes its price, a series of rights not normally recognized to self-employed workers are extended to the provider[32].

In other systems, faced with qualification uncertainties and the consequent difficulty of recognising to the working figures involved the subordination link, "intermediate categories" have been used, as in the case of English workers (like Uber drivers have been referred to). In Italy, project-based work and hetero-organized work[33] have been used, with a broad doctrinal debate also regarding the use of these contractual schemes in the context of platform work.

---

[30] Treu, T. (2017). Rimedi e fattispecie a confronto con i lavori della Gig economy, in *WP C.S.D.L.E. "Massimo D´Antona"*, INT - 136/2017; Id. Rimedi, tutele e fattispecie: riflessioni a partire dai lavori della Gig economy, in LD, p. 367 ss.

[31] New freedoms and protections for businesses and assets (translator's note).

[32] These are social insurance in the event of accidents and occupational diseases, a right to professional training and certification of skills, but also collective rights such as the right to organize trade unions, a sort of right to strike understood as a particular instrument of protection against the retaliatory behavior of the platform, and finally the unemployment benefit for workers who miss the opportunities to operate on the market through technological platforms.

[33] For the critical dialogue established with the doctrine and for the bibliographical references, reference to Perulli A. (2015), Le collaborazioni organizzate dal committente, in Fiorillo, L., and Perulli, A. (a cura di), *Tipologie contrattuali e disciplina delle mansioni*, Giappichelli, Torino, p. 279 ss.; Perulli, A. (2016), Le nuove frontiere del diritto del lavoro, in *Riv. giur. lav.*, Vol. I, p. 11 ss.

Even the Italian legislator, following the interpretative perspective opened by the ruling of the Court of Appeal of Turin in the Foodora case (confirmed by the Court of Cassation, n. 1663/2020) has expressly established the applicability of the rule on hetero-organised collaborations also to workers who use digital platforms, thus guaranteeing the protection of the employment relationship.

5. THE QUALIFICATION OF THE WORK RELATIONSHIP OF PLATFORM WORKERS AND THE COMPARATIVE METHOD

Platform work, while being similar in different national contexts, should not be analysed in the light of a possible paradigm of homogeneous qualification of employment relationships, but in relation to the definitive legal provisions (where existing) or to the jurisprudential guidelines. Consequently, the logical-legal process of qualification is implemented in a systematic perspective, with the awareness that the analysis of comparative systems must be particularly careful[34]. The variability of classification systems is proved by the diversity of the notions of subordination that are used for the purposes of qualifying employment relationships. It is no coincidence that when the ILO adopted Recommendation no. 198 on the employment relationship, it provided for as many as fifteen criteria or indices of qualification of the employment contract, proving the complexity and diversity of the indices of subordination used in the different legal systems, even the apparently closest, such as Italy, France or Spain.

Over the years, many doubts have been raised about the effectiveness of the methods of qualifying employment relationships, which have been questioned as being arbitrary[35] and being "out of sync with the purpose of labour" and "out of touch with the reality of new forms of work arrangements"[36]. The doctrine invites us to revisit the criteria for identifying employment in order to adapt them to the changed organizational contexts, thus counteracting the

---

[34] A good example of a comparative series is Hiessl, C. (2021), The Classification of Platform Workers in Case Law: A Cross-European *Comparative Analysis, in Comparative Labour Law & Policy Journal, 2*, Vol. 42, p. 465 ss.

[35] Langille, B., and Mayer-Goodman, B. (2022). *Hunting for employees, employers, independent contractors, dependent contractors, independent employees, workers, and other figments of the legal imagination*, May 9, Faculty of Law, University of Toronto.

[36] Davidov, G., and Alon-Shenker, P. (2022). The ABC Test: A New Model for Employment Status Determination? in *Industrial Law Journal*, 51, p. 235.

elusive and fraudulent practices of bogus self-employment to reaffirm the "true nature" of the work relationship[37]. In order to overcome such issues, some EU member states have tried to follow the path of the presumption of employment relationship, indicated by ILO Recommendation 198/20064[38].

These uncertainties and criticisms have been partly acknowledged by the jurisprudence itself in some European and non-European jurisdictions. According to the Spanish Supreme Court "*in the post-industrial society the concept of dependency has become more flexible. Technological innovations have favoured the birth of digitalized control systems for the provision of services. The existence of a new productive reality forces us to adapt the concepts of dependence and alienation to the social reality of the time in which the rules must be applied*"[39]. The reference of the Spanish Supreme Court to the concepts of "dependence and alienation" is well suited to the provisions of the art. 1 of the *Estatuto de los Trabajadores*, where alienation is configured as a fundamental requirement of the employment contract[40], given that the statutory legislation applies "to workers who voluntarily provide their paid activity on *behalf of others*" and "within the scope of organization and management of another natural or legal person. Furthermore, the Spanish law, unlike the Italian or French one, provides for a general presumption of employment relationship relating to all those who provide a service on behalf of others, within the control and direction of others (art. 8, co. 1). This presumption, of a general nature and also applicable to the field of social security, is widely used to qualify activities whose legal nature is ambiguous or difficult to classify[41], in particular, as far as this is concerned, in the context of platform work[42].

Both regulations contain a reference to the requirements of "alienness" (understood as a service rendered in favour of others) and "organization", as

---

[37] Davidov, G., Freedland, M., and Kountouris, N. (2015). The Subjects of Labour law: "Employees" and Other Workers, in M. Finkin, G. Mundlak (eds.), *Comparative Labour Law*, Edward Elgar.

[38] *ILO, Regulating the Employment Relationship in Europe: A Guide to Recommendation, 198.*

[39] TS, sentenza 805/2020.

[40] Cfr. Martelloni, F., op. cit.

[41] Waas, B., op. cit., p. lviii.

[42] Cfr. López Balaguer, M. (2018). Trabajo en plataformas digitales en Espana: primeras sentencias y primeras discrepancias, in *LLI, 2*, Vol. 4, p. 53 ss. (qui p. 57).

well as "direction", whose co-presence allows us to derive a different and broader notion of subordination, inclusive of "alienness", "organization" and "direction". This led the *Tribunal Supremo* to state the need to jointly valorise the indices of "dependence" and "alienness" for qualifying purposes. Both dependence and alienness, specifies the *Tribunal Supremo*, are concepts "of a sufficiently high level of abstraction to manifest themselves differently according to the activities and methods of production", allowing us to recognize the "work constraint" typical of subordination[43]. In this perspective, the *Tribunal Supremo* has increasingly loosened its attitude related to a rigid interpretation of "dependence" and "alienness" based on the cumulative presence of the two requirements, opening up to an even broader notion of subordination, substantially identifiable whenever the provider does not provide for his/her own business organisation. For this reason, this situation is to be ascribed to the sphere of organization on behalf of others, with the consequence – unthinkable, for example, under Italian law – of qualifying a relationship as employment due to the circumstance that "decisions relating to business relationships market and relations with the public are taken by the entrepreneur, and not by the worker". That is to say that the *Tribunal Supremo* ended up adopting a "finalist" interpretative stance such as to allow the application of the discipline of the employment relationship "to any provision of services rendered personally, whether it is employment or not"[44].

In light of these necessary clarifications of the regulatory framework and jurisprudential evolution, we can observe the substantial differences with the Italian system, which has taken a different direction to support the expansive process of labour law, by using not the jurisprudential formant, but the legislative one. In Italy, the definition of subordination pursuant to art. 2094 of the Civil Code, which identifies the main index in the subjection of the worker to the direction power of the entrepreneur (and does not in any way contemplate the concept of "alienness"), has been added a rule, art. 2, co.1, of the legislative decree. lgs. n. 81/2015, which substantially expanded the scope of labour law without acting on the defining rule of subordination, but by adopting the technique of

---

[43] TS, 3 novembre 2014.

[44] Cfr. Todolí Signes, A. (2019). Plataformas digitales y concepto de trabajador: una propuesta de interpretatión finalista, in *Revista de relaciones laborales, 41*, p. 14 ss. who reports that the reason why the employment relationship of platform workers must fall within the scope of labour law is that these subjects are not "entrepreneurs with negotiating power".

extending (or assimilating) the discipline to relationships located outside the scope of subordination pursuant to art. 2094 Italian Civil Code.

The comparative analysis must, however, be completed with reference to the different regulatory connotation of the areas adjacent to subordination in the strict sense, i.e. the area of economically dependent self-employment in Spain and that of (hetero-organised) collaborations in Italy (pursuant to art. 2, co. 1, and coordinated pursuant to art. 409, n. 3, c.p.c.), highlighting the different concepts that also concern this regulatory area. In Spain, the economically dependent self-employed worker (TRADE) only apparently corresponds to the concept of "para-subordinate" worker. In fact, the TRADE can absolutely be neither *hetero-organized*, as it actually happens for the collaborator pursuant to art. 2, co.1, nor coordinated, as it used to happen[45] for the collaborator pursuant to art. 409, n. 3, c.p.c.[46]. Consequently, pursuant to the Spanish

---

[45] As is known, in fact, the art. 15 of law no. 81/2017, by establishing that "Collaboration is considered coordinated when, in compliance with the coordination methods established by mutual agreement between the parties, the collaborator independently organizes the work activity", it placed the coordination within a mutually established negotiation program by the parties, differently from the unilateral prerogative of organizing the execution methods of the service referred to in the art. 2, paragraph 1. In the contractual program pursuant to art. 409, n. 3, c.p.c., not only is the work or service requested consensually predefined, this constituting the content of the obligation agreed upon in the formative phase of the contract and without this implying the inclusion of the provider in the client's organization, but also the ways of coordination between the provider and the client's activity. That is to say that the coordination manifests itself, in the absence of the exercise of direction power or hetero-organization, in the simple concatenation of subsequent services which, on the basis of elements *ex ante* predetermined by the parties in the negotiation program, are aimed at realizing the overall interest of the client. In this way, coordination distinguishes itself from the situation of hetero-organization (art. 2, paragraph 1) in which the autonomy in the execution of the service is strongly compromised (if not completely excluded) due to the exercise of a unilateral prerogative of the creditor. This systematic interpretation has received the approval of the Court of Cassation (1663/2020), which, once the hetero-organization has been considered as "an element of a functional collaborative relationship with the client's organization", highlights "the difference compared to a coordination established by mutual agreement between the parties which, instead, in the norm under analysis, is imposed from the outside, matter-of-factly hetero-organised" (point 32; the same concept is reiterated in point 53 of the sentence).

[46] The Spanish legislator has in fact disregarded the indication, coming from the technical committee, which suggested adopting, when defining the figure of economically dependent worker, the criteria of the art. 409, n. 3. c.p.c. Italian, with the consequence that the only characteristic that distinguishes the TRADE from the rest of the self-employed workers is the status of economic dependence, consisting in receiving at least 75% of the income from the

legislation, it is sufficient for the work performance to be hetero-organised to exclude the autonomous nature of the relationship, whereas, in Italian law, if the performance is hetero-organised it may well be, in the absence of hetero-direction, be classified as autonomous (although the effects of this qualification entail the application of the regulations on employment relationships). In fact, to be qualified as TRADE, the worker must have a "production infrastructure" and "own materials" necessary in order to carry out the activity and independent from those of his/her client (art. 11, paragraph 2, letter c), and also be able to carry out the activity according to *his/her* own organizational criteria (art. 11, paragraph 2, letter d). The self-organization characteristic of the TRADE – who might be included in the more general definition of self-employed worker as a natural person who carries out an activity "outside the direction or organizational authority of another person" (art. 1, paragraph 1) – reinforces the idea related to such provider belonging to the self-employed work *genus*. More specifically, because such provider must have autonomous decision-making power regarding the methods of organizing and providing his/her service: that's why the Spanish jurisprudence has denied *riders* the qualification of TRADE.

As we can see, the regulatory scenario related to the decision of the *Supremo Tribunal* is significantly different from the Italian regulatory system: for this reason, the claim to move the meaning of that decision into a different legislative context is equivalent to using legal comparison in a legally incorrect way[47].

Mutatis mutandis, similar considerations apply to French jurisprudence, which introduced the criterion of *service organisé* as a further qualification parameter of the employment relationship. It is first of all necessary to recall that the French system, while offering the interpreter a real *Code du Travail*, does not include a legal notion of subordination, whose legal morphology is entrusted to jurisprudence and its evolution. This consideration alone, in its simplicity, should make us aware of the structural difference between the Italian and French systems:

---

main client, as income from economic or professional activity: cfr. Valdés Alonso, A. (2008), El concepto de trabajador autónomo económicamente dependiente, in Cruz Villalón, J., and Valdés Dal-Ré, F. (dir.), *El Estatuto del Trabajo Autónomo*, Wolters Kluwer, p. 197 ss.; vedi anche Montya Melgar, A. (2009), *El contrato del TRADE. La Ley y el Reglamento*, Thomson Reuters, p. 48.

[47] Cfr. Perulli, A. (2022). Il rider di Glovo: tra subordinazione, eteroorganizzazione, e libertà, in *Argomenti di diritto del lavoro,* 1, p. 37 ss.

the one based on a defining provision of the law (art. 2094 of the Civil Code), the other on a concept of jurisprudential development. The main consequence of this different arrangement of sources when defining the case is that French jurisprudence is much freer to adopt an interpretative-creative approach to the extent that it does not have to deal with a legal text, thus developing with greater ease its own creative function (and therefore also its own function of hermeneutical re-writing of a concept developed over time by the Courts). This depends, decisively, on the lack of legislative definitions of subordination, as it happens with certain "purposive" approaches of the common law tradition. In order to make a correct comparison between the two systems, it is necessary to add that in France, unlike what happened in Italy and Spain, a regulation of "parasubordinate" or economically dependent work relationships has never been adopted, nor does it exist a norm comparable to the art. 2, co.1, of the legislative decree. lgs. n. 81/2015, whereby the jurisprudential notion of subordination, expanded through the index of *service organisé*, clearly contrasts the notion of self-employment. It is true that mechanisms for the partial assimilation of certain forms of (even entrepreneurial) self-employment to employment also operate in France, leading the legislator to extend the provisions of the *Code du Travail* beyond the perimeter of legal subordination. However, this extensive technique completely ignores the identification of a subordination link, and is based on the observation that such self-employed workers are in a situation of (partially "organizational") "economic dependence" such as to justify their (limited or total, depending on the case) assimilation to employees[48].

The *Cour de cassation* 4th March 2020, n. 374, concerning an Uber case, decided to use the concept of "organised service" for qualification purposes, which has long been considered a simple index among the many used by the French jurisprudence to concretely identify the existence of the *lien de subordination*[49]. The *service organisé* criterion proposes an expanded vision of

---

[48] Virassamy, V. G. J. (1986). *Les contrats de dépendence. Essai sur les activités professionelles exercées dans une dépendance économique, LJDJ*, Paris, p. 182.

[49] This criterion, in French jurisprudence, however, came to a halt with the famous *Société Générale* decision (Cass. Soc. 13 November 1996) which reaffirmed the centrality of the control power (even if only in programmatic mode: see the ruling *Société Humanitaire*, Cass. Soc. 15 October 1998), degrading the *service organisé* to a mere index among many. See A. Perulli, *Subordinate, Autonomous and Economically Dependent Work: A Comparative Analysis of Selected European Countries*, cit., p. 151 s. and 160 s.

subordination, free from the exercise of direction power. Although presenting some similarities with the notion of hetero-organised work coined by the Italian legislator (art. 2, co.1), the concept of the worker's inclusion in the organized service (in this case a driver) leads to the qualification of the relationship in the sense of subordination, whereas the Italian notion of hetero-organization instead indicates an independent employment relationship (to which, however, the protections of employment are to be applied). While the first is an index of subordination developed by jurisprudence, used in this specific case to adapt the notion of subordination to the technological context of digital platforms[50], the Italian concept of hetero-organised work is of legislative source, and does not affect the notion of subordination, as it may be placed in the extremity of self-employment performed in conditions of "organizational dependence".

6. THE POWER OF DIRECTION AND THE FREEDOM OF CHOOSING WHETHER AND WHEN TO WORK

One of the peculiarities of platform work – arising both doubts about qualification and reflections on the evolution of the work relationship towards greater freedom and autonomy, is represented by the ability to accept or not the platform's request.

This is a hot topic in all European courts: just think of the contract between the Cour d'Appel of Paris and the Cour de Cassation, or the fluctuating rulings of the Italian Supreme Court. The European Court of Justice in the Yodel Delivery Network Ltd case of 22 April 2020, C-692/19, after reiterating that the possibility of using substitutes or accepting or not the various tasks offered are incompatible with the status of employment relationship, specifies, however, that the dependent nature of the relationship is excluded as long as "*the independence of this person is not fictitious*" (p.12). Based on this, the Italian Court of Palermo ruled that the rider's freedom to accept or not the tasks offered by the Glovo platform was purely fictitious to the extent that the worker is not really free to choose not only *when* but also whether the service is actually *due*, being able only to apply for the shifts made available by the platform and distributed on

[50] Cour de Cassation, Chambre Sociale, 374, 4 March 2020, in *RDT*, 12/2018, p. 820, with *Observation* by T. Pasquier. According to the Court, when the driver logs in to the *Uber* platform, he/she is integrated into an "organized service".

the basis of a score, determined, among other things, precisely on the basis of the worker's conduct (including the refusal of a booked shift). Furthermore, the rider would suffer from "atypical" disciplinary sanctions, consisting of a classification penalty and, at most, disconnection from the platform.

Similar arguments were used, in a completely different regulatory context, by the Australian Fair Work Commission in a *Foodora* case. The Commission found in the metric used by the "*batching system*", which classifies the worker's performance, a sufficient reason to qualify the rider's relationship as employment.

Now, while it is certainly true that the worker is (at least in part) conditioned in his/her freedom of choice by the criteria established by the platform (which assigns the slots based on the score assigned by the algorithm), I think we cannot automatically deduce the full subjection of the provider to hetero-direction (at least in systems, such as the Italian one, in which the index of subordination coincides with the subjection to direction power). The exercise of direction power in fact concerns the conformation of the service, as well as the determination of its implementation methods, the choice of the place and times of execution, and implies the full subjection of the provider to the employer's power. Unlike the assembly line worker, referred to in the sentence of the Court of Palermo, who has no possibility of escaping the direction power, the rider can refuse to accept a call, or discard an already booked service, even though the exercise of this freedom impairs scores and, therefore, better future job opportunities. The argument used by the Court apparently has a high degree of plausibility, because it uses the traditional method of verifying the actual methods of carrying out the service which, not only in the Italian legal reality, are used by jurisprudence and doctrine to identify the real nature of the work relationship.

Ultimately, the Court of Palermo seems to follow a path that could be summarized in the following terms. When a self-employment contract is stipulated between the parties (in this case a project-based collaboration) negotiations are modulated on the autonomous nature of the service. However, the employer – through the imposition of specific directives on the content of the service or the obligation to carry out the work activity at times other than those contained in the contract – actually modifies the content of the contract itself. And this change involves its reclassification as an employment contract. *Mutatis mutandis*, the situation would be the same even in the case of an abstract freedom not to perform the service and to choose whether and when to work,

which would correspond to a completely different factual reality. The freedom of choice may not be concretely exercised, because the worker would in any case be "forced" to work according to the methods imposed by the algorithm, with the consequence that said freedom would be only "apparent and fictitious".

In order to get to the conclusions of the Court, we should fully equate the situation in which it is the client/employer who unilaterally imposes different methods of carrying out the relationship – incompatible with the autonomy of the service – with the one where the content of the contract is conditioned by choices of the worker or by his/her performance or by choices external to the client. This would also lead us to further consequences. Whenever the provider is influenced in various ways in carrying out the work, due to his/her economic weakness, because he/she has no employment alternatives, because he/she is in a state of economic dependence, etc., the commentator should necessarily consider the case as employment, even in the absence of behaviours on the part of the employer that are such as to integrate the logical-legal scheme of employment.

In my opinion there is a stretch in this argumentation. In typically capitalist production systems, such as that of platforms, the use of other people's work and the exercise of prerogatives in the broad sense related to "direction" and "control" are not limited to the context of employment relationships. However, they concern with variable intensity all long-term contractual relationships maintained by the company with its suppliers, with mechanisms characterized by economic dependence, information asymmetry, obligation to comply with technical standards, imposition of sales prices, compliance with clauses relating to guarantee of a certain volume of business requiring the collaborator to maintain a certain volume of trade with a preferred partner, etc. This obviously does not mean that all these relationships can be referred to the scheme of employment in the technical-juridical sense. It means, rather, that even accentuated forms of organizational pre-eminence of the stronger contractor are present in the vast area of relationships that a self-employed worker maintains with a (sole or prevalent) privileged client, in the context of relationships variously denominated in terms of "imperfect subjection", "economic dependence", "quasi-hierarchy", "parasubordination", etc.

7. THE EU DIRECTIVE ON PLATFORM WORK

The Digital Platforms Directive introduces a dual definition of worker: on the one hand, a "person performing platform work", meaning "any individual performing platform work, irrespective of the nature of the contractual relationship or its designation by the parties involved (art. 2, co. 3). On the other hand, "digital platform worker", to be understood as "any person performing platform work who has an employment contract or is deemed to have an employment relationship as defined by the law, collective agreements or practice in force in the Member States with consideration to the case-law of the Court of Justice" (art. 2, co. 4).

The first definition expresses a very broad work protection strategy, proposing for the first time a notion of personal work and extending protections beyond the confines of subordination. In this case, the Directive attributes the protections relating to Algorithmic Management to the employment relationships of all platform workers (articles 8-11 of the Directive). The European Commission has moved in a similar direction on the application of competition law to collective agreements concerning the working conditions of self-employed workers in conditions of economic dependence[51].

The second definition concerns employees, whose qualification is implemented through the presumption of employment relationship, which we are now going to talk about.

The co-presence of these two definitions of worker expresses a new complexity in the *montage* of the legal categories guiding labour law[52]. Thanks to the first definition, that of personal work, the axiological-normative discourse is not limited to the employment status, but opens up to universalistic justifications linked to the use of new conceptual categories. The notion of personal work is one of these new legal concepts, but other research paths are possible. Think, for

---

[51] *Communication from the commission Guidelines on the application of Union competition law to collective agreements regarding the working conditions of solo self-employed persons*, 2022/C 374/02.

[52] Cfr. Punta, R., del (2022). Diritto del lavoro e valori, in Del Punta, a cura di, *Valori e tecniche nel diritto del lavoro*, Florence University Press.

example, of the category of "relational" contracts[53], of the notion of economic dependence to select protections to be distributed beyond the sphere of subordination[54], or of the universalistic conception of social rights promoted by the ILO, regardless of the qualification of the work relationship.

On the other hand, the European legislator intends to facilitate the qualification of employee through a legal presumption, combating the abuse of the qualification of self-employed worker on the part of platforms, also due to the unfair competitive advantage that this practice entails. A similar competitive argument is raised both by the recitals of the European Directive and by the California Supreme Court which, in the *Dynamex* case, expressly refers to the "unfair competitive advantage the business may obtain over competitors that properly classify similar workers as employees"[55].

Basically, the supranational legislator, as well as the European Court of Justice (for example in the *FNV*[56] ruling), evokes "bogus self-employment" as a concept characterized by the simulation of relationships which, on the basis of consolidated jurisprudential criteria, must be referred to the sphere of employment. The Directive is then concerned with establishing some principles for a "correct determination of the employment status" by stating that "Member States have adequate and effective procedures to verify and guarantee the correct determination of the employment situation of persons performing platform work". Furthermore, the art. 4, paragraph 2, provides that the determination of the existence of an employment relationship is mainly based on the "facts relating to the actual performance of work, including the use of automated monitoring or decision-making systems in the organisation of platform work, irrespective of how the relationship is classified in any contractual arrangement that may have been agreed between the parties involved".

It is often difficult for persons performing digital platform work to have adequate access to the tools and information necessary to assert before a

---

[53] Van Gehuchten, P.-P. (2016). Aborder les formes juridiques du travail (indépendance ou salariat) par le prisme de la notion de « contrat relationnel »? Propos d'étape, in *Revue interdisciplinaire d'études juridiques*, 1, Vol. 76, p. 119 ss.

[54] Perulli, A. (2002). *Study on economically dependent work/parasubordinate (quasi-subordinate) work*, EU Commission, Brussels, 2002.

[55] *Dynamex*, 416 P. 3d1.

[56] ECJ, 4th Dec 2014 C-413/13, *FNV*, EU:C:2014:2411.

competent authority the actual nature of their contractual relationship and the rights deriving from it. Furthermore, the management of persons performing platform work through automated decision-making and monitoring systems is characterized by an opaque flow of information on the part of the digital platform. These characteristics of digital platform work perpetuate the phenomenon of misclassification as bogus self-employment, thus hindering the correct determination of employment status and access to decent living and working conditions for digital platform workers.

Such observations are certainly not new. In recent years, most labour law systems have acquired different methodologies in order to revisit the categories of labour law for the purposes of correct and effective qualification of the relationship. This occurred both in civil law and common law systems, with significant elements of convergence ranging from the aforementioned denial of any relevance to the *nomen iuris* of the contract in favour of the actual development of the relationship[57], to the valorisation of techniques or indices (even different from traditional ones) that extend the scope of labour law, to tests highlighting the economic and organizational reality in which work is integrated[58], up to the use of legal presumptions[59].

The choice to use a relative legal presumption of employment relationship therefore represents the qualifying point of the directive, and constitutes – at least in line of principle – an important innovation both from the point of view of EU law and for the repercussions that this provision will have on individual national regulations. The use of legal presumptions was indicated by the ILO in its Recommendation no. 198/2006 on employment relationship as one of the tools to ensure the correct qualification of work relationships in order to remove uncertainty regarding the existence of an employment relationship and, therefore, "guarantee fair competition and effective protection of workers in an

---

[57] The objective is to bring out the "true agreement", establishing the simulation, as in the United Kingdom Supreme Court case, *Autoclenz Limited v Belcher and others*, 27 July 2011.

[58] In U.K. "*integration test*" ed "*economic reality test*", in Francia il service organisé, in Germania *l'eingliederung in den betrieb.*

[59] E.g. in Belgium the law has created a presumption of employment relationship for certain economic sectors (see references in the text).

employment relationship in a manner appropriate to national law or practice" (as stated in the recital)[60].

From the point of view of comparative law, however, we should observe that the majority of Member States (seventeen) have not adopted the legal presumption technique, while the remaining ten Member States have legal presumptions applicable to all employment relationships (Croatia, Estonia, Greece, Malta, Holland, Portugal, Slovenia, Spain) or to particular groups or sectors (Belgium, France)[61]. Furthermore, Spain has recently adopted an *ad hoc* legal presumption for platform workers, but the rule, due to its peculiar formulation, does not seem useful at all. The Spanish experience in the matter of legal presumptions is indeed rather unsuccessful, as regards the general presumption – to the point of doubting whether it is a real legal presumption considering the essentially tautological nature of the norm: "*the employment contract (...) will be presumed to exist between anyone who provides a service on behalf of and within the scope of organization and direction of another and anyone who receives it in exchange for remuneration to the former*."[62]. Moreover, it might be considered unsuccessful even as regards the specific presumption introduced by the *Ley rider* 12/2021, which paradoxically places the burden of proof on the worker, who must provide elements regarding the existence of directive, organization and control power, directly, indirectly or implicitly exercised by the platform through an algorithm[63].

The result of the comparative analysis on the effects of conditional legal presumptions is not positive. The allegation and proof of facts relating to subordination which, in the case of platform work, can be particularly difficult, contradicts the need for procedural simplification of the legal qualification of the work relationship.

---

[60] ILO, Regulating the Employment Relationship in Europe: A Guide to Recommendation No. 198 (European Labour Law Network, 2013), 28-30.

[61] Cfr. B.Waas, B., and Heerma van Voss, G. (eds) (2017). *Restatement of Labour Law in Europe: the Concept of Employee*, Vol. I, Oxford, Hart.

[62] "El contrato de trabajo (...) se presumirá existente entre todo el que presta un servicio por cuenta y dentro del ámbito de organización y dirección de otro y el que lo recibe a cambio de una retribución a aquél".

[63] Cfr. Olivieri, A. (2022). La presunzione di subordinazione nel lavoro tramite piattaforma: dall'esempio spagnolo alla proposta di Direttiva europea. Quasi todos caballeros? in *LDE, 2*, p. 2 ss.

In addition to the findings already made regarding the Spanish law, the legal presumption provided for by the Belgian system also raises many doubts because it requires verifying *ex ante* the existence of all the criteria envisaged by the notion of subordination, thus resulting in a truly useless exercise. The same applies to the Portuguese system, where a previous "pre-digital" legal presumption, difficult to adapt to platform work, was substituted by Law 13/2023 (art. 12-A, labour Code).

The new Portuguese conditional legal presumption follows the logical-legal scheme of the previous draft of the European Directive: six indicators of employment relationship are identified (including the exercise of direction and control power, the reduction of the provider's autonomy in the organization of work and the exercise of disciplinary power), conditioning the activation of the legal presumption on the occurrence of at least two of these indicators.

The same criticisms that the doctrine had addressed to the original proposal for a European Directive on platform work apply here. Having conditioned the presumptive effects on the proof of facts inherent to the notion of subordination risks producing poor or even counterintuitive results[64], to the extent that on the one hand, the worker must allege and prove the existence of presumptive facts which, in all jurisdictions, would allow the judge to qualify the relationship as employment. On the other hand, it enables the platform to overturn the presumption where, in a normal procedural dynamic, once the existence of the subordination indices has been proven and the judge's conviction has been formed, the qualification of the relationship can no longer be questioned. Furthermore, the first ruling of the Portuguese Court relating to *Uber Eats* (February 2024), albeit being in favour of the worker, confirms the validity of the criticisms, to the extent that the work relationship with the platform has been classified as employment because five parameters of employment relationship out of the six provided for by the law were satisfied[65].

---

[64] Cfr. Stefano, V., di (2022). The EU Commission's proposal for a directive on Platform Work: an overview, in *Italian Labour Law e-Journal*, Vol. 15, p. 1 ss.

[65] Cfr. Teresa Ribeiro, a. (2024). An Employment Presumption for Platform Work. The Portuguese experience, in *Global Workplace Law & Policy*, 18/03/2024, p. 4.

The overall assessment is therefore very problematic[66], even if many look favorably on the adoption of the legal presumption[67]. In the recitals of the European Directive, the choice of the presumption is motivated by the virtues of such a measure to create "an effective procedural facilitation for persons performing platform work when ascertaining the correct determination of their employment status". These alleged advantages are yet to be proved: the legal presumption, especially if it is a presumption conditioned on the verification of certain circumstantial facts of subordination, is certainly not a *panacea* against all evils of legal qualification, nor can it be said *ex se* to be an efficient tool for guaranteeing workers' rights, as the Directive actually seems to consider.

8. A CRITIQUE OF THE LEGAL PRESUMPTION OF THE EU DIRECTIVE ON PLATFORM WORK

Let us now try to delve into the more technical aspects of the provision, starting from a consideration: the legal *montage* concerning the legal presumption is different compared to the previous drafts of the Directive. The previous version identified seven presumptive indices, some intrinsic to the work performance, others extrinsic (such as that indicated in letter e), relating to the "effective limitation of the possibility of building one's own clientele or performing work for third parties"). The presence of at least three out of seven indices *prima facie* placed the case within the scheme of employment relationship. Since it was a rebuttable presumption, the platform could refute this qualification on the basis of the qualification indices of employment relationships specific to each system, overturning the presumption[68]. The wisest doctrine, then followed by the European Parliament, had proposed adopting a presumption of fact, not conditioned by the verification of significant "facts" of the employment relationship status, shifting

---

[66] Hießl, C. (2024). Case Law on the Classification of Platform Workers: Cross-European Comparative Analysis and Tentative Conclusions, *Forthcoming, Comparative Labour Law & Policy Journal*, March 12, available at SSRN: https://ssrn.com/abstract=3839603 or http://dx.doi.org/10.2139/ssrn.3839603

[67] Kullmann, M. (2022). 'Platformisation' of work: An EU perspective on Introducing a legal presumption, in *ELLJ*, Vol. 13(1), p. 66 ss.

[68] The proposal for a rule (art. 3a, 3, a) stated: "If the digital work platform claims that the contractual relationship involved is not a work relationship as defined by the law, the collective agreements or the practices in force in the Member State in question", taking into account the jurisprudence of the Court of Justice, the burden of proof falls on the digital work platform".

the burden of proof onto the platform-employer, based on the demonstration of the lack of those same indices[69]. The unconditional presumption would have really been beneficial to the weaker party in the relationship, affecting the disparity in contractual power and the information asymmetry between the parties, decisively directing the qualification in the direction of subordination, unless the platform proves otherwise.

However, this solution was not accepted, and the Commission's regulatory strategy followed a regulatory model similar to the Spanish one, where the presumption of employment relationship appears based on a sort of tautology: "The contractual relationship between a digital labour platform and a person performing platform work through that platform shall be legally presumed to be an employment relationship when facts indicating *control and direction*, according to national law, collective agreements or practice in force in the Member States and with consideration to the case-law of the Court of Justice, are found." (Art. 5, emphasis added). Since the "facts" indicating the existence of control or direction are constitutive of the (legal or jurisprudential, depending on the different regulatory systems) notion of subordination, the statement sounds more or less in these terms: the work relationship is supposed to an employment relationship when it is an employment relationship.

The formulation of the rule raises multiple critical considerations. On the one hand, it appears excessively generic in referring to "facts indicating control or direction" compared to previous versions which bore specific elements ("facts" selected from the undifferentiated variety of the real world), which triggered the rebuttable presumption of employment relationship. On the other hand, the formulation proves to be rather rigid and excessively focused on the elements of *control and direction* as presumptive indices of employment relationship. It is true that the disjunctive "or" present in the norm, unlike the "and" of the *recitals* could be valorised during the transposition in order to lighten the evidentiary burden relating to the significant "facts" of "control" or "direction". However, control and direction are, in the legal tradition of civil law legal systems,

---

[69] Cfr. Aloisi, A., Rainone, S., and Countouris, N. (2023). An unfinished task? Matching the Platform Work Directive with the EU and international "social acquis", in *ILO Working papers*; ma già Stefano, V., di (2022), The EU Commission's proposal for a directive on Platform Work: an overview, in *Italian Labour Law e-Journal*, Vol. 15, p. 1 ss.

inextricably linked, or even indicative of the same "directive" conception, as demonstrated by the *control test* of common law systems[70].

By delimiting the scope of relevance of the possible abstractly symptomatic "facts", which must necessarily be attributable to the concept of "control power" or "directive power", the Directive, *de facto*, precludes the possibility of adapting the notion of subordination to the current technological evolutionary context, which in all jurisdictions – not just European ones – pushes the legislator (and/or jurisprudence) to go beyond subordination, adopting *purposive* interpretations that largely disregard the technical inclination of work[71]. The cultural background emerging from the logical structure of the norm therefore expresses a narrow, very traditional – I would say "Fordist" – conception of the notion of employment, understood as subjection to the typical powers of the employer. But it is exactly these historically determined forms of subordination that are being called into question by technological evolution, which – especially in the case of digital platforms – require innovative legal solutions, and certainly not returns to the past. As a consequence, the formulation of the presumption – in the univocally directive terms of *command and control* as per the Directive – conflicts not only with the social reality, but with the more advanced guidelines of the ECJ itself, which, in the *Yodel Delivery* case downgraded the "directive" component of subordination to the advantage of a renewed attention to the economic dimension of the employment contract[72].

Thus said, we still need to understand the meanings and limits of a formulation which appears, as we said, substantially tautological. First of all, we are dealing with the issue of defining the "facts" that can be considered as legally relevant for the purposes of the proof. In this case the "facts", although not specifically identified by the law, are still institutionally defined with reference

---

[70] In particolare in US, UK, Canada and Australia. Cfr. Ready Mixed Concrete (South East) Ltd v Minister of Pensions and National Insurance [1967] EWHC QB 3 [1968] 2 QB 497; Montreal v Montreal Locomotive Works (n 22); Stevens v Brodribb Sawmilling Co Pty Ltd (1968) 160 CLR 16.

[71] Perulli, A. (2020). The legal and jurisprudential evolution of the notion of employee, in *ELLJ*, Vol. 11, Issue 2, p. 117 ss.

[72] Ord., 22 avril 2020, C-692/19; sul diverso approccio della Corte di giustizia rispetto alle giurisdizioni nazionali, ed in particolare francese, cfr. F. Perrone, *La subordination-dépendance en Europe: la protection des droits fondamentaux des travailleurs à la lumière des contraintes définitionnelles du droit de l'Union européenne*, in Revue de droit du travail, 2020, p. 448 ss.

to the legal categories of "control or direction". It is this categorical reference that brings the discussion on the "facts" back to a precise legal relevance as "factual presuppositions" of the presumption of employment relationship. It is difficult to imagine that these "facts" might be different from those normally relevant in order to identify subordination in the traditional sense of subjection to hetero-direction: the selective criterion of the "facts" that will have to be attached and, in some measure, proven to trigger the rebuttable presumption, is nothing more than the "facts" constituting the legal category of subordination. However, in order to trigger the legal presumption, it requires "facts" directly referable to the command and control of the platform. For this reason, the burden of attaching and proving facts pertaining to control and direction risks making the claimant's task more difficult, and not easier, considering the usual set of legal and jurisprudential indices which, depending on the different legal systems, connote subordination without necessarily requiring proof of the exercise of direction power and control power: working hours, stable inclusion in the organization, continuity of performance, etc. *The claimant will not be able to attach and prove symptomatic indices other than control or direction*. In the selection of the "facts" it will be possible, if necessary, to think of some newly minted presumptive "facts", or of an adaptation of the presumptive indices to the organizational and productive context of the platform, expressive of what has been defined as a "directive control power"[73]. For example, "facts" that may indicate control or direction might be: the use of algorithms or other digital technologies functional to creating forms of technological/IT subordination[74]; the use of geolocation tools for the purposes of continuously monitoring the places where the worker is located; the use of control systems conveyed by an online connection to verify the manner and times of execution of the assigned task[75]; the adoption, on the part the platform, of rating systems which may vary the quality of the tasks entrusted, but also forms of performance control or the exercise of disciplinary prerogatives (such as lowering the rating) or the power of

---

[73] Tebano, L. (2020). *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, p. 239.

[74] Cfr. Zappalà, L. (2021). Le condizioni di lavoro nelle piattaforme: quali strategia europea di tutela del lavoro digitale? in *Professionalità studi*, IV, 1, p. 4 ss.

[75] Cfr. *Work on-demand via apps*, in Borelli, S., Brino, V., Faleri, C., Lazzeroni, L., Tebano, L., and Zappalà, L. (2022). *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Giappichelli, Torino, p. 233.

withdrawal (dismissal due to poor performance due to a plurality of converging negative ratings)[76].

We may specularly apply similar critical considerations to the proof to the contrary. According to the Directive, the application of the legal presumption should not automatically lead to the reclassification of platform workers, which is in accordance with the civil law systems general principle, according to which what is (or is presumed to be) proven can be countered with a proof to the contrary.

The rule is formulated in these terms: "Where the digital labour platform seeks to rebut the legal presumption, it should be for the digital labour platform to prove that the contractual relationship in question is not an employment relationship as defined by the law, collective agreements or practice in force in the Member States". If the worker must provide elements that allow factual confirmation of the control or direction, the platform, in order to overturn the presumption, will in turn have to prove the non-existence of such facts. This is a negative test (absence of control, absence of direction) that is pretty similar to the one any employer must prove if he/she wants to counter a request for requalification of the work relationship based on the presence of indices of employment relationship. However, other indicators such as, for example, the lack of stable inclusion of the provider in the organization of the platform, the discontinuity of the service, etc, may not be relevant as regards the test. Conversely, elements such as the absence of a rigid time predetermination of the performance, or the absence of geolocalisation tools – indicative of the worker's autonomy in the spatio-temporal organization of the activity – may be valorised when proving the contrary. Further, what may also be relevant is the evidence of the absence of *customer satisfaction* practices which involve the acquisition of information relating to performance through tools (such as questionnaires, surveys, interviews, etc.) intended for a different purpose (the construction of the company's reputational capital), but whose effects can be compared to those of remote control of workers. The issue did not escape the attention of the ECJ in the *Uber* case, where the Court found that through the evaluation of customers, the Company exercised control over the quality of drivers as well

---

[76] Cfr. Rating, in Borelli, S., Brino, V., Faleri, C., Lazzeroni, L., Tebano, L., and Zappalà, L., *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, cit., p. 179.

as the behaviour of the latter[77]. As a consequence, the doctrine considered as applicable to platform work the rules limiting the power to remotely control the performance. Furthermore, in order to overturn the presumption, the platform may prove the guarantee of the worker's freedom to choose whether and when to perform the service (freedom considered by the drafters of the Directive as a characteristic of true self-employment). However, this very element must be analyised with particular attention. In fact, if on the one hand it is possible to argue that such freedom is incompatible with an employment relationship (the *mutuality of obligation* test used by English jurisprudence also supports this), it is also true that this freedom can be fictitious if the client reduces the job opportunities of the provider, "sanctioning" in an atypical way the fact of having evaded the service.

9. THE BAN TO PENALISE THE RIDER THROUGH REPUTATIONAL ALGORITHMIC *RANKING*

The considerations above must now be compared with the regulatory framework as defined by law no. 128/2019, inexplicably ignored by the Court of Palermo. We are referring to the legislative intervention which – having acknowledged the excessive contractual power of the platform and the consequent operativeness of algorithmic regulation systems of the rider's behaviour and performance – sanctioned the prohibition on using worker ranking systems to exclude the provider from the job market managed by the platform, or to penalize him/her in the allocation of job opportunities. Such behaviour of the platform (adopted based on its own algorithm) is expressly prohibited by the art. 47-*quinquies*, of the legislative decree lgs. 81/2015, which establishes as illegitimate the exclusion from the platform and the reductions in job opportunities attributable to the rider's failure to accept the call. The legislator, by intervening on the controversial issue of exclusion from the platform and on the reductions in job opportunities attributable to the rider's failure to accept the call, and by sanctioning these practices as illegitimate, therefore fundamentally eliminates the problem of the (self-employed) rider's freedom to decide whether and when to work. Consequently, the platform can

[77] CJEU, 20 December 2017, C:434/15, *Asociacion Profesional Elite Taxi c. Uber Sistems SpainSL*, point 39.

no longer sanction the worker who refuses the call by excluding him/her from access to subsequent job opportunities, or by denying him/her entry to "reward" levels with better contract conditions, or by reducing job opportunities by banning the provider from "priority access" based on the statistics on absence rates, thus implementing demotions, "deactivations", etc.

The norm therefore guarantees the effectiveness of the main guarantee of (albeit limited) autonomy of the provider, i.e. the freedom to respond or not to the offer and to "show up" at work to provide the service (without having to justify and without suffering assessments and/or "atypical sanctions" on the part of the platform). Matter-of-factly, it is this full freedom of the provider that characterizes the relationship as autonomous (although hetero-organized) due to the lack of the mandatory requirement of the service and consequent full subjection to the employer's directive power.

The legislator, however, has not provided for a specific sanction in case of non-compliance with the ban; therefore, the applicable regulations remain to be established if the client violates the prohibition involved, and effectively excludes the provider from the platform or reduces work opportunities in the event of non-acceptance of the job. First of all, the provider will be able to resort to the general principles regarding termination of the contract for non-fulfilment (art. 1453 of the civil code), requesting its fulfillment (consisting in the client's acceptance of the job offer, regardless of any previous failure of the provider to respond to the calls) or, failing that, the termination, without prejudice in both cases to compensation for the damages sustained[78]. But that's not all. By applying to the above-mentioned case the general rule-clause aimed at repressing the abuse of economic dependence in the field of self-employment (art. 3, law no. 81/2017), it can be reasonably believed that the unmotivated and without-notice exclusion from the platform on the part of the client constitutes an arbitrary interruption of the ongoing contractual relationships, integrating a case of abuse of economic dependence. As a consequence, the provider will be able to invoke injunctive protection, while any clause providing for this faculty of the client will be devoid of effect and the provider will be entitled to

[78] Cfr. Raimondi, E. (2019). *Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie*, in *L&L Issues, 2*, Vol. 5.

compensation for damages, also promoting a conciliation attempt through the authorized bodies[79].

Apparently, therefore, the violation of the art. 47-*quinquies* has nothing to do with the qualification of the relationship in terms of subordination, as it is a prohibition whose non-observance does not in any way determine the automatic re-qualification of the employment contract. However, the "remedy" in the event of violation of the provision may be represented by the judicial request for the recognition of a work relationship hetero-organized by the client pursuant to art. 2, paragraph 1, with full application of the regulation of the employment relationship. In other words, such remedy would be the qualification of the relationship in terms of subordination (art. 2094 civil code) where the conditions are met, to the extent that the disadvantage caused to the rider by a behaviour consistent with the autonomous nature of the relationship (at least in its "genetic" phase) brings down the barrier that does not allow the relationship to be classified as employment. In fact, if – following the Court of Palermo's argument – the client excludes the rider from the platform or reduces his/her work opportunities, atypically "sanctioning" having evaded the service, a typical element of the self-employed employment relationship is missing, at least with respect to that autonomy in the genetic phase which the Court of Cassation, in the case of the Foodora riders, believes must be complete, due to the right of the worker whether or not to perform the service (point 33). Consequently, the platform may well have abusively used the self-employed rider work relationship scheme, as provided for by law no. 128/2019, in order to disguise a different relationship, with a different legal nature. Given that in the functional phase the platform certainly and substantially determines the methods of execution of the relationship, the latter will have to be carefully scrutinized and possibly requalified in the sense of hetero-organization. It may as well be considered as employment, where the judge concretely ascertains the existence of a real subjection to hetero-direction according to the normal criteria developed by jurisprudence, in light of the rule of effectiveness of protection,

---

[79] Cfr. Perulli, A. (2017). Economia digitale e qualificazione dei rapporti di lavoro, in Alessi, Barbera, and Guaglianone (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Cacucci editore, Bari, p. 430.

functional to "the purpose of combating the abusive use of contractual "shields" pursued by the legislator"[80].

Similar findings are completely absent in the sentence of the Court of Palermo, but they may, perhaps, be used on a future occasion, to make the motivation of the decision more in line with the data of positive law.

10. ALGORITHMIC DISCRIMINATION

Among the social pathologies of the platforms we certainly have the possible discrimination achieved through the functioning of the algorithm. Many empirical studies prove how the algorithms used by the platforms, far from being "neutral" and free of prejudice, produce discriminatory effects to the detriment of female workers, especially in matters of remuneration, and so on. Given that the platform entrusts the determination of compensation levels to algorithms, the systematic reduction of incomes received by female workers raises the issue of the adequacy of European anti-discrimination legislation to combat these practices[81]. The anti-discrimination legislation and in particular Directive 2010/41/EU, directly applicable also to self-employed workers, may have a significant impact with reference to platform work, both from the point of view of access to job opportunities both for equal treatment in the contractual conditions applicable to the workers involved. However, this has not produced significant results in terms of application so far[82]. It is therefore necessary to deepen the knowledge of the apparently neutral mechanisms adopted by the platforms that produce indirect discrimination, as well as workers selection criteria, performance evaluation systems by users and compensation levels. Subsequently, we need to verify how all these elements retroactively affect the algorithms' *decision-making*, in order – also by using statistical data – to intervene with corporate-decision-correcting tools to remedy the discriminatory effects produced by artificial intelligence.

---

[80] Cass. 24 gennaio 2020, n. 1663, punto 43, che richiama Corte cost. n. 115 del 1994.

[81] Cfr. Kullmann (2018). Platform Work, Algoritmic Decision-Making, and EU Gender Equality Law, in *Int. Jour. Comp. Lab. Law and Ind. Rel., 34*, p. 1 ss.

[82] Alessi, C. (2019). Lavoro tramite piattaforma e divieti di discriminazione nell'UE, in Alessi, C., M. Barbera, M., and Guaglianone, L., (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Cacucci, Bari.

Particular attention is due – because of its connections with the riders' working methods – to the issue of the possible discriminatory effects of *customer satisfaction* practices which allow platforms to acquire evaluations of the service and the performance provided by the worker (for example through the rating system) and, in the event of low customer satisfaction, to interrupt the collaboration by disconnecting the account. Practices of this type, widespread for example in the production system of Uber services, raise issues of privacy protection (when the evaluation produces information which the platform comes into possession of and can "process"). Further, we might be dealing with possible "indirect control" over the performance (since the assessment system allows an appreciation of the work activity "mediated" by the judgment of users even in the absence of control by the company management and physical organizational integration), and the exercise of disciplinary prerogatives in a broad sense (the disconnection of the account as the functional equivalent of a disciplinary dismissal), as well as, indeed, discriminatory practices.

From this last point of view, we should observe that the discriminatory effect can arise from a negative assessment of the service provided on the basis of elements which do not concern the service at all, but are due to the user's prejudices towards the worker (for example example, racial prejudice against a black driver or rider). In this way, reputational *customer satisfaction* systems are characterized as potentially suitable tools for "channeling" the user's discriminatory attitude within the work relationship (therefore a "third" element which is brought back into the context of the relationship thanks to the satisfaction assessment techniques implemented by the company), producing consequences in the broad sense of "sanctions". As an example, the disconnection of the account can be regarded as the effect of a discriminatory mechanism to the detriment of the provider, and not as a legitimate reaction of the platform to a non-fulfilment, or imperfect performance, by the debtor.

Furthermore, the existence of indirect discriminatory practices in the field of work (including self-employment) via platforms is now well established. Numerous studies conducted on service platforms such as Uber or Lyft reveal significant evidence of racial discrimination, which sees black riders forced to face up to 35% longer waiting times and frequent cancellations compared to white riders, with worse effects in low-density areas, where it is more difficult

to find drivers[83]. The same Italian experience, with reference to Foodora riders, has showed phenomena of discrimination for *trade union reasons*, with providers who unjustifiably suffered the deactivation of the account by the client, accompanied by the establishment of *fictitious* unions with the sole purpose of maintaining control over workers and inhibiting collective claim activities.

The imperative of indirect non-discrimination therefore stands as one of the main barriers against arbitrary algorithmic regulation. The value of this principle in the context of platform work can be useful to counteract discriminatory practices based on gender factors, but also trade unions, race, etc., which find fertile ground in the *Gig economy* on equal terms, if not more, than what happens in traditional working contexts. The topic falls within an even broader area, that of the digital economy and Artificial Intelligence, which, as the European Commission recognizes in the Communication of 5 March 2020 (*A Union of Equality: Gender Equality Strategy 2020-2025*), risks intensifying gender inequalities: "*Algorithms and related machine-learning, if not transparent and robust enough, risk repeating, amplifying or contributing to gender biases that programmers may not be aware of or that are the result of specific data selection". Consequently, the Commission's White Paper on this matter sets out a series of European strategies based on "EU values and fundamental rights, including non-discrimination and gender equality*"[84].

With an important ruling, the Court of Bologna ascertained the discrimination implemented by the system, governed by an algorithm, which regulates the conditions of access to work sessions, accepting the appeal of the trade union organizations. The latter claim that the platform, by sanctioning with the loss of their *ranking score* the riders who do not respect work sessions, penalizes all legitimate forms of abstention from work (strike initiatives, collective self-defense coinciding with one's work shift, other legitimate causes such as illness, needs related to a minor child, etc.), thus resulting in the demotion to the bottom of booking slots and limiting future job opportunities.

---

[83] Ge, Y., Knittel, C.R., MacKenzie, D., and Zoepf, S. (2016). Racial and Gender Discrimination in the Transportation Network Companies, *NBER Working Paper Series National Bureau of Economic Research* 1050 Massachusetts Avenue Cambridge, October.

[84] Brussels, 5th March 2020 COM(2020) 152 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Union of Equality: Gender Equality Strategy 2020-2025.

The Court ascertained "that joining a collective abstention from work initiative is likely to jeopardize the rider's statistics, since the rider who joins a strike, by abstaining from work and therefore by not participating in a booked session, will be inevitably suffer a decrease in its score in terms of reliability, and possibly also in terms of participation, whereby the booked session falls in the 8.00-10.00 pm time slot on the weekend". In essence, if the rider joins a strike, and does not cancel the booked session in good time, "he/she risks seeing his/her statistics worsen and losing any position held in the priority group, with the related advantages".

There is no doubt, in the current state of jurisprudence, that the exercise of the right to strike, deriving from trade union affiliation, constitutes a possible factor of indirect discrimination, given that said affiliation "represents the pragmatic profession of an ideology other than the religious, characterized by specific reasons of belonging to an organism socially and politically qualified to represent opinions, ideas, beliefs susceptible to protection as the object of possible prohibited discriminatory acts". The rider who, by participating in a strike, sees his/her reputational statistics penalized regardless of the reasons for his/her conduct because the platform does not know and does not want to know the reasons why the rider cancels his/her booking or does not fulfil a booked and not canceled session", suffers indirect discrimination, by applying an apparently neutral provision (the contractual regulation on the early cancellation of booked sessions) which determines a particularly disadvantageous situation for a category of workers.

Unlike the case of direct discrimination and harassment, indirect discrimination, by broadening the scope of the employer's responsibility, admits – as a counterweight to this lengthening of the causal chain – justifications and among these the so-called market defenses[85]. However, we should observe that the standard of control of this justification is particularly severe, to the extent that it requires (proof of) the necessity of the market and/or economic needs of the company and the proportionality of the means employed, according to a test set out by the Court of Justice (*Bilka* and *Nimz* cases). In light of such a balance,

---

[85] Cfr. Barbera, M. (2019). Principio di eguaglianza e divieti di discriminazione, in Barbera, M., and Guariuso, A., a cura di, *La tutela antidiscriminatoria, fonti, strumenti, interpreti*, Giappichelli, Torino, p. 59 ss.

we may reasonably doubt that the algorithmic choice is not only responsive to the technical-organizational needs of the company, but also adequate and proportionate, and that other solutions involving a reduction in the degree of exclusion of protected subjects were not feasible. The algorithm was therefore reprogrammed, eliminating the discriminatory mechanism which was evidently unnecessary for the production activity of the platform.

We should recall that in Italy law no. 128/2019 established in art. 47-*quinquies* that exclusion from the platform and reductions in work opportunities attributable to the rider's failure to accept the call are illegitimate and, therefore, prohibited. The rule is substantial, because it fundamentally eliminates one of the main methods of control of workers who operate via a digital platform, alternative to the traditional *command and control* system based on the typical powers of the employer (direction-control-disciplinary). It consists in the exercise of a sanctioning "power" with which the platform/company implements the selection of riders, establishes their belonging (or not) to its internal labour market, and, together with digital reputation evaluation mechanisms, exercises its dominion over the riders. Consequently, the platform will no longer be able to improperly sanction the worker who refuses the call, excluding him/her from access to subsequent job opportunities, or denying him/her entry to "reward" levels with better contract conditions, or reducing job opportunities, banning the provider from "priority access" due to statistics on absence rates, implementing demotions, "deactivations", etc. Also, from this point of view, labour law exercises its function of control over the "social pathologies" of platform capitalism, requiring the algorithm to respect the dignity of the person.

BIBLIOGRAPHY

Aloisi, A., Rainone, S., and Countouris, N. (2023). An unfinished task? Matching the Platform Work Directive with the EU and international "social acquis", *ILO Working papers.*

Avent, R. (2016). *The Wealth of Humans. Work and its Absence in the Twenty-First Century*, Allan Lane, UK, p. 51.

Barbera, M. (2016). L'idea di impresa. Un dialogo con la giovane dottrina giuslavorista, in Perulli, A., a cura di, *L'idea di diritto del lavoro, oggi. In ricordo di Giorgio Ghezzi*, Wolters Kluwer Cedam, Milano, p. 688.

Barbera, M. (2019). Principio di eguaglianza e divieti di discriminazione, in Barbera, M., Guariuso, A., a cura di, *La tutela antidiscriminatoria, fonti, strumenti, interpreti*, Giappichelli, Torino, p. 59 ss.

Dagnino, E. (2015). *Uber law: prospettive giuslavoristiche sulla sharing/on demand economy*, Adapt Labour Studies, giugno.

Däubler, W. (2016). Challenges to Labour Law, in Perulli, A., a cura di, *L'idea di diritto del lavoro, oggi. In ricordo di Giorgio Ghezzi*, Wolters Kluwer Cedam, Milano, p. 503.

Davidov, G., Freedland, M., and Kountouris, N. (2015). The Subjects of Labour law: "Employees" and Other Workers, in Finkin, M., and Mundlak, G. (eds.), *Comparative Labour Law*, Edward Elgar.

Davidov, G. (2016). *A purposive approach to labour law*, Oxford University Press, p. 116 s.

Davidov, G., and Alon-Shenker, P. (2022). The ABC Test: A New Model for Employment Status Determination? *Industrial Law Journal*, *51*, p. 235.

Felstiner, A. (2011). Working the crowd: employment and labour law in the crowding industry, *Berkley Journal of Employment and labour law*, *32,* 1, p. 197.

Freedland, M. (2016). Le contrat de travail et les paradoxes de la précarité, *Rev. Dr. Trav*., p. 289 ss.

Ge, Y., Knittel, C.R., MacKenzie, D., and Zoepf, S. (2016). Racial and Gender Discrimination in the Transportation Network Companies, *NBER Working Paper Series National Bureau of Economic Research*, 1050 Massachusetts Avenue Cambridge, October.

Hießl, C. (2024). Case Law on the Classification of Platform Workers: Cross-European Comparative Analysis and Tentative Conclusions, *Forthcoming, Comparative Labour Law & Policy Journal*, March 12, available at SSRN: https://ssrn.com/abstract=3839603 or http://dx.doi.org/10.2139/ssrn.3839603

Jolly, C., and Prouet, E. (coord.) (2016). L'avenir du travail: quelles redéfinitions de l'emploi, des status et des protections? *WP, 4*, p. 42. www.strategie.gouv.fr

Kullmann, M. (2018). Platform Work, Algoritmic Decision-Making, and EU Gender Equality Law, *Int. Jour. Comp. Lab. Law and Ind. Rel*., 34, p. 1 ss.

Kullmann, M. (2022). 'Platformisation' of work: An EU perspective on Introducing a legal presumption, *ELLJ,* Vol. 13(1), p. 66 ss.

Langille, B. and Mayer-Goodman B. (2022). *Hunting for employees, employers, independent contractors, dependent contractors, independent employees, workers, and other figments of the legal imagination*, May 9, Faculty of Law, University of Toronto.

López Balaguer, M. 82018). Trabajo en plataformas digitales en Espana: primeras sentencias y primeras discrepancias, *LLI, 2,* Vol. 4, p. 53 ss. (qui p. 57).

Luhmann, N. (1973). *Il senso come concetto fondamentale della sociologia*, in Habermas-Luhmann, *Teoria della società o tecnologia sociale*, Etas Kompas, p. 14 ss.

Lyon-Caen, A. (2016). Plateforme, *Rev. Dr. Trav*., p. 301.

Mainieri, M, and Bucci, V. *Sharing Economy: la mappatura delle piattaforme italiane 2014.*

Mori, L. (2016). Rivoluzione informatica e lavoro tra XX e XXI secolo, in *Il lavoro dopo il novecento. Da produttori ad attori sociali*, a cura di Gramolati, A. and Mari, G., Firenze University Press, p. 139.

Olivieri, A. (2022). La presunzione di subordinazione nel lavoro tramite piattaforma: dall'esempio spagnolo alla proposta di Direttiva europea. Quasi todos caballeros? *LDE*, *2*, p. 2 ss.

Perulli, A. (2002). *Study on economically dependent work/parasubordinate (quasi-subordinate) work*, EU Commission, Brussels, 2002.

Perulli, A. (2017). Economia digitale e qualificazione dei rapporti di lavoro, in Alessi, Barbera, and Guaglianone (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Cacucci editore, Bari, p. 430.

Perulli, A. (2020). The legal and jurisprudential evolution of the notion of employee, *ELLJ,* Vol. 11, Issue 2, p. 117 ss.

Perulli, A. (2022). Il rider di Glovo: tra subordinazione, eteroorganizzazione, e libertà, *Argomenti di diritto del lavoro, 1*, p. 37 ss.

Perulli, P. (2018). Dopo il capitalismo, in Perulli, A., a cura di, *Lavoro autonomo e capitalismo delle piattaforme*, Wolters Kluwer-Cedam, p. 147 ss.

Punta, R. del (2022). Diritto del lavoro e valori, in Punta, del, a cura di, *Valori e tecniche nel diritto del lavoro*, Florence University Press.

Raimondi, E. (2019). Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie, *L&L Issues*, *2*, Vol. 5.

Razzolini, O. (2014). La nozione di subordinazione alla prova delle nuove tecnologie, *Dir. Rel. Ind*. p. 974 ss.

Stefano, V. di (2016). Introduction: Crowdsourcing, the Gig Economy and the Law*, Comparative Labour Law & Policy Journal*, *37*, p. 1 ss.

Stefano, V. di (2016). The rise of the "just-in-time workforce: On demand work, crowdwork and labour protection in the "gig economy", *ILO*, p. 22.

Stefano, V. di (2022*).* The EU Commission's proposal for a directive on Platform Work: an overview, *Italian Labour Law e-Journal*, Vol. 15, p. 1 ss.

Teresa Ribeiro, A. (2024). An Employment Presumption for Platform Work. The Portuguese experience, *Global Workplace Law & Policy*, 18/03/2024, p. 4.

Todolí Signes, A. (2019). Plataformas digitales y concepto de trabajador: una propuesta de interpretatión finalista, *Revista de relaciones laborales*, *41,* p. 14 ss.

Treu, T. (2017). Rimedi e fattispecie a confronto con i lavori della Gig economy, *WP C.S.D.L.E. "Massimo D'Antona",* INT - 136/2017; Id. Rimedi, tutele e fattispecie: riflessioni a partire dai lavori della Gig economy, *LD*, p. 367 ss.

Van Gehuchten, P.-P. (2016). Aborder les formes juridiques du travail (indépendance ou salariat) par le prisme de la notion de « contrat relationnel »? Propos d'étape, *Revue interdisciplinaire d'études juridiques*, *1*, Vol. 76, p. 119 ss.

Virassamy, V. G. J. (1986). Les contrats de dépendence. Essai sur les activités professionelles exercées dans une dépendance économique, *LJDJ*, Paris, p. 182.

Waas, B., and Heerma van Voss, G. (eds.) (2017). *Restatement of Labour Law in Europe: The Concept of Employee*, Vol. I, Oxford, Hart.

Winslow Taylor, F. (1960). *L'organizzazione scientifica del lavoro*, Milano, Ediz. Comunità, p. 169 ss.

Zappalà, L. (2021). Le condizioni di lavoro nelle piattaforme: quali strategia europea di tutela del lavoro digitale? *Professionalità studi*, *1*, IV, p. 4 ss.

Capítulo 16
PLATAFORMAS, ALGORITMOS Y PODER EMPRESARIAL

Daniel Pérez del Prado
Profesor Titular de Derecho del Trabajo y de la Seguridad Social
Universidad Carlos III de Madrid
https://orcid.org/0000-0001-7106-6769

1. INFORMACIÓN, DATOS Y TECNOLOGÍA COMO FUENTES DEL PODER EMPRESARIAL

La empresa, como organización, es fuente de poder. Este a su vez se articula a través de muy diversas manifestaciones, como el poder legítimo, que emana del puesto jerárquico, el poder retributivo, que deriva de la retribución; el poder coercitivo, en el que cristaliza la capacidad de sancionar; el poder personal, fruto de las propias habilidades del sujeto en su relación con otros; y el poder experto, que se sustenta en el conocimiento y la información[1]. Si nos fijamos en este último y tenemos en cuenta la importancia que ha cobrado en la sociedad digital, podemos deducir fácilmente como en la empresa de nuestros días la información es un elemento clave para el ejercicio del poder[2].

En efecto, la empresa moderna, la información tiene un papel muy destacado, hasta tal punto que su organización interna se explica en parte por la necesidad de reunirla, analizarla e interpretarla. La información es el elemento basal sobre el que articular, no solamente las decisiones clave, sino las diarias en la compañía. La dependencia que actualmente tienen las empresas de la información

---

[1] Kaufmann, A. E. (1993). *El poder de las organizaciones*, Esic, Madrid, pp. 76-78.

[2] Desde una perspectiva incluso más general se ha dicho que, en el capitalismo de la era digital, el propio sistema productivo, sustentado por los avances técnico-digitales, permite modificar y guiar las conductas, aunque también predecirlas y controlarlas. A esto se le ha denominado "poder instrumental". Zuboff, S. (2020), *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, Barcelona, pp. 471-474.

obedece a exigencias de índole tecnológica, pues la emergencia y uso de nuevas tecnologías requiere del manejo de información; de naturaleza organizativa, pues cualquier estrategia, planificación o acción ha de basarse necesariamente en la mejor información posible; y relacionadas con la coordinación, ya que una empresa eficiente requiere inexcusablemente de un adecuado nivel de coordinación entre todos los elementos que la integran[3]. La eficacia y eficiencia de la empresa depende de "la calidad de la información que consiga y de la precisión con la cual la contraste y estime"[4].

Los estudios demuestran que aquellos sujetos que ostentan una posición privilegiada dentro de una organización en cuanto al acceso y control de la información gozan de cuotas más amplias de poder. Esto es así, tanto en los supuestos más livianos, en los que el simple control sirve para colocar al resto de actores en una posición de desventaja, como en aquellos otros más graves, en los que la información es selectivamente filtrada y distorsionada para que la percepción del problema, la formación de alternativas y la evaluación de las mismas tomen un sesgo determinado a favor de quien la maneja[5].

Es más, incluso en estos casos extremos, en los que el resto de sujetos saben que no solamente se controla la información, sino que se utiliza en beneficio propio, puede resultar difícil desarrollar estrategias efectivas de acceso a la información. Los motivos son múltiples: no es fácil probar tanto la tenencia de información como el abuso en cuanto a su uso; puede resultar costoso obtener tales pruebas y la información misma; el acceso a la información puede derivar en conflictos que se procuran evitar, etc.[6] El resultado final es que quien tiene la información puede definir la realidad, el campo de juego, en el que se moverán el resto de actores[7].

---

[3] Galbraith, J.K. (1984). *El nuevo estado industrial*, Edición puesta el día, Ariel, Barcelona, pp. 106-110.

[4] *Ibid.*, pp. 117-118.

[5] Pettigrew, A. M. (1972). "Information control as power resource", *Sociology*, Vol. 6, núm. 2, p. 190.

[6] Alcaide Castro, M. (1987). *Conflicto y poder en las organizaciones*, Centro de Publicaciones, Ministerio de Trabajo y Seguridad Social, Madrid, pp. 207-208.

[7] Pérez del Prado, D. (2020). "Representación de los trabajadores y protección de datos de carácter personal como fuente de poder", *Documentación Laboral*, núm. 119, Cinca, p. 58.

Nótese que esto deriva en una situación que se retroalimenta, puesto que los sujetos que se encuentran en una posición dependencia dentro de la organización verán mermadas también sus posibilidades de incrementar sus cotas de poder. Dicho de otra forma, cuanta menos información se controla en el seno de una organización, menos poder se dispone en la misma[8]. Esto es especialmente importante en el marco de los sistemas de relaciones laborales, caracterizados precisamente por el distinto poder de las partes. La falta de límites o compensaciones en cuanto a la tenencia y uso de la información puede devenir en un desequilibrio incluso mayor.

Desde esta perspectiva, el desequilibrio de poderes en el seno de la empresa se explicaría, entre otras causas, porque el empleador posee más información que quienes trabajan para él. Lógicamente, este no es el único elemento explicativo de esta asimetría de poder, pero no es poco relevante. Entre otros factores que se han señalado se encuentran los de índole económico, organizativo, jurídico y técnico[9].

Centrándonos en este último, es preciso señalar que existe consenso acerca de que, en la relación entre tecnología y poder, aquella sirve para robustecer e intensificar el ejercicio de este[10]. De ser esto así, la sociedad digital produciría una doble influencia sobre el poder empresarial que deriva en una extrema intensificación, pues, por una parte, buena parte de los avances de nuestro tiempo redundan en un mayor y más fácil acceso y gestión de la información[11]. Por otra, la propia irrupción de estos cambios tecnológicos trastocaría, como otros en el pasado, el equilibrio de poderes en el seno de la empresa. El resultado final sería

---

[8] Blackburn, R. S. (1981). "Lower participant power: Toward a conceptual integration", *Academy of Management. The Academy of Management Review (pre-1986); Briarcliff Manor*, Vol. 6, núm. 1, pp. 127-131.

[9] Loy, G. (2005). "El dominio ejercido sobre el trabajador", en Escudero Rodríguez, R. (ed.), *El Poder de dirección del empresario: nuevas perspectivas*, 1ª edición, La Ley-Actualidad, Las Rozas, Madrid, pp. 59-83.

[10] Luhmann, N. (1995). *Poder*, Antropos, Barcelona, pp. 99-103.

[11] En contra, Sanguineti, quien argumenta que el mayor o menor poder de dirección, en el ámbito de la digitalización, depende de la actividad que se desarrolle y, en particular, de las cualificaciones exigidas para ejecutarla. Sanguineti Raymond, W. (2024), "El poder de dirección ante el cambio económico y productivo y la emergencia de la inteligencia artificial", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 109, La Ley (España). Probablemente ambas posturas no sean incompatibles del todo, pues aquí se hace una valoración global de la tendencia, mientras que allí se desagrega por facultades del poder de dirección.

que la tecnología digital afectaría al poder empresarial en tanto que tecnología y como herramienta de acceso y gestión de la información.

Entre estos avances tecnológicos del particular momento que vivimos ocupa un lugar destacado la gestión algorítmica que, gracias a la actual expansión de la capacidad de captación, almacenamiento y computación o tratamiento de datos, propicia de forma instantánea una amplia variedad de soluciones y alternativas para la toma de decisiones en el ámbito empresarial. A su vez, el algoritmo es el corazón o, mejor dicho, el cerebro de otras, como las plataformas, pues es gracias a este instrumento matemático la plataforma puede proveer diversas respuestas u opciones. De ahí que sea una herramienta tan útil en el marco del poder de dirección, pues facilita la toma de decisiones de toda índole, hasta el punto de que, de una forma un tanto hiperbólica, se ha dicho que "el jefe puede ser un algoritmo"[12]. Sin embargo, debe observarse que la relación entre algoritmo y plataforma no es unidireccional, pues a través de la plataforma el algoritmo obtiene los datos que necesita para respirar[13].

Dada la estrecha relación entre ambos y de ambos con el tratamiento de la información, resulta interesante a nuestro juicio detenernos en el modo en que la gestión algorítmica está afectando ya al poder empresarial y cómo ha cristalizado esto en el particular ámbito de las plataformas, visto que las actividades que se han articulado a través de ellas se han caracterizado por unas condiciones de trabajo, en general, bastante precarias[14]. De lo que se trata es de corroborar que algoritmos y plataformas habrían contribuido a robustecer en exceso los poderes empresariales y, de ahí, que resulte lógica la reacción tendente a establecer límites y contrapoderes.

2. ALGORITMOS Y PODER EMPRESARIAL

Como acabamos de señalar, en los algoritmos no solamente cristalizan buena parte de los avances tecnológicos de nuestro tiempo, al permitir tratar cantidades

---

[12] Aloisi, A. y De Stefano, V. (2022). *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour*, Hart Publishing, Gordonsville.

[13] Acertada metáfora de Mercader Uguina, J. R. (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Tirant lo Blanch, Valencia, p. 28.

[14] Eurofound (2018). *Employment and working conditions of selected types of platform work*, Publications Office of the European Union, Luxembourg.

inmensas de datos para obtener soluciones concretas a las disyuntivas que se plantean en el día a día de las empresas; sino que representan el modo en que estas gestionan en el contexto digital. La gestión empresarial es hoy gestión algorítmica, pues prácticamente la totalidad de las facultades que integran el poder de dirección pueden articularse a través de algoritmos. En particular, la gestión algorítmica afecta al poder de dirección, en síntesis, en tres ámbitos principalmente: la organización de la actividad productiva, la capacidad de ordenación o de dictar órdenes y el control de la actividad laboral.

Comenzando por lo primero, por la organización de la propia empresa, hoy en día, en algunos sectores de actividad, basta con un simple algoritmo para que la empresa pueda ponerse en funcionamiento o, si se prefiere, en términos clásicos, pueda producir, sin que sea necesario recurrir a ningún otro elemento material. "Frente a la visión clásica de la fábrica repleta de maquinaria, los algoritmos nos trasportan a una realidad productiva que, como la nube, está vacía"[15] y, de ahí, que se hable de la "desmaterialización de la empresa"[16].

A través de los algoritmos se descentraliza la propia facultad de toma de decisiones, que queda en manos de un medio que nos promete darnos el mejor resultado posible sobre la base de criterios aparentemente objetivos. Se trata de "instrumento básico en la ordenación y gestión de los poderes de empresario"[17], una herramienta empleable en todas las facultades que integran el poder de dirección[18], por más que ahora nos refiramos a esta faceta en particular.

---

[15] Pérez del Prado, D. (2022). "Los tradicionales conceptos de trabajador y empresario en un mundo digital", en Mercader Uguina, J. R. y de la Puebla Pinilla, A. (eds.), *Cambio tecnológico y transformación de las fuentes laborales. Ley y convenio colectivo ante la disrupción digital*, Tirant lo Blanch, Valencia, p. 110.

[16] Mercader Uguina, J. R. (2022). "La gestión laboral a través de algoritmos", en AEDTSS, Ministerio de Trabajo y Economía Social (eds.), *Digitalización, recuperación y reformas laborales: XXXII Congreso anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social, Alicante, 26 y 27 de mayo de 2022*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid, pp. 264-265.

[17] Mercader Uguina, J. R. (2022). "En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo", *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, Iustel, p. 140.

[18] Álvarez Cuesta, H. (2020). *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*, Aranzadi Thomson Reuters, p. 30.

Nótese que hasta ahora hemos hablado de herramientas, técnicas y métodos de gestión en manos de un sujeto que, a efectos laborales, permanece inalterado, la empresa o empleador. También hemos dicho que la empresa se desmaterializa, cambia su morfología, lo que no quiere decir que mute en otro sujeto. Lo que ocurre es que la implosión de las técnicas avanzadas de gestión de datos se ha producido en el más absoluto vacío normativo, lo que ha sido empleado por las empresas para utilizar la información y el poder que de ella se deriva sin ninguna limitación. De ahí que hayamos afirmado en otro lugar que "no es que el jefe sea un algoritmo, sino que el jefe usa el algoritmo de forma enmascarada, sin ningún tipo de límite o restricción"[19].

El hecho diferencial que estas herramientas, técnicas y métodos aportan es la capacidad de ejercer la facultad de dirección de una forma objetiva y racional. El valor que esto reporta a la empresa es la posibilidad de reducir errores e incrementar la eficiencia en el uso de los recursos y, en particular, en relación al más relevante de todos ellos, el factor trabajo. A ello hay que unir su enorme polivalencia, pues la gestión algorítmica tiene capacidad de afectar todos los estadios de la vida laboral, desde su inicio hasta su finalización pasando por las diversas vicisitudes por las que esta puede atravesar[20].

Antes del inicio mismo de la relación laboral, las empresas ya ponen en manos de un software los procesos de selección de las personas candidatas asumiendo que "los seres humanos son muy buenos en especificar lo que se necesita para un determinado puesto y obtener información de los candidatos, pero son muy malos en la ponderación de los resultados"[21]. Surge así, lo que se ha denominado "reclutamiento tecnológico"[22].

---

[19] Pérez del Prado, D., "Los tradicionales conceptos de trabajador y empresario en un mundo digital", cit., p. 109. Véase este trabajo para una argumentación más extensa acerca de cómo la digitalización altera los poderes empresariales sin que ello suponga que el sujeto cambie a efectos de la aplicación del Derecho del Trabajo.

[20] Una evaluación de las condiciones de trabajo más frecuentemente afectadas puede verse en la primera parte del estudio European Parliament (2022), *AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework | Think Tank | European Parliament*, European Parliament, Brussels (Belgium), fecha de consulta 15 mayo 2022, en https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729516

[21] Kuncel, N. R., Ones, D. S. y Klieger, D. M. "In Hiring, Algorithms Beat Instinct", *Harvard Business Review*, 2014, fecha de consulta 6 mayo 2022, en https://hbr.org/2014/05/in-hiring-algorithms-beat-instinct.

[22] Alameda Castillo, M. T. (2021). "Reclutamiento tecnológico. Sobre algoritmos y acceso al empleo", *Temas laborales: Revista andaluza de trabajo y bienestar social*, 159, Consejo Andaluz

Una vez iniciada la relación laboral, el potencial aplicativo de la gestión algorítmica no disminuye, sino que incluso se incrementa. El espectro de actuación abarca prácticamente todas las condiciones de trabajo[23], como la promoción, la formación y la clasificación profesional, la remuneración, el tiempo de trabajo[24], la adopción de modificaciones sustanciales (o dentro del mero *ius variandi*) mediante decisiones automatizadas[25], la transmisión de empresas anteriormente mencionada, las distintas formas de terminación de la relación laboral o la prevención de riesgos[26].

Lógicamente, de lo anterior se deduce que la gestión algorítmica va a afectar también al ámbito colectivo del Derecho del Trabajo[27]. Prueba de ello es el caso Ericsson (STS de 3 de febrero de 2021[28]), en la que se declaró la existencia de vulneración del derecho de huelga pues, a través de una herramienta electrónica ubicada en Rumanía, la empresa asignaba incidencias a otras personas trabajadoras como vía para amortiguar el efecto de quienes estaban en huelga. A juicio de la Sala, "la automatización hace más difícilmente explicable que cupiera una

---

de Relaciones Laborales, pp. 11-52. Sobre la cuestión de la discriminación en la concreta parcela del acceso al empleo, véase Olarte Encabo, S. (2020), "La aplicación de inteligencia artificial a los procesos de selección de personal y ofertas de empleo: impacto sobre el derecho a la no discriminación", *Documentación Laboral*, 119, Cinca; Sáez Lara, C. (2020), "Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria", *Nueva revista española de derecho del trabajo*, núm. 232, Aranzadi Thomson Reuters.

[23] Salvador del Rey Guanter (ed.) (2018). *Inteligencia artificial y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales: Proyecto Technos*, La Ley Wolters Kluwer, Las Rozas (Madrid), pp. 281-295.

[24] Martínez Yáñez, N. M. (2021). "Entre robots y pandemias: retos de la regulación del tiempo de trabajo en el siglo XXI", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 78, Wolters Kluwer.

[25] Álvarez Cuesta, H. *El impacto de la inteligencia artificial en el trabajo*, cit., p. 40.

[26] Todoli Signes, A. (2022). "Prevención de riesgos laborales ante la inteligencia artificial y en la reputación digital de las personas trabajadoras", Molina Navarrete, C. y Vallecillo Gámez, M. R. (eds.), *De la economía digital a la sociedad del e-work decente: condiciones sociolaborales para una Industria 4.0 justa e inclusiva*, Aranzadi-Civitas.

[27] Los análisis realizados apuntan también hacia un amplio espectro de áreas susceptibles de ser afectadas por las muy diversas materializaciones de la inteligencia artificial y, en concreto, en relación con la libertad sindical, los derechos de los representantes de las personas trabajadoras, la negociación colectiva o, como en el caso señalado, el derecho de huelga. Salvador del Rey Guanter (ed.), *Inteligencia artificial y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales*, cit., pp. 304-339.

[28] ECLI:ES:TS:2021:643

atribución de tareas a personas distintas a las que, en buena lógica, se hallaban en el sistema de asignación "automatizado", por ser las que tenían atribuidas las mismas. Además, se constata que, a partir del inicio de la huelga, los casos se despacharon a una contrata no habitual, con el resultado de que, en los tres supuestos expresamente señalados en la narración de la sentencia recurrida, se produjo una asignación de las incidencias claramente distinta de la que hubiera resultado de no hallarse en huelga parte de la plantilla".

Pero si la digitalización afecta al nacimiento y desarrollo de la relación laboral, también lo hace, como se adelantó, a su terminación. Alcanzó un alto eco mediático la SJS de Las Palmas de 23 de septiembre de 2019[29] que declaró que la sustitución de un empleado por un bot debe ser considerada despido improcedente[30]. La misma solución empleó la STSJ de Madrid de 7 de octubre de 2019 ante la sustitución de nueve operarios por tres máquinas, pues, aunque habían incrementado la productividad de la empresa, no quedó acreditado que de ello se derivara la necesidad de prescindir de tal número de personas trabajadoras[31].

Algunos años antes, en el caso Skill Competence Matrix (STS de 25 de septiembre de 2018[32]), el Tribunal Supremo tuvo la oportunidad de analizar la

---

[29] ECLI:ES:JSO:2019:4141

[30] Sobre esta sentencia, véase el análisis de Mercader Uguina, J. R. (2019), "Despido de una administrativa cuyo trabajo ha sido sustituido por un Robot: ¿es posible poner Puertas al Campo?", *El Foro de Labos*, fecha de consulta 1 octubre 2019, en https://www.elforodelabos.es/2019/10/despido-de-una-administrativa-cuyo-trabajo-ha-sido-sustituido-por-un-robot-es-posible-poner-puertas-al-campo/. También se sitúa en este ámbito la STSJ Galicia de 19 de julio de 2016 (ECLI:ES:TSJGAL:2016:6138), que declaró la improcedencia del despido de una trabajadora por no quedar probada la conexión entre la causa técnica "implantación de la historia clínica electrónica" y el descenso de la actividad que supuestamente habría tenido lugar; descenso de la carga de trabajo que sería lo que determinaría la necesidad de proceder a los despidos y su justificación, entre otros factores analizados. Un resultado similar se puede encontrar en la STSJ de Castilla y León de 23 de marzo de 2005 (Rec. núm. 426/2005), en la que no se entiende probado que la instalación de un nuevo sistema informático que, teóricamente, haría innecesario el trabajo de la despedida, produzca un efecto de la suficiente entidad como para justificar el despido.

[31] ECLI: ES:TSJM:2019:9239. Más recientemente el debate ha resurgido como consecuencia del empleo, por parte de una cadena de televisión, de una influencer virtual en un programa de televisión. *El País*, "El caso de Alba Renai en Mediaset: ¿le pueden despedir para que un robot ocupe su sitio?", *El País*, 2024, fecha de consulta 24 marzo 2024, en https://elpais.com/economia/negocios/2024-03-24/el-caso-de-alba-renai-en-mediaset-le-pueden-despedir-para-que-un-robot-ocupe-su-sitio.html.

[32] ECLI:ES:TS:2018:3463.

idoneidad de una aplicación que ponderaba tres variables a la hora de seleccionar las personas para permanecer en la empresa (o ser despedidos, según se vea) en caso de despido colectivo: índice de polivalencia, (40%), número de operaciones con aptitud (40%) y número de certificaciones (20%). A pesar de que 17 de los 25 trabajadores afectados por la medida extintiva eran afiliados a CC. OO., la Sala entendió que no había discriminación, pues la empresa no solo acreditó la concurrencia de causas económicas y productivas (lo que sería insuficiente) sino también, lo que es lo más importante a los efectos del presente estudio, la utilización de criterios objetivos, razonables y no arbitrarios de selección[33].

En segundo lugar, la capacidad de dictar órdenes e instrucciones también se ve afectada por la gestión algorítmica. De hecho, a la luz de los avances técnicos de nuestros días, esta otra facultad ha experimentado una notable expansión. La empresa es capaz de dar más órdenes, ya sea porque las versiones avanzadas de las tecnológicas propias de la anterior revolución industrial (las llamadas TICs) así lo permiten en un escenario de hiperconexión, ya sea porque estas sean tomadas con el apoyo de la gestión algorítmica, cuando no directamente a través de esta. Por cualquier de estas vías o a través de todas ellas conjuntamente la empresa puede dictar más instrucciones, asegurándose un control más estrecho del desarrollo de la actividad profesional y una mayor y mejor alineación con sus objetivos. La otra cara de la moneda es, lógicamente, que las posibilidades de incumplimiento, voluntario o no, también se incrementan y con ello, las probabilidades de sanción[34].

---

[33] No obstante, a pesar de que la gestión algorítmica resulte una garantía en cuanto a la objetividad de los criterios de decisión, se ha advertido que "debe someterse a las debidas cautelas para evitar que la identificación de los trabajadores afectados genere riesgos de discriminación", para lo que se ha propuesto que "el algoritmo forme parte del período de consultas de modo que se asegure la transparencia en su diseño e incluso la participación de los trabajadores para definir la lógica parcialidad en el sistema". de la Puebla Pinilla, A. (2021). "El despido por causas empresariales", Congreso Nacional de Derecho del Trabajo y de la Seguridad Social (ed.), *Reestructuraciones empresariales: XXXI Congreso de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social, Subdirección General de Informes, Recursos y Publicaciones, Madrid, Informes y estudios. Empleo, p. 216.

[34] Cuando no la propia utilización del algoritmo para sancionar, lo cual también agiliza el ejercicio de esta potestad empresarial. UGT (2019). *UGT ante la digitalización: tres años de acción sindical*, Comisión Ejecutiva Confederal de UGT, Secretaría de Política Sindical, Madrid, p. 93.

Además, esta particular facultad se beneficiaría de la tendencia general hacia una difuminación de los límites de lugar y tiempo de trabajo. La empresa puede ejercer su facultad ordenadora fuera del lugar de trabajo y, frecuentemente, al margen de la jornada laboral. El derecho a la desconexión surge precisamente ante la necesidad de poder no tomar en consideración instrucciones o encargos dados fuera del tiempo de trabajo y del lugar habitual de producción, sin que por ello se pueda derivar consecuencia sancionadora alguna por incumplimiento o incumplimiento extemporáneo. Nótese que, a este respecto, la intervención normativa se ha hecho necesaria al desaparecer cualquier tipo de autolimitación en una sociedad que valora positivamente la inmediatez y conexión constante[35].

En suma, ya sea porque la propia tecnología aporta determinadas ventajas en el ejercicio del poder de dirección, ya sea porque permita un mayor número de órdenes, además de en cualquier tiempo en lugar, ya sea porque estas sean percibidas de forma más justa o simplemente sean más efectivas, lo cierto es que, se mire donde se mire, todo apunta hacia la misma dirección, un incremento del poder de dirección.

Esto resulta corroborado, aún más si cabe, si nos fijamos en la última de las facultades objeto de atención, el control. Que esta se viene reforzando no es algo completamente novedoso. Hace ya años, durante la anterior revolución industrial y probablemente vislumbrando la siguiente, se nos advirtió del advenimiento de la "empresa panóptica" y de un nuevo "feudalismo virtual"[36], muestra de la creciente capacidad de la empresa de controlar a las personas trabajadoras dando pie a un remozado vasallaje digital[37]. Veinte años después, esto ya no se otea en el horizonte, sino que es una realidad de nuestros días[38], hasta el punto de que puede afirmarse que hay práctica unanimidad en la doctrina al afirmar

---

[35] Tomlinson, J. (2007). *The Culture of Speed: The Coming of Immediacy*, SAGE.

[36] Mercader Uguina, J. R. (2002). *Derecho del trabajo. Nuevas tecnologías y sociedad de la información*, Editorial Lex Nova, Valladolid, p. 99. Aunque quizá podríamos añadir algún año más a la cuenta, pues lo de la empresa panóptica ya se empezó a analizar en Mercader Uguina, J. R. (2001), "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones laborales: Revista crítica de teoría y práctica*, núm. 1, Wolters Kluwer, pp. 665-686.

[37] Un paso más en la evolución que analizara Alonso Olea, M. (1987). *De la servidumbre al contrato de trabajo*, 2ª edición revisada y ampliada, Ed. Tecnos, Madrid.

[38] Mercader Uguina, J. R. (2017). *El futuro del trabajo en la era de la digitalización y la robótica*, Tirant lo Blanch, Valencia, pp. 121-182.

que uno de los rasgos distintivos de la digitalización es precisamente el reforzamiento de la capacidad de control empresarial a través de una vigilancia "omnipresente y omnipotente"[39], incluso, "infinita"[40]. La clave está en que los avances tecnológicos, "al tiempo que permiten intensificar, a extremos insospechados en el pasado, la capacidad de vigilancia y seguimiento de la actividad del trabajador por parte del empleador, se han convertido en medios poco costosos que como tales facilitan su extensión a la generalidad de las empresas"[41]. Ha nacido el "neotaylorismo digital"[42].

No obstante, este es un proceso que se ha producido más por acumulación que por decantamiento. En la práctica, resulta difícil distinguir aquellas tecnologías que, habiendo nacido en la anterior revolución industrial, incorporan otras

---

[39] Álvarez Cuesta, H., *El impacto de la inteligencia artificial en el trabajo*, cit., p. 42. El interés de la doctrina por el control empresarial es amplio intenso y variado, repartiéndose entre estudios iniciáticos como el de Goñi Sein, J. L. (1988). *El Respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Cívitas, Madrid.; pasando por los que se elaboraron al hilo de la revolución de las TIC, como el de Desdentado Bonete, A. y Muñoz Ruiz, A. B. (2012). *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid; para terminar por los más recientes vinculados a la digitalización y que quizá tengan su más reciente actualización en la interlocución de Valdeolivas García, Y. (2022). "Derechos de información, transparencia y digitalización", en *Digitalización, recuperación y reformas laborales. XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid, Informes y estudios. Empleo, pp. 187-222; y Todolí Signes, A. (2022). "Control tecnológico: una propuesta de aplicación del triple juicio de proporcionalidad conforme a la normativa europea de protección de datos", *Digitalización, recuperación y reformas laborales. XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid, Informes y estudios. Empleo (Consúltese la bibliografía de estos trabajos para mayor detalle).

[40] Ajunwa, I., Crawford, K. y Schultz, J. (2016). *Limitless Worker Surveillance*, Social Science Research Network, Rochester, NY. Lo que ha llevado a la profesora Ginès a hablar también de un "incremento infinito" del poder de control. Ginès Fabrellas, A. (2022). "La gestión algorítmica del trabajo: nuevos retos jurídicos, tecnológicos y éticos", *Digitalización, recuperación y reformas laboralesMinisterio de Trabajo*, Ministerio de Trabajo y Economía Social, Subdirección General de Informes, Recursos y Publicaciones, Madrid, Informes y estudios. Empleo, pp. 300-301.

[41] Cruz Villalón, J. (2019). "Las facultades de control del empleador ante los cambios organizativos y tecnológicos", *Temas laborales: Revista andaluza de trabajo y bienestar social*, 150, Consejo Andaluz de Relaciones Laborales, p. 15.

[42] Baz Rodríguez, J. (2022). "Responsabilidad algorítmica y gobernanza de la inteligencia artificial en el ámbito sociolaboral. Entre la perspectiva y la prospectiva", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 89, Wolters Kluwer, p. 4 (ejemplar digital).

de la presente; de las que son netamente digitales. Aquellas resultan hoy además más sencillas de usar, no solamente porque resulten más baratas, sino porque han solido sufrir un proceso de miniaturización, se han incorporado a otras ampliamente extendidas como el teléfono móvil o han resultado mejoradas por sus hermanas digitales. Tal sería el caso de la videovigilancia, la microvigilancia, la geolocalización, las etiquetas electrónicas y las tarjetas inteligentes o la vigilancia informática a través de software[43]. El empleo por parte de las empresas de esta tecnología para controlar el desarrollo de la actividad laboral, por tanto, no es nueva. Lo que cambia con la disrupción digital es que su uso es más barato, más sencillo y, lo que es más importante, la información obtenida a través de ella es más fácil de producir, enviar, almacenar, tratar y analizar.

Por consiguiente, el control de la actividad laboral de nuestros días resulta de un "mix" entre las tecnologías de la tercera y de la cuarta revolución industrial en el que el hecho diferencial es que la información proveniente de las primeras puede ser manejada de forma más ágil y eficiente, lo que permite un control más continuo, más ajustado y más exhaustivo. De ahí que, probablemente, lo que nos permite diferenciar los cambios experimentados por esta facultad empresarial respecto de los de la revolución inmediatamente anterior sea la capacidad de gestionar esos datos y de tomar decisiones de forma asistida o automática en función de ellos. El poder de control de la empresa en el mundo actual es poder de control algorítmico[44].

De ello podemos derivar ya una primera conclusión, que es que las herramientas con que contaba la empresa para el control de la actividad laboral de las personas trabajadoras se van a ver, como mínimo, mejoradas, de lo que se deduce una mayor facilidad en el uso de esta facultad, cuando no su reforzamiento e intensificación. A partir de ahí, las tecnologías digitales abren la puerta

---

[43] Goñi Sein, J. L. (2009). "Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia Laboral. Revista de Derecho del Trabajo y de la Seguridad Social*, núm. 39, pp. 11-58; Mercader Uguina, J.R., *Derecho del trabajo. Nuevas tecnologías y sociedad de la información*, cit., pp. 95-124.

[44] Mercader Uguina, J. R., *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., pp. 90-101. De hecho, de las tecnologías propias de esta revolución industrial, el big data, la inteligencia artificial, la analítica de datos y la nube serían las que más tocan al ámbito laboral y, por lo que aquí respecta, a la facultad de control. Sobre estas tecnologías y su implementación en el marco del despliegue de la cuarta revolución industrial, véase Joyanes Aguilar, L. (2017), *Industria 4.0: la cuarta revolución industrial*, Alfaomega; Marcombo, Barcelona.

a la posibilidad de controles "exhaustivos", como los ha llamado el Parlamento europeo, ante los que ha solicitado a los interlocutores sociales, así como a las autoridades de supervisión de la protección de datos, "que velen por que los instrumentos de supervisión laboral solo se utilicen cuando sea necesario y proporcionado y garanticen el derecho a la intimidad de los trabajadores y a la autodeterminación en su trabajo"[45]. Sin embargo, la posición de la alta institución europea, que es extrapolable a la de cualquier otra autoridad pública en general, pivota entre esta admisión con cautelas y la alarma, pues, apenas un año después, condenaba "que cada vez se esté recurriendo más a la vigilancia basada en IA en el lugar de trabajo, lo que sucede a menudo sin el conocimiento de los trabajadores, y mucho menos su consentimiento, en particular también en el contexto del teletrabajo", a lo que añadía que "esta práctica no debe permitirse, ya que es extremadamente abusiva con respecto al derecho fundamental a la privacidad, a la protección de datos y a la dignidad humana del trabajador y a los derechos sociales y laborales, y también tiene efectos negativos sobre la salud mental de los trabajadores debido al grado de intrusión, su efecto general o indiscriminado y la falta de salvaguardias para las personas afectadas"[46]. Por tanto, existe preocupación acerca de hasta dónde puede llevar la capacidad de control empresarial. No en vano, esta facultad es considerada también de alto riesgo por el Reglamento sobre inteligencia artificial[47]. No es para menos, tanto si se tiene en cuenta tanto las funcionalidades presentes de herramientas antiguas como de los instrumentos netamente digitales.

Por tanto, las herramientas de sobre control informático no son nuevas en el día a día de nuestras empresas. De hecho, podemos encontrar resoluciones judiciales a finales de los 90 y principios de este siglo que se refieren a controversias sobre el control por parte de la empresa de las webs visitadas durante el tiempo

---

[45] Resolución del Parlamento Europeo, de 21 de enero de 2021, con recomendaciones destinadas a la Comisión sobre el derecho a la desconexión [2019/2181(INL)].

[46] Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital [2020/2266(INI)].

[47] "Al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones". Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024. Anexo III.

de trabajo[48], el uso del correo electrónico profesional[49] o el registro de los archivos informáticos[50]. La diferencia fundamental con el control informático que se ejerce en nuestros días es que este permite el seguimiento en tiempo real y de un elenco de datos más amplio, como el número de operaciones efectuadas, el número de errores cometidos, el tiempo empleado para cada una, el tiempo total de trabajo, la memoria utilizada, el número de frecuencia y la duración de las interrupciones. Si a ello le sumamos la gestión algorítmica de esta información, el control se intensifica, pues de acuerdo con los datos obtenidos podrán sugerirse actuaciones de restricción, limitación o, incluso de sanción o adoptarlas automáticamente por parte del algoritmo y, ello, de forma instantánea o en tiempo real.

Algo parecido puede decirse de otros mecanismos de control como el biométrico[51], herramienta en franca expansión. Desde las primeras fórmulas de reconocimiento dactilar o a través del iris hemos pasado al reconocimiento facial, pero con la particularidad de que esto resulta posible a gran escala, de forma indiscriminada[52], acumulando una alta cantidad de información que puede ser gestionada y tratada de forma algorítmica con relativa facilidad, hasta

---

[48] STSJ Madrid de 16 de octubre de 1998 (Rec. núm. 4215/1998). Lo que ha propiciado también debates judiciales no menores y probablemente tampoco acabados, como el de la llamada doctrina Barbulescu. Desdentado Bonete, A. y Desdentado Daroca, E. (2018). "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", *Revista de información laboral*, núm. 1, Lex Nova, pp. 19-39.

[49] STSJ Madrid de 4 de diciembre de 2001 (Rec. núm. 4294/2001).

[50] STSJ Andalucía de 25 de febrero de 2000 (Rec. núm. 2207/1999).

[51] Fernández Orrico, F. J. (2020). "Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación", Rodríguez-Piñero Bravo-Ferrer, M., Todoli Signes, A. (eds.), *Vigilancia y control en el Derecho del Trabajo Digital,* ISBN 978-84-1346-551-7, págs. 301-326, Aranzadi Thomson Reuters, pp. 301-326; Mercader Uguina, J. R. (2020). "Datos biométricos en los centros de trabajo", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, extra 11, Wolters Kluwer; Rodríguez-Piñero Royo, M. (2020). "Registro de jornada mediante controles biométricos: un caso de incoherencia en el Derecho del Trabajo Digital", Rodríguez-Piñero Royo, M. y Todolí Signes, A. (eds.), *Vigilancia y control en el Derecho del Trabajo Digital*, Aranzadi Thomson Reuters, pp. 273-300.

[52] De hecho, esto es uno de los aspectos clave del caso analizado por la AEPD (PS/00120/2021) en el que, para hacer efectiva una condena de alejamiento a dos sujetos, una cadena de supermercados decidió establecer un sistema de reconocimiento facial de todos los clientes que accedieran a sus centros. Este asunto fue posteriormente resuelto por el AAP Barcelona de 15 de febrero de 2021 (Rec. Núm. 840/2020 –ECLI:ES:APB:2021:1448ª–).

el punto de que se puede trascender el mero control o identificación para acceder a otra información relativa al individuo, como su estado de ánimo, nivel de cansancio o posibles enfermedades.

En su estadio máximo, la gestión algorítmica permitirá a la empresa realizar también prospectiva y previsión, en lo que se ha venido a denominar "minority report" laboral[53]. A través de la ponderación de los datos obtenidos del seguimiento de la actividad laboral, los algoritmos pueden predecir la posibilidad de que exista una amenaza. Sobre esta base, la empresa podrá tomar medidas adicionales de control sobre las personas trabajadoras a fin de evitarlas antes de que ocurran.

Estamos, en estos supuestos, en un ámbito enormemente delicado. De ahí que el Reglamento de Inteligencia Artificial opte entre la prohibición (se prohíbe expresamente "la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para inferir las emociones de una persona física en los ámbitos de la aplicación de la ley (...) en lugares de trabajo (...)" [art. 5.1 f)]; así como "la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual (...)" [art. 5.1 g)]) y su consideración como de alto riesgo (se considera como tal "sistemas de IA destinados a utilizarse para la contratación o selección de personas físicas, especialmente para anunciar puestos vacantes, clasificar y filtrar solicitudes o evaluar a candidatos en el transcurso de entrevistas o pruebas; [y la] IA destinada a utilizarse para tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas y al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones" (Anexo III en relación con el art. 6.2)).

---

[53] Mercader Uguina, J. R., *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., p. 99. En alusión a la película de ciencia ficción del mismo título basada en la idea de una herramienta de inteligencia artificial que permitía adelantarse a la comisión de crímenes. *Minority Report,* Amblin Entertainment & Blue Tulip Productions, 2002. La película se basa en el relato corto con el mismo título escrito por Philip K. Dick en 1956 en la revista "Fantastic Universe".

En suma, de todo lo dicho hasta aquí, podemos extraer una segunda y última conclusión en torno al modo en que la facultad de control empresarial se transforma en el marco digital: el control algorítmico incrementa exponencialmente el poder de dirección del empresario, pues a las facultades tradicionales de control añaden otras de naturaleza no menor.

Así, gracias al control algorítmico la empresa puede "direccionar" a las personas trabajadoras de forma dinámica, tanto en la forma como en relación al lugar, esto es, las instrucciones, que normalmente no son expresas, se pueden adaptar de forma continua al desempeño, incluso más allá del tiempo y lugar de trabajo. Además, la gestión algorítmica permite restringir aún más tanto la información como las actuaciones de la mano de obra de forma instantánea y encubierta. Lo primero es causa, aunque sea parcial de lo segundo, pues al reforzarse la situación de información asimétrica es más fácil restringir determinadas actividades no deseadas. Del mismo modo, el control algorítmico, como otros mecanismos de control, permite evaluar el desarrollo de la actividad profesional, pero en este caso incorporando nuevas perspectivas, como el uso de información interna y externa, y, lo que es más importante, en tiempo real y de forma instantánea. Por último, no resultan menos relevantes las posibilidades que otorga en el campo de los incentivos, ya sean de tipo positivo, esto es, recompensas, o, negativo, sanciones, pues como en casos anteriores no solamente es posible aplicarlos instantáneamente, sino de forma continua, dirigiendo la actividad laboral de forma constante.

En suma, es indudable que la gestión algorítmica aporta a la empresa una ventaja que va más allá de la facilidad y eficiencia en la gestión para alcanzar una suerte de inatacabilidad práctica de las decisiones adoptadas a través de ellos, en lo que se ha venido a denominar "la mano invisible e irresponsable" de los algoritmos[54]. Asimismo, permite dictar un mayor número de instrucciones y expandir el control de su cumplimiento o, simplemente, del desempeño de la actividad laboral de forma casi ilimitada. La nueva empresa panóptica se alza con poderes más amplios y más intensos de los que hace unos años nos podíamos incluso imaginar. En uno y otro caso, la técnica ha dotado a la empresa de un amplio margen de flexibilidad, que ha sido aún mayor ante un marco normativo prácticamente

---

[54] Rivas Vallejo, M. P. (2022). "Sesgos de género en el uso de inteligencia artificial para la gestión de las relaciones laborales: análisis desde el derecho antidiscriminatorio", *e-Revista Internacional de la Protección Social*, Vol. 7, núm. 1, p. 54.

inexistente ante esta nueva realidad. El resultado final es un reforzamiento del poder empresarial que resulta a todas luces excesivo desde el punto de vista de la eficiencia y la equidad[55] y ante el que se ha hecho necesario establecer límites y contrapoderes.

3. PLATAFORMAS Y PODER EMPRESARIAL

De lo dicho hasta aquí se puede deducir que el poder de dirección es más fuerte que nunca, gracias precisamente a la gestión algorítmica. No podemos decir que el taylorismo en su versión primigenia siga vivo, aunque sí ha habido quien se ha atrevido a describir y analizar un nuevo "taylorismo digital"[56].

Esto es especialmente significativo en el ámbito del trabajo en plataformas, en el que todo ese incremento del poder propiciado por los algoritmos se ha visto acrecentado aún más como consecuencia del intento de huida del Derecho del Trabajo a causa de la utilización de la propia plataforma.

En efecto, se ha dicho que una de las características de la plataforma como avance tecnológico es precisamente la de descansar sobre la gestión algorítmica, que propiciaría tanto un incremento del poder de dirección directo, tal y como hemos venido explicando anteriormente, como indirecto, en el sentido de que las órdenes se sustituyen por amplios espacios de libertad atribuidos al prestador del servicio, esto es, el poder de dirección es ejercido mediante incentivos, mediciones o expectativas sobre el volumen, la calidad o el mantenimiento del empleo[57].

---

[55] Este, el de la equidad, no es un ámbito menor, pues los algoritmos tendrían también un fuerte impacto desde el punto de vista de distributivo y redistributivo. En este sentido, recoge los aportes de la ya relativamente abundante literatura norteamericana al respecto y los cristaliza en el concepto de "algoritmo extractivo", en el sentido de que no crean valor, sino que lo aliena, Todolí Signes, A. (2023). *Algoritmos productivos y extractivos: cómo regular la digitalización para mejorar el empleo e incentivar la innovación*, Aranzadi, Cizur Menor Navarra.

[56] Prassl, J. (2018). *Humans as a service: the promise and perils of work in the gig economy*, First edition, Oxford University Press, Oxford, United Kingdom, New York, NY, p. 72.

[57] Gil Otero, L. (2023). "La economía de plataformas ante las categorías clásicas del Derecho del Trabajo", Universidade de Santiago de Compostela, p. 118. Previamente, destacan las monografías Rodríguez Fernández, M. L. (ed.) (2019). *Plataformas digitales y mercado de trabajo*, Ministerio del Trabajo, Migraciones y Seguridad Social, Subdirección General de Información Administrativa y Publicaciones, Madrid; Rodríguez-Piñero Royo y Hernández-Bejarano, M. (2017). *Economía colaborativa y trabajo en plataforma: realidades y desafíos*, Bomarzo; Todolí Signes, A. y Hernández-Bejarano, M. (eds.) (2018). *Trabajo en plataformas digitales: innovación, derecho y mercado*, Aranzadi.

Pero junto a la gestión algorítmica, como hemos dicho, las plataformas también pueden caracterizarse como herramienta de intermediación. A diferencia de otros avances tecnológicos de esta revolución industrial, la plataforma habría tenido la capacidad de aunar una mayor, más ágil e intensa gestión de los recursos humanos, a través de la gestión algorítmica; con la posibilidad de hacerlo a distancia y sin prácticamente intervención física, en su vis de herramienta de interconexión. De esto último se deriva una, sin lugar a dudas, mayor flexibilidad para la empresa, pues es capaz de gestionar más personas, con menos recursos y a distancia. También, lógicamente, un menor coste, pues, tras una primera inversión inicial, podrá hacerlo con una mínima infraestructura. El resultado final es otro ámbito de fortalecimiento del poder dirección, pues esa capacidad para emplear un amplio número de sujetos fácilmente intercambiables es sinónimo de una mayor flexibilidad cuantitativa y, en consecuencia, mayor poder empresarial.

Con todo, la mayor fuente de poder de la empresa en el ámbito del trabajo de plataformas no deriva ni de la gestión algorítmica, ni como herramienta de intermediación, sino de las bases sobre las que se ha pretendido asentar su modelo de negocio. Desde esta perspectiva, el mayor poder empresarial deriva de intentar justificar un modelo en el que no era necesario establecer, sostienen muchas de las empresas que las emplean, ningún tipo de relación laboral. Al margen del Derecho del Trabajo, ese poder omnímodo propiciado por las flexibilidades técnicas y cuantitativas quedaba además libre de ningún tipo de limitación o compensación. Por si todo esto fuera poco, ello ha resultado acrecentado aún más si cabe por la existencia de un auténtico vacío normativo, pues la realidad de las plataformas y del trabajo en plataformas no había sido integrada por el ordenamiento jurídico-laboral.

De ahí que, aunque la cuestión del estatus jurídico del trabajo en plataformas haya sido el auténtico protagonista en el ámbito político y científico[58], a los efectos del presente estudio revista una importancia relativa, pues no afecta al poder en sí mismo, sino a los límites y compensaciones que se van a poder establecer frente a ese poder. Bajo este prisma, el fenómeno del trabajo en plataformas debe ser abordado desde dos ámbitos diferenciados. Por un lado, el de cuál es el marco jurídico idóneo para su regulación. No debe olvidarse que, aunque

---

[58] Gil Otero, L., "La economía de plataformas ante las categorías clásicas del Derecho del Trabajo", cit.

numerosísimas sentencias en todo el mundo han concluido, particularmente en el sector del "delivery", que existe relación laboral, esta no tiene por qué ser la única solución, sino que dependerá de la actividad y, sobre todo, del modo en que se emplee la plataforma[59]. Por otro, cuando se concluye que tal marco es el laboral, determinar cuáles son los límites y compensaciones que han de establecerse para propiciar la existencia de una relación laboral equilibrada y, sobre todo, eficiente. A ello dedicaremos las páginas que siguen.

4. LÍMITES Y CONTRAPODERES AL PODER EMPRESARIAL: EL CASO DE LAS PLATAFORMAS

Aclarado lo anterior, en las primeras reacciones judiciales y normativas que han tendido a embridar el poder de dirección en el ámbito del trabajo en plataformas se observa que esto se ha articulado a través de dos herramientas básicas. Por una parte, mediante el establecimiento de limitaciones en su empleo, pues, como recuerda el Reglamento de Inteligencia Artificial, "los sistemas de IA empleados para controlar el rendimiento y el comportamiento de estas personas también pueden socavar sus derechos fundamentales a la protección de los datos personales y a la intimidad". Por otra, a través del recurso a contrapoderes que hagan posible un uso equilibrado de la gestión algorítmica. Cuando se habla de introducir "transparencia", no se hace referencia más que al hecho de situar a todas las partes concernidas en una situación homologable, de tal forma que puedan tomar decisiones con información suficiente.

4.1. Herramientas basadas en el establecimiento de limitaciones

El juego entre la ampliación y potenciación de los poderes empresariales derivado de la aplicación de las herramientas digitales y el vacío normativo en esta concreta materia han propiciado una suerte de círculo vicioso que termina por robustecer y expandir aún más aquellos. Como consecuencia, la falta de un marco legal adecuado coloca a las personas trabajadoras en una situación de desventaja, lo que conduce a peores condiciones laborales, en particular, en lo que

---

[59] Todolí Signes, A. (2017). *El trabajo en la era de la economía colaborativa: la clasificación jurídica de trabajadores y autónomos y los efectos de la reputación online en la economía de las plataformas virtuales*, pp. 45-59.

respecta al salario, la salud y la seguridad, tiempo de trabajo, igualdad de trato y no discriminación y protección social[60].

De ahí que no pocas organizaciones internacionales, y también Estados, particularmente en Europa, hayan iniciado procesos tendentes a la regulación de la inteligencia artificial y la gestión algorítmica en sus muy diversos ámbitos de aplicación, incluyendo el laboral y social. De lo que se trata no es solamente de cubrir lo que no está regulado, sino también de evitar situaciones de abuso mediante la imposición de límites, garantías y contrapoderes a facultades e instrumentos que hasta ahora se han utilizado sin prácticamente ninguna restricción.

En particular, el Consejo de Europa ha llamado al seguimiento de los desarrollos tecnológicos y la revisión de posibles impactos negativos, con especial atención al uso de técnicas de procesamiento algorítmico. Según su análisis, las respuestas efectivas a tales impactos negativos podrían incluir enfoques regulatorios experimentales sobre la mejor manera de proteger los derechos de los demás y garantizar los objetivos regulatorios, siempre que vayan acompañados de un seguimiento sistemático de sus efectos[61]. De hecho, desde el propio Consejo se vienen aprobando diversas recomendaciones acerca de cómo abordar esta tarea regulatoria[62].

Al margen de lo anterior, la herramienta más destacable en este particular ámbito es el Convenio Marco sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho[63]. Su propósito fundamental es garantizar que las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial sean plenamente coherentes con los derechos humanos, la democracia y el Estado de Derecho. Para ello, se parte de una definición de inteligencia artificial

---

[60] Schmid-Drümer, M. (2016). *The situation of workers in the collaborative economy | Eurofound*, European Parliament, Brussels.

[61] Recommendation 2102(2017) of the Parliamentary Assembly of the Council of Europe about Technological convergence, artificial intelligence and human rights.

[62] Entre estas, destacan la "Declaration Decl(13/02/2019)1 of the Committee of Ministers on the manipulative capabilities of algorithmic processes", y la "Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems". Próximamente está previsto que se publique "A transversal legal instrument to regulate the design, development and use of artificial intelligence systems - CAI". Puede accederse al contenido íntegro a través del siguiente enlace: https://www.coe.int/en/web/artificial-intelligence/work-in-progress#01EN

[63] https://www.coe.int/es/web/portal/-/artificial-intelligence-human-rights-democracy-and-the-rule-of-law-framework-convention

(art. 2) prácticamente idéntica al del Reglamento de Inteligencia Artificial de la UE, que a su vez la tomaba de la propuesta por la OCDE[64].

A partir de aquí, y por lo que al objeto de este estudio se refiere, el Convenio se centra en garantizar la protección de los derechos humanos a lo largo del ciclo de vida de los sistemas de inteligencia artificial (art. 4), prestando especial atención a la dignidad humana y la autonomía individual (art. 6), la igualdad y no discriminación (art. 9), la intimidad y la protección de datos de carácter personal (art. 10) y la salud y el medio ambiente (art. 11).

A este respecto, se hace mención expresa a algunos instrumentos como la transparencia y supervisión (art. 7), sin que se nos dé una definición expresa de que ha de entenderse por aquella ni de qué forma alcanzarla[65]; la rendición de cuentas y responsabilidad (art. 8); y el aseguramiento de la fiabilidad y confianza (art. 12). En relación a esto último, se afirma que "cada Parte adoptará medidas apropiadas para promover la confiabilidad, seguridad, validez y confianza en sistemas de inteligencia artificial, que podrían incluir el establecimiento de requisitos que busquen garantizar que la seguridad, la protección, la precisión, el rendimiento, la calidad, la calidad, integridad y seguridad de los datos, la gobernanza, la ciberseguridad y la solidez se aplicarán durante todo el ciclo de vida de los sistemas de inteligencia artificial". Por otra parte, aunque no se reconoce un derecho al "humano al mando", como veremos más adelante, sí, al menos, a ser informado de que se está interactuando con inteligencia artificial (art. 15.2).

Al margen de lo anterior, el Convenio contiene algunas disposiciones interesantes desde un punto de vista práctico y que trascienden la mera garantía de los derechos fundamentales concernidos, tales como la especial protección de niños y personas con discapacidad (art. 18), la extensión de la figura del denunciante a este particular ámbito de la inteligencia artificial (art. 19) o el deber de fomentar y promover una alfabetización digital adecuada y habilidades digitales para todos segmentos de la población, incluidos los responsables de la identificación,

---

[64] Mercader Uguina, J. R. (2024). "El Reglamento de Inteligencia Artificial: frecuentemos el futuro", *Los Briefs de la AEDTSS, Asociación Española de Derecho del Trabajo y de la Seguridad Social,* núm. 42, fecha de consulta 20 marzo 2024, en https://www.aedtss.com/el-reglamento-de-inteligencia-artificial-frecuentemos-el-futuro/

[65] Aunque sí se encuentran entre las medidas correctivas el derecho a la información tanto de los sujetos afectados como de los concernidos, lo que abriría la puerta a su reconocimiento a la representación legal de las personas trabajadoras.

evaluación, prevención y mitigación de los riesgos que plantean los sistemas de inteligencia artificial (art. 21).

En el ámbito de la Unión Europea, el Parlamento Europeo ha pedido que se actualice y complemente el marco legal existente con principios rectores éticos basados en un enfoque de la inteligencia artificial "centrada en el ser humano", que respete los valores y principios europeos[66]. Como parte de este enfoque, la Comisión Europea ha puesto en marcha dos medidas complementarias, el Reglamento sobre inteligencia artificial y un nuevo plan coordinado con los Estados miembros. Mientras que el primero tiene un marcado carácter normativo, el segundo es más de índole político, incluyendo actuaciones conjuntas concretas de colaboración en el marco de la Estrategia Europea sobre inteligencia artificial y el Pacto Verde Europeo, un plan para acelerar las inversiones en inteligencia artificial o la coordinación y estímulo de las estrategias nacionales de inteligencia artificial.

Si nos centramos en el plano estrictamente normativo, el Reglamento sobre inteligencia artificial, a que ya hicimos alusión en varias ocasiones, resulta sin lugar a dudas decisivo, pues aborda los riesgos vinculados al uso de determinados sistemas de inteligencia artificial, incluyendo la gestión algorítmica.

Al tratarse de una norma general, es decir, que trasciende el ámbito laboral, resulta necesario abordarla desde el prisma de esta particular perspectiva, para lo que se han sugerido varios núcleos clave: las definiciones, los principios orientadores, los ámbitos laborales prohibidos y de alto riesgo y las garantías de aplicación y régimen sancionador[67]. Como recuerda el considerando 6 del Reglamento, con ello se logra "ofrecer seguridad jurídica, armonización y una

---

[66] Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI)). Un comentario puede leerse en Rojo Torrecilla, E. (2022), "Importante Resolución de Parlamento Europeo, de 3 de mayo, sobre la inteligencia artificial en la era digital. Unas notas descriptivas de su contenido laboral, y atención a la nueva bibliografía existente sobre IA", *El Blog de Eduardo Rojo. El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales*, 8-5-20222, fecha de consulta 8 mayo 2022, en http://www.eduardorojotorrecilla.es/2022/05/importante-resolucion-de-parlamento.html.

[67] Mercader Uguina, J. R. (2024). "El reglamento de Inteligencia Artificial entra en la recta final, una primera lectura en clave laboral", *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 67, Iustel.

amplia aceptación, al mismo tiempo que se proporciona la flexibilidad necesaria para adaptarse a los rápidos avances tecnológicos en este campo".

Por lo que respecta a las definiciones, ya hemos adelantado que tanto el Consejo de Europa, como la Unión Europea y la OCDE se encuentran perfectamente alineadas, es decir, las definiciones de Convenio y Reglamento toman como referencia la que en su momento propusiera esta última organización internacional[68]. De hecho, en el caso del Convenio la asume tal cual, mientras que el Reglamento introduce algunas diferencias que no revisten especial importancia en lo que hace al objeto del presente trabajo.

En lo que respecta a sus principios orientadores y objetivos, el Reglamento pretende garantizar que los sistemas de inteligencia artificial comercializados y utilizados en la UE sean seguros y respeten los derechos fundamentales, destacando la igualdad de trato y no discriminación. Asimismo, aborda retos inherentes al uso de la inteligencia artificial como la existencia de sesgos (incluido el de género[69]) y la falta de responsabilidad, entre otras cosas, estableciendo requisitos para los conjuntos de datos de alta calidad, lo que ayuda a abordar el riesgo de discriminación.

Para alcanzar estos objetivos, el Reglamento sigue un enfoque basado en el riesgo, que diferencia entre los usos de la inteligencia artificial que crean un riesgo inaceptable y, por tanto, prohibido, un riesgo alto y un riesgo bajo o mínimo. Para los dos primeros se establecen restricciones o limitaciones.

Dentro las prácticas prohibidas, se identifican hasta un total de ocho que se consideran como inaceptables, entre las que sobresalen, por su repercusión en el trabajo, las siguientes: 1) las que utilicen técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el efecto de alterar de manera sustancial el comportamiento de una persona o grupo; 2) las que exploten vulnerabilidades de una persona o grupo derivadas de su edad o discapacidad, o de una situación social o económica específica; 3) las que pretendan evaluar o clasificar a personas o grupos

---

[68] OECD (2019). *Recommendation of the Council on Artificial Intelligence*, OECD, fecha de consulta 2 abril 2024, en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[69] Casas Baamonde, M. E. (2020). "El Derecho del Trabajo, la digitalización del trabajo y el trabajo a distancia", *Derecho de las relaciones laborales*, núm. 11, Francis Lefebvre, pp. 1413-1437.

atendiendo a su comportamiento social o a características personales para provocarles un trato perjudicial o desfavorable; 4) las que detecten emociones de una persona en los lugares de trabajo, salvo las justificadas por motivos médicos o de seguridad; y 5) los sistemas de categorización biométrica de las personas para deducir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.

Uniendo algunas de estas (en particular las tres últimas) con las que ya existían en el ámbito de la protección de datos de carácter personal (Reglamento 2016/679 (UE)), el art. 7 de la Directiva sobre la mejora de las condiciones de trabajo de las personas que trabajan a través de plataformas laborales digitales prohíbe el uso de datos personales obtenidos del propio trabajo en plataformas o empleados para alguna finalidad propia del trabajo en plataformas[70] mediante sistemas automatizados o semiautomatizados[71] de supervisión o de toma de decisiones. Aún así, el encaje no es completo, pues las prácticas prohibidas por el Reglamento de IA lo son con independencia del tipo de dato que respiren. Dicho de otra forma, se ha perdido una buena oportunidad para concretar en qué se traducen, el ámbito del trabajo de plataformas, algunas de estas prohibiciones, como la relativa a la evaluación o clasificación a personas o grupos atendiendo a su comportamiento social o a características personales, como probablemente

---

[70] Tales prohibiciones, que no son más que concreciones de la regulación general a la particular actividad prestada en el trabajo de plataformas son: "a) tratar ningún dato personal sobre el estado emocional o psicológico de la persona que realiza trabajo en plataformas; b) tratar ningún dato personal relacionado con conversaciones privadas, tampoco los intercambios con otras personas que realicen trabajo en plataformas ni con los representantes de estas; c) recoger datos personales cuando la persona que realiza trabajo en plataformas no esté ofreciendo ni realizando trabajo en plataformas; d) tratar datos personales para predecir el ejercicio de los derechos fundamentales, en particular el derecho de asociación, el derecho de negociación y a la acción colectivas o el derecho a la información y consulta, tal como se definen en la Carta; e) tratar datos personales para inferir el origen racial o étnico, la situación migratoria, las opiniones políticas, las convicciones religiosas o filosóficas, la discapacidad, el estado de salud, en particular las enfermedades crónicas o el VIH, el estado emocional o psicológico, la afiliación sindical, la vida sexual o la orientación sexual de una persona; y f) tratar datos biométricos, tal como se definen en el artículo 4, punto 14, del Reglamento (UE) 2016/679, de una persona que realiza trabajo en plataformas para establecer su identidad mediante el cotejo de sus datos con los datos biométricos de personas físicas almacenados en una base de datos". No obstante, existen algunas diferencias a las que conviene prestar atención entre una y otra norma. A este respecto, véase Valverde Asencio, J. A. (2023), "La propuesta de Directiva sobre trabajo en plataformas", *Temas laborales: Revista andaluza de trabajo y bienestar social*, Vol. 168, pp. 321-326.

[71] Art. 7.3.

el ejemplo más destacado. En todo caso, supone un avance significativo ante las limitaciones que en este concreto ámbito presentaba el RGPD[72].

Por lo que respecta a las prácticas de alto riesgo, además, de una descripción general de su caracterización, se recoge expresamente en el anexo III las siguientes relacionadas con el empleo y la formación profesional: 1) sistemas de IA destinados a la contratación y la selección, en particular para publicar anuncios de empleo específicos, analizar y filtrar las solicitudes de empleo y evaluar a los candidatos; y 2) sistemas de IA destinados a la adopción de decisiones que afecten a las condiciones laborales, a la promoción o despido, a la asignación de tareas a partir de comportamientos, rasgos o características personales, o bien para supervisar y evaluar el rendimiento y el comportamiento de los trabajadores. Aparte de ello, con carácter general, aunque de evidente repercusión sobre la gestión del empleo, se incluyen también dentro de los sistemas de IA de alto riesgo los que utilicen la biometría, en la que medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable[73].

De la consideración como de alto riesgo se deriva su sometimiento a una serie de garantías de efectividad, que van más allá de las sanciones, por más que estas sean potentes, para alcanzar materias como la gestión de riesgos (art. 9) o auditoría; las prácticas adecuadas de gestión y gobernanza de datos (art.10); exigencias de documentación técnica (art. 11) y de registro (art. 12); de transparencia y suministro de información a los usuarios (art. 13); la supervisión humana (art. 14); y la precisión, robustez y ciberseguridad (art. 15). En este amplio elenco de garantías no se encuentran, sin embargo, como puede observarse, ninguna de tipo colectivo propia del ámbito laboral[74], que quedan al arbitrio de su desarrollo en el ámbito nacional, sin perjuicio de la senda que marca la Directiva

---

[72] Gil Otero, L. (2022). "Un paso (necesario) más allá de la laboralidad. Análisis y valoración de la propuesta de directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas", *Lex social: revista de los derechos sociales*, Vol. 12, núm. 1, Centro Euro-Árabe de Estudios Jurídicos Avanzados, pp. 109-112.

[73] Cruz Villalon, J. (2024). "El control del impacto laboral de la inteligencia artificial", *ON ECONOMIA - El Nacional*, fecha de consulta 7 mayo 2024, en https://www.elnacional.cat/oneconomia/es/opinion/control-impacto-laboral-inteligencia-artificial-jesus-cruz-villalon_1208780_102.html

[74] Sáez Lara, C. (2022). "Gestión algorítmica empresarial y tutela colectiva de los derechos laborales", *Cuadernos de relaciones laborales*, Vol. 40, núm. 2, Escuela de Relaciones Laborales, pp. 291-292.

relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales, a que nos referiremos inmediatamente.

Aunque se ha sugerido que estas garantías de aplicabilidad podrían clasificarse en función de su desarrollo antes o después de la comercialización del producto de IA[75], lo cierto es que algunas de ellas podrían situarse a ambos lados de este límite. Tal sería el caso de la auditoría o gestión de riesgos, que se configura como un proceso iterativo continuo, lo que provoca que sea aplicable no solamente en el diseño, sino también en su implementación, con las lógicas consecuencias que de ello se derivan en relación a los sujetos responsables. Lo mismo podría decirse y por idénticos motivos de la gobernanza de los datos, por más que el art. 10 del Reglamento parezca referirse solamente al desarrollo de los sistemas de IA. De lo que no cabe duda es que las medidas relacionadas con la transparencia integrarían el núcleo duro de la fase ulterior de aplicación o desarrollo, aunque como estas, como veremos, son más contrapeso que limitación, las analizaremos en el siguiente apartado.

Algunas de estas garantías han encontrado su traducción en el concreto ámbito del trabajo de plataformas. En el caso de la gestión o auditoría de riesgos, el art. 10 de la Directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas digitales establece diversas obligaciones que actúan como límites al poder de disposición de la empresa de estas herramientas. En particular, garantiza el desarrollo de estas auditorías periódicamente y, en cualquier caso, cada dos años; la existencia de personas encargadas de su realización, que, además, deben tener la competencia, la formación y la autoridad necesarias para ejercer esa función, e, incluso, para anular las decisiones automatizadas y gozarán de protección contra el despido o su equivalente y contra medidas disciplinarias (lo que apuntaría hacia una suerte de comité auditor de la inteligencia artificial); la obligación de adoptar medidas en función de los resultados obtenidos cuando de estos se deriven un riesgo elevado de discriminación o de vulneración de derechos; y que determina-

---

[75] Cruz Villalon, J. "El control del impacto laboral de la inteligencia artificial", cit. "estos sistemas de alto riesgo, aun permitiéndose su despliegue, se someten a estrictos controles antes de su comercialización, entre los que destaca la realización de una precisa evaluación y mitigación de los riesgos, especialmente aquellos que puedan provocar tratamientos discriminatorios, registro de la actividad y trazabilidad de los resultados, con especial exigencia de supervisión humana a través de medidas adecuadas".

dos tipos de decisiones, en concreto, las de restringir, suspender o poner fin a la relación contractual o a la cuenta de una persona sea adoptada por un ser humano.

Muy relacionada con esta obligación, el art. 11 del mismo cuerpo legal prevé el derecho a la revisión humana de decisiones adoptadas o respaldadas por un sistema automatizado de toma de decisiones, que tiene un carácter bifronte, pues, por una parte, obliga a informar sobre determinados extremos a que nos referiremos más adelante, pero, por otra, impone que las plataformas digitales de trabajo proporcionen a las personas que realizan trabajo en plataformas acceso a una persona de contacto para debatir y aclarar los hechos, circunstancias y motivos que hayan conducido a la decisión. Tales personas de contacto deberán contar con la competencia, la formación y la autoridad necesarias para ejercer esa función.

Como complemento de lo anterior, las personas que realizan trabajo en plataformas y los representantes que actúen en su nombre tendrán derecho a solicitar a la plataforma digital de trabajo que revise tales decisiones. La plataforma digital de trabajo responderá a esa solicitud facilitando a la persona que realiza trabajo en plataformas una respuesta suficientemente precisa y adecuadamente motivada en forma de documento escrito que podrá estar en formato electrónico, sin demora indebida y, en cualquier caso, en el plazo de dos semanas a partir de la recepción de la solicitud (art. 11.3). Cuando se constante que existe vulneración de derechos de la persona que realiza trabajo en plataformas, la plataforma digital de trabajo rectificará dicha decisión sin demora y, en cualquier caso, en el plazo de dos semanas a partir de la adopción de la decisión. Si dicha rectificación no fuera posible, la plataforma digital de trabajo ofrecerá una indemnización adecuada por los daños sufridos. En cualquier caso, la plataforma digital de trabajo adoptará las medidas necesarias, incluyendo, si procede, una modificación del sistema automatizado de toma de decisiones o la interrupción de su uso, con el fin de evitar tales decisiones en el futuro (art. 11.4).

En suma, tanto las prohibiciones expresas, ya sean absolutas o relativas, como las garantías de aplicación tienen un mínimo común denominador, que es poner límites al uso de la gestión algorítmica y la inteligencia artificial, lo que en la esfera del Derecho del Trabajo se traduce en establecer límites al poder de dirección, o lo que es lo mismo, a pesar de la modernidad, ejercer su función clásica[76].

---

[76] Rivero Lamas, J. (1986). *Limitación de los poderes empresariales y democracia industrial*, : Universidad, Secretariado de Publicaciones, Zaragoza.

Sin embargo, en muchas ocasiones, no se trata simplemente de establecer límites al poder de dirección, en el sentido clásico de constreñir, restringir y, en algunos casos, incluso, prohibir el libre ejercicio de determinadas facultades o facetas de ese poder. Al contrario, no son pocas las medidas planteadas en que tales límites son más sutiles o indirectos o, incluso, resultan de la voluntad de los distintos sujetos que integran la empresa, ya sea de forma acordada o por separado. De hecho, en el debate en torno a la digitalización no son infrecuentes las referencias a determinados aspectos éticos que habría de conducir la utilización de las herramientas digitales en el seno de la empresa, alcanzando lo que se venido a llamar "empresa tecnológicamente responsable", es decir, aquella capaz de integrar los riesgos derivados de la digitalización y actuar para prevenirlos[77].

Pero junto a la previsión del riesgo y la prevención del daño, se han enumerado otros principios éticos que han de regir la gestión en la empresa de las herramientas digitales[78] y que, en buena medida, han terminado por encontrar hueco, en mayor o menor medida, también en el ámbito normativo. Tal es el caso del respeto a la autonomía humana, lo que incluye aspectos tan significativos desde un punto de vista práctico como la realización de auditorías de impacto sobre los derechos laborales, la información y la participación en torno al gobierno de las herramientas digitales y la capacidad de supervisión humana de tales herramientas; la garantía de la equidad, en el sentido de que los sistemas tecnológicos estén libres de sesgos injustos, discriminación y estigmatización, pero también de aprovecharlos al máximo para fomentar la igualdad de oportunidades; o el respeto del principio de explicabilidad, que se basa en que los sistemas de inteligencia deben ser transparentes y, por tanto, explicables directamente a las personas trabajadoras y sus representantes[79].

---

[77] Mercader Uguina, J. R. (2018). "Riesgos laborales y transformación digital: hacia una empresa tecnológicamente responsable", *Teoría y derecho: revista de pensamiento jurídico*, núm. 23, Tirant lo Blanch, pp. 92-107.

[78] Goñi Sein, J. L. (2019). "Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo", *Documentación Laboral*, núm. 117, Cinca, pp. 66-70.

[79] Lo cual se materializa en tres aspectos básicos, la trazabilidad, la explicabilidad y la comunicación. *Ibid.*, p. 71.

Junto a los anteriores principios ético-jurídicos, sigue gozando de un vigor envidiable el principio de proporcionalidad[80]. De revestimiento más jurídico, resulta dudoso que tenga un trasfondo ético menor que los anteriores. Ello viene dado en buena medida por el papel que cumple en esa confrontación a la que venimos prestando atención entre el poder empresarial y los derechos de las personas trabajadoras, cual es la de ponderar los distintos elementos en juego de tal suerte que se pueda obtener una solución en torno alcance de uno y otro y, por lo que aquí respecta, sobre los límites y contrapoderes del poder empresarial.

4.2. Herramientas basadas en la introducción de transparencia

Junto a la imposición de limitaciones el empleo de las facultades que integran el poder empresarial, el ordenamiento jurídico ha venido incluyendo algunas medidas basadas en el establecimiento de contrapesos o contrapoderes. De lo que se trata es de situar a las partes en una situación equiparable, de tal suerte que las negociaciones entre ellos puedan derivar en resultados óptimos o eficientes.

Estas han estado protagonizadas de forma destacada por un ensanchamiento del derecho a la información, fundamentalmente de la representación legal de las personas trabajadoras, pero también de ellas mismas e, incluso, sujetos al margen de la relación laboral. Así, bajo el paraguas de la "transparencia", lo que se ha hecho ha sido ensanchar derechos tradicionales de acceso a la información y crear manifestaciones nuevas en un ámbito, el de las plataformas y la inteligencia artificial, caracterizado precisamente por su opacidad. Si la información es poder, eliminando o limitando su monopolio por una de las partes reducimos el suyo e incrementamos el de la contraparte.

El término jurídico de "transparencia", pues, en general, es un concepto polisémico y transversal que concierne a una amplia variedad de disciplinas[81], nace en el ámbito público precisamente para combatir la creciente opacidad de

---

[80] Mercader Uguina, J. R., *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, cit., pp. 165-170.

[81] Cotino Hueso, L. (2022). "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad...). Para qué, para quién y cuánta", Cotino Hueso, L. y Castellanos Claramunt, J. (eds.) *Transparencia y explicabilidad de la inteligencia artificial*, 1a edición, Tirant lo Blanch, Valencia, pp. 25-70.

gobiernos y administraciones y expandir, entre otros, el derecho a la información[82]. A partir de ahí, salta al sector privado, alcanzando lógicamente el ámbito laboral, y adquiere nuevos tintes con la Cuarta Revolución Industrial, hasta el punto no solamente de poder hablar de "transparencia algorítimica", sino de configurarse como un auténtico principio vertebrador del gobierno de los algoritmos, la robótica y la inteligencia artificial[83].

En este sentido, ya hemos hecho mención a que el art. 8 del Convenio Marco sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho obliga a las partes a "garantizar que existan requisitos adecuados de transparencia y supervisión adaptados a los contextos y riesgos específicos con respecto a las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial, incluso en lo que respecta a la identificación de contenidos generados por sistemas de inteligencia".

Por su parte, ya vimos que el Reglamento de inteligencia artificial establece en su artículo 13 que los sistemas de IA de alto riesgo se diseñen y desarrollen de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida. Esto, traducido al ámbito laboral, implica el establecimiento de importantes obligaciones a quien es responsable de su despliegue, esto es, el empleador.

Así, como regla específica en el campo laboral, se impone que, antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los empleadores informen tanto a la representación legal de las personas trabajadoras como a estas individualmente consideradas de que se encuentran expuestos a la utilización de un sistema de IA de alto riesgo. Además, este deber de información en que se traduce el principio de transparencia ha resultado enriquecido por un acompañante no menor, que es la explicabilidad. No basta con proporcionar la información, sino que esta ha de adaptarse a la audiencia de tal forma que sea inteligible. Así, la explicabilidad es "la capacidad de generar una explica-

---

[82] Guichot, E. (2020). "Transparencia", Pendás, B. y Herrero de Miñón, M. (eds.), *Enciclopedia de las Ciencias Morales y Políticas para el siglo XXI*, Boletín Oficial del Estado, Madrid, pp. 1122-1125.

[83] Cotino Hueso, L. "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad...). Para qué, para quién y cuánta", cit., p. 30.

ción sobre el comportamiento del modelo a partir de los datos utilizados, de los resultados obtenidos y del proceso completo de la toma de decisión en función de la audiencia o perfil de los destinatarios a los que se dirige la explicación"[84]. Por si todo esto fuera poco, cuando se trate de sistemas de IA de alto riesgo, estos deberán ir acompañados instrucciones de uso que incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios y cuyo contenido mínimo se determina expresamente (art. 13.3).

Junto al Reglamento, dos directivas contribuyen a reforzar la transparencia en este concreto ámbito. Con carácter general, la Directiva (UE) 2019/1152 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a unas condiciones laborales transparentes y previsibles en la Unión Europea[85]. A falta de la aprobación del texto definitivo de su transposición, el proyecto de Ley[86] no se aparta en exceso de la norma europea, por lo que, en lo que hace al objeto del presente estudio, interesa destacar, la ampliación de los derechos de información individual en lo que respecta a los aspectos esenciales y cualesquiera otros que deriven específicamente del contrato. Aunque es este un avance significativo y puede contribuir a arrojar transparencia en el ámbito de las plataformas, lo cierto es que se trata de un derecho de escaso contenido digital.

De ahí la importancia que, con carácter específico, reviste la Directiva sobre la mejora de las condiciones de trabajo de las personas que trabajan a través de plataformas laborales digitales[87], pues introduce mayor transparencia a través de varios mecanismos. Para empezar, mediante la obligación de proporcionar información sobre el uso de sistemas automatizados de supervisión o de toma de decisiones, a las personas que realizan trabajo en plataformas, a los representan-

---

[84] Mercader Uguina, J. R. "El reglamento de Inteligencia Artificial entra en la recta final, una primera lectura en clave laboral", cit., p. 340.

[85] DOUE de 11 de julio de 2019, núm. 186. Para un estudio completo, véase Miranda Boto, J. M., *Condiciones de trabajo transparentes y previsibles. Desafíos para el Derecho español en la Transposición de la Directiva (UE) 2019/1152*, Valencia, Tirant lo Blanch, 2023.

[86] BOCG de 16 de febrero de 2024, Serie A, núm. 8-1.

[87] Además de todo lo anterior, debe tenerse presente que estas propuestas regulatorias no se hacen en el vacío, pues ya se cuenta con un asidero importante el RGPD (desarrollado en España por la LOPD). Estos tres serían los pilares fundamentales que en la actualidad tendría lo que se ha venido a llamar la gobernanza multinivel de la inteligencia artificial. Baz Rodríguez, J., "Responsabilidad algorítmica y gobernanza de la inteligencia artificial en el ámbito sociolaboral. Entre la perspectiva y la prospectiva", cit.

tes de las personas trabajadoras de plataformas y, si así lo solicitan, a las autoridades nacionales competentes (arts. 9 y 10). En concreto, la información que ha de suministrarse en todo caso comprendería tres ámbitos:

En primer lugar, todos los tipos de decisiones respaldadas o adoptadas por sistemas automatizados de toma de decisiones, también cuando respalden o adopten decisiones que no afecten de manera significativa a personas que realicen trabajo en plataformas.

En segundo lugar, por lo que respecta a los sistemas automatizados de supervisión: a) que tales sistemas están en uso o en proceso de introducción; b) las categorías de datos y acciones controlados, supervisados o evaluados por tales sistemas, incluida la evaluación por el destinatario del servicio; c) el objetivo del sistema de supervisión y el modo en que el sistema debe lograr dicho objetivo; y d) los destinatarios o categorías de destinatarios de los datos personales tratados por dichos sistemas y toda transmisión o transferencia de dichos datos personales, también dentro de un grupo de empresas.

Por último, en lo concerniente a los sistemas automatizados de toma de decisiones: a) que tales sistemas están en uso o en proceso de introducción; b) las categorías de decisiones adoptadas o respaldadas por tales sistemas; c) las categoría de datos y los principales parámetros que tales sistemas tienen en cuenta, y la importancia relativa de esos parámetros principales en la toma de decisiones automatizada, incluida la forma en que los datos personales o el comportamiento de la persona que realiza trabajo en plataformas influyen en las decisiones; y d) los motivos de las decisiones de restringir, suspender o cancelar la cuenta de la persona que realiza trabajo en plataformas, de denegarle el pago por el trabajo realizado, y de las decisiones sobre su situación contractual o cualquier decisión con efectos equivalentes o perjudiciales. En relación con esto, el art. 11 aclara que las personas que realizan trabajo en plataformas tienen derecho a obtener una explicación de la plataforma digital de trabajo, "sin demora indebida, en relación con cualquier decisión adoptada o respaldada por un sistema automatizado de toma de decisiones. La explicación, oral o escrita, se presentará de manera transparente e inteligible, sirviéndose de un lenguaje claro y sencillo". Tal explicación, deberá darse necesariamente por escrito cuando verse "sobre los motivos de cualquier decisión respaldada o, en su caso, adoptada por un sistema automatizado de toma de decisiones de restringir, suspender o cancelar la cuenta de la persona que realiza trabajo en plataformas,

cualquier decisión de denegar la remuneración por el trabajo realizado a la persona que realiza trabajo en plataformas, cualquier decisión sobre la situación contractual de la persona que realiza trabajo en plataformas, cualquier decisión con efectos similares o cualquier otra decisión que afecte a los aspectos esenciales del empleo u otras relaciones contractuales, sin demora indebida y a más tardar el día en que surta efecto".

Tanto en un caso como en otro, esto es, ya se trate de sistemas automatizados de supervisión o de toma de decisiones, es necesario recordar que también existe obligación de informar de los resultados de la auditoría o evaluación, conforme a lo dispuesto en el art. 10.4. Este derecho de información se aplica a los tres sujetos indicados anteriormente, persona trabajadora o prestadora del servicio, representantes y autoridades administrativas si así lo solicitan.

Al margen de los sistemas automatizados y semiautomatizados, la Directiva extiende el principio de transparencia a otros ámbitos (art. 17), de tal suerte que las plataformas digitales de trabajo deberán poner a disposición de las autoridades competentes, así como de los representantes de personas que realizan trabajo en plataformas, la siguiente información: a) el número de personas que realizan trabajo en plataformas desglosado por nivel de actividad y por situación contractual o laboral; b) las condiciones generales determinadas por la plataforma digital de trabajo y aplicables a dichas relaciones contractuales; c) la duración media de la actividad, el número de horas semanales trabajadas por término medio por persona y los ingresos medios derivados de la actividad de las personas que realizan trabajo en plataformas con regularidad a través de la plataforma digital de trabajo de que se trate; y d) los intermediarios con los que la plataforma digital de trabajo tiene una relación contractual. Como complemento de esto, la representación de las personas que realizan trabajo en plataformas tendrá derecho a lo que se ha venido a denominar "transparencia activa"[88], esto es, a solicitar aclaraciones y datos adicionales a las plataformas digitales de trabajo en relación con cualquier información facilitada, incluidos los detalles del contrato laboral. Las plataformas digitales de trabajo responderán a tal solicitud proporcionando sin demora indebida una respuesta motivada.

---

[88] Valverde Asencio, J. A. "La propuesta de Directiva sobre trabajo en plataformas", cit., p. 334.

Junto al tipo de información que se ha de suministrar, la Directiva también se refiere al modo, distinguiendo entre la que se provee a las personas trabajadoras y a sus representantes. No obstante, en todo caso, la información ha de entregarse por escrito, incluyendo formato electrónico, y de forma transparente, inteligible y fácilmente accesible, sirviéndose de un lenguaje claro y sencillo (art. 9.2).

En el caso de la información individual, esta será concisa, sobre los sistemas y las características de estos que les afecten directamente y, en particular, en su caso, sobre sus condiciones laborales. Se suministrará, a más tardar, el primer día hábil, previamente a la introducción de cambios que afecten a las condiciones laborales, la organización del trabajo o la supervisión de su ejecución, o en cualquier momento a petición suya. También recibirán información exhaustiva y detallada a petición suya sobre todos los sistemas pertinentes y las características de estos. Dicha información se extenderá a la fase precontractual, aunque, en este caso, "solo se referirá a los sistemas automatizados de supervisión o de toma de decisiones utilizados en dicho procedimiento y se facilitará antes del inicio de dicho procedimiento"[89].

En el lado colectivo, la información será pormenorizada y detallada[90] y referida a todos los sistemas pertinentes y las características de estos. Tal información se recibirá antes de utilizar dichos sistemas o previamente a la introducción de cambios que afecten a las condiciones laborales, a la organización del trabajo o a la supervisión de su ejecución, o en cualquier momento a petición suya. Además, el art. 13 señala expresamente que los derechos de información y consulta de la Directiva 2002/14/CE abarcan las decisiones que puedan conducir a la introducción de sistemas automatizados de supervisión o de toma de decisiones o a cambios sustanciales en el uso de dichos sistemas. Cuando se trate de uno u

---

[89] La redacción del precepto es algo confusa, pues en un primer momento se remite a toda la información que, con carácter general, se provee a cualquier persona trabajadora, aunque parece que el último inciso, restringe la remisión a las dos áreas señaladas. Aún así, las contradicciones no acaban, pues el artículo se refiere a los sistemas automatizados de supervisión, que se definen como "sistemas que se utilizan para supervisar, controlar o evaluar, por medios electrónicos, la ejecución del trabajo de personas que realizan trabajo en plataformas o actividades realizadas en el entorno laboral, en particular mediante la recopilación de datos personales, o que sirven para respaldar tales acciones", lo que implica que la actividad profesional ya se está desarrollando y que, por tanto, se ha superado un proceso de selección, aun cuando aquella estuviera sometida a período de prueba.

[90] También de este modo las autoridades nacionales competentes en cualquier momento a petición suya.

otro y el modo dependerá de las concretas circunstancias del caso, es decir, si el evento que lleve aparejado la introducción del sistema de IA conlleva un derecho u otro (por estar relacionados, por ejemplo, con despidos colectivos, sería consulta) o, en caso contrario, porque se elija expresamente una de las dos opciones.

En relación con esto, este precepto establece una garantía adicional, pues declara expresamente el derecho de la representación a contar con la asistencia de un experto de su elección, en la medida en que lo necesiten para examinar el asunto objeto de información y consulta, y formular un dictamen. Además, cuando una plataforma digital de trabajo tenga más de doscientos cincuenta personas trabajadoras, los gastos del experto correrán a cargo de la plataforma digital de trabajo, siempre que sean proporcionados. Los Estados miembros podrán determinar la frecuencia de las solicitudes de expertos, garantizando al mismo tiempo la eficacia de la asistencia.

De no tener representantes, establece el art. 14 que las plataformas digitales de trabajo informarán directamente a los trabajadores de plataformas afectados sobre las decisiones que puedan conducir a la introducción de sistemas automatizados de supervisión o de toma de decisiones o a cambios sustanciales en el uso de dichos sistemas. La información se facilitará en forma de documento escrito que podrá estar en formato electrónico y se presentará de forma transparente, inteligible y fácilmente accesible, sirviéndose de un lenguaje claro y sencillo.

De aquí surgen dos dudas. Por una parte, parece que, en defecto de representación, el modo en que se provee la información a las personas trabajadoras cambia, pues no se dice, como en el caso de aquella, que la información haya de ser pormenorizada y detallada. Esto puede obedecer a que, al tratarse de empresas pequeñas, se piense que el volumen de información va a ser más escaso, pero dadas las dificultades técnicas de la materia, no se entiende este cambio de criterio, máxime cuando se está regulando el caso subsidiario en ausencia de representación.

Por otra parte, esta obligación se concibe sólo en defecto de representación, lo que conduciría a una cierta contradicción con lo dispuesto en el art. 9.3 que, como vimos, establece el derecho individual a recibir "información concisa sobre los sistemas y las características de estos que les afecten directamente, en particular, en su caso, sobre sus condiciones laborales, a más tardar el primer día hábil, previamente a la introducción de cambios que afecten a las condiciones laborales, la organización del trabajo o la supervisión de la ejecución del trabajo". Comparando ambos preceptos, parece que el art. 14 se refiere única y exclusivamente

a la introducción de sistemas de IA, mientras que el 9.3, al modo en que su funcionamiento o los cambios que se articulen sobre él pueda afectar a sus condiciones de trabajo o de su organización. De ser esta interpretación correcta, parece contradictorio que, cuando existe representación, puedan recibir información directamente una vez implantado el sistema de IA, pero no antes, en relación a la propia potencial implantación. Es cierto que la representación puede encargarse de esta tarea, pero el legislador europeo ha sido ciertamente algo cicatero en este sentido, pues nada impedía que las personas trabajadoras recibieran también esta información, máxime cuando la propia Directiva impone un grado de detalle menor que en el caso de información directa acompañada de la indirecta a través de la representación de las personas trabajadoras.

Pero también puede ocurrir que la ausencia de representación no sea total, existiendo de las personas que prestan servicios por cuenta propia. En este caso, el art. 15 señala que podrán ejercer los derechos conferidos a los representantes de las personas trabajadoras en virtud del artículo 8, apartado 2 (protección de datos), el artículo 9, apartados 1 y 4 (sistemas automatizados), el artículo 10, apartado 4 (auditoría de los sistemas automatizados), y el artículo 11, apartado 2 (revisión humana), "únicamente en la medida en que actúen en nombre de personas que realizan trabajo en plataformas que no sean trabajadores de plataformas en lo que respecta a la protección de sus datos personales". De nuevo, este precepto plantea también algunos interrogantes.

Comenzando por este último inciso, la referencia a los datos personales debe entenderse como una habilitación expresa a que su capacidad de representación pueda extenderse también a estos, especialmente si se tiene en cuenta lo dispuesto en el art. 8. Lo contrario, entender que su capacidad de representación únicamente se efectúa en lo que respecta a los datos personales, además de ser una restricción desproporcionada respecto de otras fórmulas de representación, dejaría sin contenido la ejercida en relación a los sistemas automatizados y su auditoría y la aplicación del principio "humano al mando", pues estos mecanismos emplean tanto datos personales como no personales.

Por otra parte, el precepto se refiere a "los representantes de las personas que realizan trabajo en plataformas distintos de los representantes de los trabajadores". De ello hay que deducir, que, cuando la representación de las personas trabajadoras, en el caso español, los sindicatos, representen también a las personas trabajadoras por cuenta propia, sus prerrogativas permanecen intactas, pudiendo

ejercer la representación en las mismas áreas que para las personas trabajadoras por cuenta ajena, pues esta norma especial se refiere solo a las fórmulas de representación distintas a esta, en nuestro caso, las asociaciones de autónomos o empresariales. Esta interpretación deja a esta última forma de representación en una situación de desventaja, aunque nada impide potenciar, en aras de una mayor efectividad, unos tipos de representación frente a otros.

Por último, también contribuye a impulsar la transparencia la obligación establecida en el art. 20 de crear la posibilidad de que las personas que realizan trabajo en plataformas y sus representantes se pongan en contacto y se comuniquen entre ellas en privado y de manera segura a través de la propia plataforma, por cuanto que permite a la contraparte beneficiarse de las ventajas que esta proporciona en lo que hace a la facilidad para intercambiar flujos de información y comunicarse.

Pero si la acción europea ha sido notable, España no se ha quedado atrás en estos primeros compases de la regulación de la esfera laboral del fenómeno digital. Nuestro país ha sido pionero en regular las condiciones de trabajo en plataformas a través de los cambios operados por la Ley 12/2021[91]. A través de esta ley, se han introducido herramientas nuevas de información en materia de gestión algorítmica e inteligencia artificial. Dicho esto, no es menos cierto que la acción reguladora no ha hecho más que empezar y, aunque sea solo por tener que introducir las adaptaciones necesarias de progresar las iniciativas europeas antes mencionadas, España deberá seguir regulando, todo ello sin contar con el hecho de que se decidiera seguir un paso por delante.

De acuerdo con la normativa española, la empresa está obligada a facilitar todo dato que sea necesario para el ejercicio de las actividades propias de la representación de los trabajadores. En este sentido, cualquiera de las bases jurídicas que habilitan el acceso a datos de carácter personal servirían, con mayor motivo, para los no personales. Esto, que ya era posible antes de la reforma laboral de 2021, ha encontrado un refuerzo significativo con la inclusión del aparado d) del art. 64.4, que señala que el comité tendrá derecho a "ser informado

---

[91] Un estudio de conjunto de la normativa española y europea puede encontrarse en Fernández García, A. (2023). "Los algoritmos y la inteligencia artificial en la Ley 12/2021, de 28 de septiembre", en Moreno i Gené, J. y Romero Burillo, A. M. (eds.). *Los nuevos escenarios laborales de la innovación tecnológica*, Tirant lo Blanch, pp. 159-190.

por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles". Este deber de información incluye, por consiguiente, tanto los datos personales como no personales y, también, tanto lo que podríamos llamar datos "ordinarios" como los de carácter confidencial, si bien en relación a estos últimos la representación de los trabajadores estará obligada a guardar un especial deber de sigilo (art. 65.1 y 2 ET).

No obstante, no debe olvidarse que el art. 65.4 ET dispone que "excepcionalmente, la empresa no estará obligada a comunicar aquellas informaciones específicas relacionadas con secretos industriales, financieros o comerciales cuya divulgación pudiera, según criterios objetivos, obstaculizar el funcionamiento de la empresa o del centro de trabajo u ocasionar graves perjuicios en su estabilidad económica"[92]. La jurisprudencia ha interpretado esta regla como una excepción a la general que, como hemos dicho, permitiría el acceso a la información de carácter confidencial a la representación de los trabajadores siempre que guarden el deber de sigilo. Como excepción, además, debe aplicarse de forma restrictiva (STS 6 de febrero de 2019, Rec. núm. 224/2017[93]).

Es más, cuando se recurre a la regulación especial, la Ley 1/2019, de 20 de febrero, de Secretos Empresariales[94] contiene normas aparentemente mucho más permisivas en cuanto al acceso de la representación de los trabajadores a la información catalogada como secreto empresarial. Así, el art. 1.3 dispone que "la protección de los secretos empresariales no afectará a la autonomía de los interlocutores sociales o a su derecho a la negociación colectiva". Por su parte, el art. 2. c) establece que la obtención de información constitutiva de secreto empresarial se considerará lícita cuando sea necesaria para "el ejercicio del derecho de los trabajadores y los representantes de los trabajadores a ser informados y consultados, de conformidad con el Derecho europeo o español y las prácticas vigentes".

De la dicción literal de estos dos preceptos podría pensarse en una derogación tácita de la excepción prevista en el art. 65.4 ET, pues, al fin y al cabo, para

---

[92] Esta excepción no abarca aquellos datos que tengan relación con el volumen de empleo en la empresa.

[93] ECLI:ES:TS:2019:615.

[94] BOE de 21 de febrero de 2019, núm. 45.

que la protección de los datos confidenciales no afecte a la autonomía de los interlocutores sociales y a la negociación colectiva ha de permitirse en todo caso el acceso, máxime cuando la Ley lo considera siempre como lícito y, además, está garantizado por el deber de sigilo. Además, el art. 6 de la Directiva 2002/14/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 2002, por la que se establece un marco general relativo a la información y a la consulta de los trabajadores en la Comunidad Europea[95], que dio pie a la actual redacción del art. 65 ET, establecía la posibilidad de negar el acceso como una opción para los Estados, que no para los sujetos privados.

Para otros autores, sin embargo, la nueva regulación no habría introducido ningún cambio en nuestro ordenamiento jurídico, siendo plenamente coherente con la excepción del art. 65.4 ET[96]. El principal argumento es que la Ley 1/2019 se estaría refiriendo a otras formas de acceso distintas a la facilitación directa por parte de la empresa, lo que sería coherente con la mención que se hace en el art. 2.3 a la obtención, utilización o revelación por parte de los trabajadores cuando lo pongan en conocimiento de sus representantes en el marco del ejercicio legítimo por parte de estos de las funciones que tienen legalmente atribuidas. Así, el empresario seguiría sin estar obligado a proporcionar determinados datos que entienda que pueden afectar a secretos industriales, financieros o comerciales cuya divulgación pudiera, según criterios objetivos, obstaculizar el funcionamiento de la empresa o del centro de trabajo u ocasionar graves perjuicios en su estabilidad económica, si bien si los trabajadores o sus representantes tuvieran acceso por otros medios, esto se considera lícito y, por tanto, no podrá dar lugar a la exigencia de ningún tipo de responsabilidad.

5. CONCLUSIONES

A lo largo de estas páginas hemos tenido ocasión de analizar cómo el binomio conformado por algoritmos y plataformas conduce por naturaleza a una mayor flexibilidad y, por tanto, a un mayor poder de gestión por parte de la empresa.

---

[95] DOUE de 23 de marzo de 2002, núm. 80.

[96] López Ahumada, J. E. (2019). "La exclusión del deber de sigilo de los representantes de los trabajadores de la noción de secretos empresariales: A propósito de la Ley 1/2019 de secretos empresariales", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 148, pp. 41-66.

Lo anterior, unido a un contexto de, hasta hace poco, prácticamente total vacío normativo, hacía que esta tendencia, la del fortalecimiento de las facultades empresariales, se exacerbara. Esto ha conducido a resultados no solamente rechazables desde un punto de vista social, como son las muestras de grave precariedad que viene caracterizando a buena parte de las actividades articuladas a través de plataformas, sino rechazables desde un punto de vista económico, pues el desequilibrio entre las posiciones de las partes lleva necesariamente a resultados no estables o ineficientes.

Es por este motivo que la reacción del ordenamiento jurídico ha pivotado en torno a dos grandes núcleos normativos. Por una parte, el establecimiento de límites al poder empresarial, que se han encauzado fundamentalmente a través de una serie de prohibiciones totales o parciales cuando existe grave riesgo de lesión de los derechos fundamentales o de garantías cuando se catalogan de alto riesgo. Las exigencias de documentación técnica y de registro, la robustez y salvaguardas de ciberseguridad, la transparencia en el suministro y gestión de la información, la auditoría algorítmica, la intervención humana, las restricciones y posibilidad de revisión de las decisiones automatizadas o semiautomatizadas limitan el poder de dirección empresarial en aras de otorgar una mejor protección a los derechos de las personas trabajadoras. Por si todo esto fuera poco, nuevos principios, como el de transparencia, u otros no tan nuevos, como el de proporcionalidad, han apuntado, con una fuera jurídica diferente, en la misma dirección.

Por otra, la introducción de diferentes medidas tendentes a mejorar la transparencia en el uso de la información en el seno de la empresa pretende situar a la parte más débil en una situación tal que sea capaz de contar con medios suficientes para la defensa de sus propios derechos e intereses, ya sea de forma heterónoma o en una negociación con la empresa. Aquí, no solamente se han abierto nuevos cauces para la representación legal de las personas trabajadoras, sino que se han desarrollado ámbitos prácticamente inexplorados, como el derecho a la información individual, o nada explorados, como el que tiene que ver con la actividad profesional de las personas trabajadoras autónomas. El mínimo común denominador de todas estas medidas es propiciar situaciones más equilibradas en cuanto al acceso y uso de la información.

A pesar de que las protagonistas de este estudio han sido las plataformas y los algoritmos, tanto el marco analítico como las medidas son extrapolables a buena parte de los avances tecnológicos de la presente Revolución Industrial, por cuanto, como hemos intentado demostrar, buena parte de ellos descansan en la captación y uso de la información, de los datos, lo que propiciaría que la flexibili-

dad tecnológica y el poder que de ella se deriva fueran especialmente intensas en comparación con otras revoluciones industriales. Ello conllevaría que, aunque las posibles soluciones sean, en abstracto, idénticas a las de otras épocas, limites y contrapoderes, varíen en cuanto su contenido, pues las presentes tecnologías exigen poner el foco en cómo se obtiene, trata y usa la información.

BIBLIOGRAFÍA

Ajunwa, I., Crawford, K. y Schultz, J. (2016). *Limitless Worker Surveillance*, Social Science Research Network, Rochester, NY.

Alameda Castillo, M. T. (2021). "Reclutamiento tecnológico. Sobre algoritmos y acceso al empleo", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 159, Consejo Andaluz de Relaciones Laborales, pp. 11-52.

Alcaide Castro, M. (1987). *Conflicto y poder en las organizaciones*, Centro de Publicaciones, Ministerio de Trabajo y Seguridad Social, Madrid.

Aloisi, A. y De Stefano, V. (2022). *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour*, Hart Publishing, Gordonsville.

Alonso Olea, M. (1987). *De la servidumbre al contrato de trabajo*, 2ª edición revevisada y ampliada, Ed. Tecnos, Madrid.

Álvarez Cuesta, H. (2020). *El impacto de la inteligencia artificial en el trabajo: desafíos y propuestas*, Aranzadi Thomson Reuters.

Baz Rodríguez, J. (2022). "Responsabilidad algorítmica y gobernanza de la inteligencia artificial en el ámbito sociolaboral. Entre la perspectiva y la prospectiva", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 89, Wolters Kluwer, p. 3.

Blackburn, R. S. (1981). "Lower participant power: Toward a conceptual integration", *Academy of Management. The Academy of Management Review (pre-1986); Briarcliff Manor*, Vol. 6, núm. 1, p. 127.

Casas Baamonde, M. E. (2020). "El Derecho del Trabajo, la digitalización del trabajo y el trabajo a distancia", *Derecho de las relaciones laborales*, núm. 11, Francis Lefebvre, pp. 1413-1437.

Cotino Hueso, L. (2022). "Transparencia y explicabilidad de la inteligencia artificial y "compañía" (comunicación, interpretabilidad, inteligibilidad, auditabilidad, testabilidad, comprobabilidad, simulabilidad...). Para qué,

para quién y cuánta", Cotino Hueso, L. y Castellanos Claramunt, J. (eds.), *Transparencia y explicabilidad de la inteligencia artificial*, 1a edición, Tirant lo Blanch, Valencia.

Cruz Villalon, J. (2024). "El control del impacto laboral de la inteligencia artificial", *ON ECONOMIA - El Nacional*, fecha de consulta 7 mayo 2024, en https://www.elnacional.cat/oneconomia/es/opinion/control-impacto-laboral-inteligencia-artificial-jesus-cruz-villalon_1208780_102.html.

Cruz Villalón, J. (2019). "Las facultades de control del empleador ante los cambios organizativos y tecnológicos", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 150, Consejo Andaluz de Relaciones Laborales.

De la Puebla Pinilla, A. (2021). "El despido por causas empresariales", Congreso Nacional de Derecho del Trabajo y de la Seguridad Social (ed.), *Reestructuraciones empresariales: XXXI Congreso de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social, Subdirección General de Informes, Recursos y Publicaciones, Madrid, Informes y estudios. Empleo.

Desdentado Bonete, A. y Desdentado Daroca, E. (2018). "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", *Revista de información laboral*, núm. 1, Lex Nova, pp. 19-39.

Desdentado Bonete, A. y Muñoz Ruiz, A. B. (2012). *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid.

El País (2024). "El caso de Alba Renai en Mediaset: ¿le pueden despedir para que un robot ocupe su sitio?", *El País*, fecha de consulta 24 marzo 2024, en https://elpais.com/economia/negocios/2024-03-24/el-caso-de-alba-renai-en-mediaset-le-pueden-despedir-para-que-un-robot-ocupe-su-sitio.html.

Eurofound (2018). *Employment and working conditions of selected types of platform work*, Publications Office of the European Union, Luxembourg.

European Parliament (2022). *AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework | Think Tank | European Parliament*, European Parliament, Brussels (Belgium), fecha de consulta 15 mayo 2022, en https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729516.

Fernández García, A. (2023). "Los algoritmos y la inteligencia artificial en la Ley 12/2021, de 28 de septiembre", Moreno i Gené, J., Romero Burillo, A. M. (eds.), *Los nuevos escenarios laborales de la innovación tecnológica*, Tirant lo Blanch, pp. 159-190.

Fernández Orrico, F. J. (2020). "Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación", Rodríguez-Piñero Bravo-Ferrer, M., Todoli Signes, A. (eds.), *Vigilancia y control en el Derecho del Trabajo Digital,* ISBN 978-84-1346-551-7, pp. 301-326, Aranzadi Thomson Reuters, pp. 301-326.

Galbraith, J. K. (1984). *El nuevo estado industrial*, Edición puesta el día, Ariel, Barcelona.

Gil Otero, L. (2023). "La economía de plataformas ante las categorías clásicas del Derecho del Trabajo", Universidade de Santiago de Compostela, p. 1.

Gil Otero, L. (2022). "Un paso (necesario) más allá de la laboralidad. Análisis y valoración de la propuesta de directiva relativa a la mejora de las condiciones laborales en el trabajo en plataformas", *Lex social: revista de los derechos sociales*, Vol. 12, núm. 1, Centro Euro-Árabe de Estudios Jurídicos Avanzados, pp. 89-121.

Ginès Fabrellas, A. (2022). "La gestión algorítmica del trabajo: nuevos retos jurídicos, tecnológicos y éticos", *Digitalización, recuperación y reformas laboralesMinisterio de Trabajo*, Ministerio de Trabajo y Economía Social, Subdirección General de Informes, Recursos y Publicaciones, Madrid, Informes y estudios. Empleo.

Goñi Sein, J. L. (2009). "Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia Laboral. Revista de Derecho del Trabajo y de la Seguridad Social*, núm. 39, pp. 11-58.

Goñi Sein, J. L. (1988). *El Respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Cívitas, Madrid.

Goñi Sein, J. L. (2019). "Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo", *Documentación Laboral*, núm. 117, Cinca, pp. 57-72.

Guichot, E. (2020). "Transparencia", en Pendás, B. y Herrero de Miñón, M. (eds.), *Enciclopedia de las Ciencias Morales y Políticas para el siglo XXI*, Boletín Oficial del Estado, Madrid.

Joyanes Aguilar, L. (2017). *Industria 4.0: la cuarta revolución industrial*, Alfaomega; Marcombo, Barcelona.

Kaufmann, A. E. (1993). *El poder de las organizaciones*, Esic, Madrid.

Kuncel, N. R., Ones, D. S. y Klieger, D. M. (2014). "In Hiring, Algorithms Beat Instinct", *Harvard Business Review*, fecha de consulta 6 mayo 2022, en https://hbr.org/2014/05/in-hiring-algorithms-beat-instinct.

López Ahumada, J. E. (2019). "La exclusión del deber de sigilo de los representantes de los trabajadores de la noción de secretos empresariales: A propósito de la Ley 1/2019 de secretos empresariales", *Temas laborales: Revista andaluza de trabajo y bienestar social*, núm. 148, pp. 41-66.

Loy, G. (2005). "El dominio ejercido sobre el trabajador", Escudero Rodríguez, R. (ed.) *El Poder de dirección del empresario: nuevas perspectivas*, 1ª edición, La Ley-Actualidad, Las Rozas, Madrid.

Luhmann, N. (1995). *Poder*, Antropos, Barcelona.

Martínez Yáñez, N. M. (2021). "Entre robots y pandemias: retos de la regulación del tiempo de trabajo en el siglo XXI", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 78, Wolters Kluwer, p. 3.

Mercader Uguina, J. R. (2022). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Tirant lo Blanch, Valencia.

Mercader Uguina, J. R. (2020). "Datos biométricos en los centros de trabajo", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. extra 11, Wolters Kluwer, p. 8.

Mercader Uguina, J. R. (2001). "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones laborales: Revista crítica de teoría y práctica*, núm. 1, Wolters Kluwer, pp. 665-686.

Mercader Uguina, J. R. (2019). "Despido de una administrativa cuyo trabajo ha sido sustituido por un Robot: ¿es posible poner Puertas al Campo?", *El Foro de Labos*, fecha de consulta 1 octubre 2019, en https://www.elforodelabos.es/2019/10/despido-de-una-administrativa-cuyo-trabajo-ha-sido-sustituido-por-un-robot-es-posible-poner-puertas-al-campo/.

Mercader Uguina, J. R. (2017). *El futuro del trabajo en la era de la digitalización y la robótica*, Tirant lo Blanch, Valencia.

Mercader Uguina, J. R (2024). "El reglamento de Inteligencia Artificial entra en la recta final, una primera lectura en clave laboral", *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 67, Iustel, p. 10.

Mercader Uguina, J. R. (2024). "El Reglamento de Inteligencia Artificial: frecuentemos el futuro", *Los Briefs de la AEDTSS, Asociación Española de Derecho del Trabajo y de la Seguridad Social,* núm. 42, fecha de consulta 20 marzo 2024, en https://www.aedtss.com/el-reglamento-de-inteligencia-artificial-frecuentemos-el-futuro/.

Mercader Uguina, J. R. (2022). "En busca del empleador invisible: algoritmos e inteligencia artificial en el derecho digital del trabajo", *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, Iustel, pp. 136-145.

Mercader Uguina, J. R. (2022). "La gestión laboral a través de algoritmos", AEDTSS, Ministerio de Trabajo y Economía Social (eds.), *Digitalización, recuperación y reformas laborales: XXXII Congreso anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social, Alicante, 26 y 27 de mayo de 2022*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid.

Mercader Uguina, J. R. (2018). "Riesgos laborales y transformación digital: hacia una empresa tecnológicamente responsable", *Teoría y derecho: revista de pensamiento jurídico*, núm. 23, Tirant lo Blanch, pp. 92-107.

Mercader Uguina, J. R. (2002). *Derecho del trabajo. Nuevas tecnologías y sociedad de la información*, Editorial Lex Nova, Valladolid.

Miranda Boto, J. M. (2023). *Condiciones de trabajo transparentes y previsibles. Desafíos para el Derecho español en la Transposición de la Directiva (UE) 2019/1152*, Valencia, Tirant lo Blanch.

OECD (2019). *Recommendation of the Council on Artificial Intelligence*, OECD, fecha de consulta 2 abril 2024, en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Olarte Encabo, S. (2020). "La aplicación de inteligencia artificial a los procesos de selección de personal y ofertas de empleo: impacto sobre el derecho a la no discriminación", *Documentación Laboral*, núm. 119, Cinca, pp. 79-98.

Pérez del Prado, D. (2022). "Los tradicionales conceptos de trabajador y empresario en un mundo digital", Mercader Uguina, J. R. y de la Puebla Pinilla, A.

(eds.), *Cambio tecnológico y transformación de las fuentes laborales. Ley y convenio colectivo ante la disrupción digital*, Tirant lo Blanch, Valencia.

Pérez del Prado, D. (2020). "Representación de los trabajadores y protección de datos de carácter personal como fuente de poder", *Documentación Laboral*, núm. 119, Cinca, pp. 57-77.

Pettigrew, A. M. (1972). "Information control as power resource", *Sociology*, Vol. 6, núm. 2, pp. 187-204.

Prassl, J. (2018). *Humans as a service: the promise and perils of work in the gig economy*, First edition, Oxford University Press, Oxford, United Kingdom; New York, NY.

Rivas Vallejo, M. P. (2022). "Sesgos de género en el uso de inteligencia artificial para la gestión de las relaciones laborales: análisis desde el derecho antidiscriminatorio", *e-Revista Internacional de la Protección Social*, Vol. 7, núm. 1, pp. 52-83.

Rivero Lamas, J. (1986). *Limitación de los poderes empresariales y democracia industrial*, Universidad, Secretariado de Publicaciones, Zaragoza.

Rodríguez Fernández, M. L. (ed.) (2019). *Plataformas digitales y mercado de trabajo*, Ministerio del Trabajo, Migraciones y Seguridad Social, Subdirección General de Información Administrativa y Publicaciones, Madrid.

Rodríguez-Piñero Royo y Hernández-Bejarano, M. (2017). *Economía colaborativa y trabajo en plataforma: realidades y desafíos*, Bomarzo.

Rodríguez-Piñero Royo, M. (2020). "Registro de jornada mediante controles biométricos: un caso de incoherencia en el Derecho del Trabajo Digital", Rodríguez-Piñero Royo, M. y Todolí Signes, A. (eds.), *Vigilancia y control en el Derecho del Trabajo Digital*, Aranzadi Thomson Reuters, pp. 273-300.

Rojo Torrecilla, E. (2022). "Importante Resolución de Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital. Unas notas descriptivas de su contenido laboral, y atención a la nueva bibliografía existente sobre IA", *El Blog de Eduardo Rojo. El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales*, 8-5 2022, fecha de consulta 8 mayo 2022, en http://www.eduardorojotorrecilla.es/2022/05/importante-resolucion-de-parlamento.html.

Sáez Lara, C. (2020). "Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria", *Nueva revista española de derecho del trabajo*, núm. 232, Aranzadi Thomson Reuters, pp. 83-126.

Sáez Lara, C. (2022). "Gestión algorítmica empresarial y tutela colectiva de los derechos laborales", *Cuadernos de relaciones laborales*, Vol. 40, núm. 2, Escuela de Relaciones Laborales, pp. 283-300.

Salvador del Rey Guanter (ed.) (2018). *Inteligencia artificial y su impacto en los recursos humanos y en el marco regulatorio de las relaciones laborales: Proyecto Technos*, La Ley Wolters Kluwer, Las Rozas (Madrid).

Sanguineti Raymond, W. (2024). "El poder de dirección ante el cambio económico y productivo y la emergencia de la inteligencia artificial", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 109, La Ley (España), p. 1.

Schmid-Drümer, M. (2016). *The situation of workers in the collaborative economy | Eurofound*, European Parliament, Brussels.

Todolí Signes, A. (2023). *Algoritmos productivos y extractivos: cómo regular la digitalización para mejorar el empleo e incentivar la innovación*, Aranzadi, Cizur Menor Navarra.

Todolí Signes, A. (2022). "Control tecnológico: una propuesta de aplicación del triple juicio de proporcionalidad conforme a la normativa europea de protección de datos", en *Digitalización, recuperación y reformas laborales. XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid, Informes y estudios. Empleo.

Todolí Signes, A. (2017). *El trabajo en la era de la economía colaborativa: la clasificación jurídica de trabajadores y autónomos y los efectos de la reputación online en la economía de las plataformas virtuales.*

Todolí Signes, A. (2022). "Prevención de riesgos laborales ante la inteligencia artificial y en la reputación digital de las personas trabajadoras", Molina Navarrete, C. y Vallecillo Gámez, M. R. (eds.), *De la economía digital a la sociedad del e-work decente: condiciones sociolaborales para una Industria 4.0 justa e inclusiva*, Aranzadi-Civitas.

Todolí Signes, A. y Hernández-Bejarano, M. (eds.) (2018). *Trabajo en plataformas digitales: innovación, derecho y mercado*, Aranzadi.

Tomlinson, J. (2007). *The Culture of Speed: The Coming of Immediacy*, SAGE.

UGT (2019). *UGT ante la digitalización: tres años de acción sindical*, Comisión Ejecutiva Confederal de UGT, Secretaría de Política Sindical, Madrid.

Valdeolivas García, Y. (2022). "Derechos de información, transparencia y digitalización", en *Digitalización, recuperación y reformas laborales. XXXII Congreso Anual de la Asociación Española de Derecho del Trabajo y de la Seguridad Social*, Ministerio de Trabajo y Economía Social Subdirección General de Información, Administrativa y Publicaciones, Madrid, Informes y estudios. Empleo.

Valverde Asencio, J. A. (2023). "La propuesta de Directiva sobre trabajo en plataformas", *Temas laborales: Revista andaluza de trabajo y bienestar social*, Vol. 168, pp. 293-338.

Zuboff, S. (2020). *La era del capitalismo de la vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*, Paidós, Barcelona.

Séptima Parte
ESTUDIO FINAL

Capítulo 17
NEUROTECNOLOGÍA Y NEURODERECHOS

Rafael Yuste
Catedrático de Ciencias Biológicas
Universidad Columbia de Nueva York
https://orcid.org/0000-0003-4206-497X

1. INTRODUCCIÓN

Los avances en la sociedad deben ir acompañados por avances en las legislaciones y en los derechos fundamentales. En una era marcada por rápidos avances tecnológicos, la conversación sobre los derechos humanos entra en una nueva frontera: los neuroderechos. Esta evolución aborda las implicaciones éticas, legales y sociales de las tecnologías que interactúan con el cerebro y el sistema nervioso periférico. Innovaciones como las interfaces cerebro-computadora (BCI), las neuroprótesis y la inteligencia artificial (IA) generativa, a pesar de tener muchas consecuencias muy positivas para la ciencia, la medicina, la economía y la sociedad, hacen también necesario el establecer y hacer cumplir reglas y directrices para que su uso en la población no tenga consecuencias negativas sobre los derechos y libertades fundamentales de los ciudadanos. Por ello, es importante establecer una serie de neuroderechos neuronales e implantarlos a nivel global. Este artículo profundiza en la esencia de los neuroderechos, sus primeras implantaciones en algunos estados y los pasos necesarios para su implementación a nivel mundial.

2. LA REVOLUCIÓN NEUROTECNOLÓGICA

Se está gestando una revolución neurotecnológica. Iniciada por la Iniciativa BRAIN de la Casa Blanca (Alivisatos, Chun et al., 2012; Insel, Landis et al., 2013), lanzada por el presidente Obama en 2013 y replicada y emulada por proyectos científicos similares a gran escala en Europa, China, Japón, Corea, Canadá y Australia (Yuste y Bargmann, 2017), cientos de laboratorios en instituciones

académicas o industriales de todo el mundo están desarrollando métodos ópticos, eléctricos, magnéticos y moleculares para registrar, cada vez con mayor precisión, la actividad de los miles de millones de neuronas que forman nuestro cerebro (Alivisatos, Andrews et al., 2013). Esfuerzos similares, aunque a un ritmo más lento, apuntan a alterar selectivamente esa actividad.

Sin embargo, el cerebro no es un órgano más del cuerpo, sino el que construye nuestro mundo mental, nuestra mente (Crick, 1979). Esta es la esencia de un ser humano. Todas nuestras capacidades cognitivas, nuestra percepción, recuerdos, imaginación, emociones, decisiones, comportamiento, etc. son generadas por la actividad de nuestras neuronas conectadas en circuitos (Kandel, 2013). Por ello, la neurotecnología, definida como métodos o dispositivos para medir o alterar la actividad del cerebro, está revolucionando la neurociencia, brindando una visión seria de la posibilidad de una comprensión científica de la mente humana (Yuste y Church, 2014). Este será un momento histórico, el tiempo en el que los humanos finalmente se comprenderán a sí mismos desde dentro (Yuste, 2023). Y, además, la neurotecnología seguramente revolucionará la medicina, al permitir conocimientos sin precedentes sobre la fisiopatología de las enfermedades mentales y neurológicas, lo que conducirá a nuevas intervenciones terapéuticas, al alterar y corregir directamente los circuitos cerebrales anormales.

Pero precisamente porque el cerebro genera la mente humana, la neurotecnología, con su capacidad de leer y escribir esa actividad neuronal, abre la posibilidad decodificar y alterar los contenidos de nuestra cognición. Esto ya no es ciencia ficción. En laboratorios científicos como el nuestro, las neurotecnologías invasivas se pueden utilizar eficazmente en experimentos con animales para descodificar la percepción de los animales y alterar selectivamente su comportamiento (Carrillo-Reid, 2019). En seres humanos, utilizando algoritmos de inteligencia artificial generativa, ya ha sido posible la descodificación del habla interna (Metzger, Littlejohn et al., 2023) y de las imágenes que una persona conjura en su mente con neurotecnología no invasiva, como cascos de electroencefalografía o escáneres cerebrales (Huth, Lee et al., 2016). Algunos de estos dispositivos se venden libremente en todo el mundo, sin ninguna regulación, como si fueran electrónica de consumidor (Neurorights Foundation, 2023).

3. LOS NEURODERECHOS

Para abordar este desafío, académicos y formuladores de políticas en varias partes del mundo han comenzado a reflexionar sobre las implicaciones de la neurotecnología para los derechos humanos. Un grupo de 25 de nosotros, reunidos en el 2017 en el campus Morningside de la Universidad Columbia, propusimos una nueva categoría de derechos humanos, llamada "neuroderechos" (Yuste, Goering et al., 2017, para complementar los derechos humanos existentes, codificados principalmente en la Declaración Universal de Derechos Humanos de 1948, en una época en la que la neurotecnología ni siquiera era imaginada, y en los 7 tratados adicionales más importantes de derechos humanos de la ONU (Yuste, 2021 #8839; Herrmann, Yuste et al., 2022). Propuestas similares abogan por una respuesta a nivel de derechos humanos a los desafíos creados por la aplicación de la neurotecnología (Ienca y Andorno, 2017).

Los neuroderechos protegerían en cierto modo los cerebros y las mentes de todas las personas. Tres neuroderechos nos parecen particularmente importantes: el derecho a la privacidad mental, el derecho a la integridad mental y el derecho a un acceso equitativo al aumento mental (Yuste, Goering et al., 2017).

Privacidad mental: el primer neuroderechos es el derecho a la privacidad mental, y tiene como objetivo proteger a las personas contra la recopilación y el procesamiento sin consentimiento de sus datos cerebrales (Goering, Klein et al., 2021; Yuste, 2023). De hecho, si se decodifican con suficiente precisión, los datos cerebrales podrían revelar aspectos internos y altamente sensibles de la actividad mental consciente, e incluso subconsciente, de la persona, incluidos recuerdos y preferencias tácitas. Al reconocer que los datos cerebrales no son simplemente otra forma de datos personales, sino datos críticos que no está suficientemente protegido por el vago mosaico de regulaciones actuales sobre privacidad de datos, este derecho permitiría a las personas determinar por sí mismas cuándo, cómo y en qué medida otros puedan acceder a su información neuronal.

Integridad mental: este segundo neuroderecho protegería la inviolabilidad de la integridad mental, es decir, la unidad de nuestra experiencia mental, abarcando nuestra identidad, personalidad y toma de decisiones (Goering, Klein et al., 2021). Por lo tanto, protegerá el libre albedrío y la libertad cognitiva de las personas, permitiéndoles su libertad básica para tomar decisiones libres y competentes, protegidas de manipulaciones externas de nuestros cerebros. Esto es importante porque, como lo demuestran experimentos con animales y algunos

casos de estimulación cerebral profunda en humanos, la manipulación de la actividad cerebral es interpretada por el animal o la persona como su propia personalidad y voluntad, algo que no debería sorprender ya que el cerebro genera toda la personalidad. y volición. Cuando estamos siendo manipulados por las redes sociales, por ejemplo, la fuente de información manipuladora (por ejemplo, un determinado algoritmo de las redes sociales) sigue siendo externa a nosotros. Pero si nuestro propio cerebro es manipulado, la información manipuladora está dentro de nosotros y probablemente será interpretada como nuestros propios recuerdos y pensamientos. Este neuroderecho evitaría escenarios futuros en los que algunos actores (por ejemplo, el Estado, las corporaciones o los criminales) podrían alterar o manipular por la fuerza tus estados mentales. El derecho a la integridad mental otorga a las personas el derecho a ser quienes quieran y a elegir si, cuándo y cómo controlar o influir en su propia mente. Estos son principios básicos de lo que significa ser humano.

Derecho a un acceso equitativo al aumento mental: el conectar cerebros y máquinas no solo puede ayudar a las personas con problemas neurológicos, sino también mejorar a las personas sanas. Esta es una buena noticia y algunas empresas de tecnología lo están persiguiendo agresivamente. A largo plazo, la mejora cognitiva podría mejorar los procesos de aprendizaje, acelerar la innovación, generar riqueza y bienestar y ayudarnos a abordar nuestros riesgos existenciales. Sin embargo, esta mejora cognitiva puede crear una desigualdad sin precedentes y destruir la cohesión social, si no se distribuye de manera justa (Goering, Klein et al., 2021). En un mundo donde los beneficios de la neurotecnología son dominio exclusivo de unos pocos, corremos el riesgo de crear sociedades paralelas. Los que tienen y los que no tienen. Garantizar un principio de igualdad relacionado con la mejora cognitiva es fundamental para proteger y promover la justicia social.

4. NECESIDAD DE NEURODERECHOS

Algunos críticos argumentan que los neuroderechos son prematuros y que los escenarios anteriores son demasiado descabellados en el futuro (Rainey, 2023; Borbón y Borbón, 2021; Fins, 2022). Por otro lado, otros críticos argumentan que es demasiado tarde porque la industria tecnológica ya está muy involucrada en una carrera de neurotecnología y algunos dispositivos, como escáneres cerebrales portátiles y cascos EEG, ya han llegado al mercado. Los críticos también

argumentan que el derecho humano existente a la dignidad, entre otros, ya cubre todos estos escenarios, por lo que los neuroderechos no son necesarios (Bublitz, 2022). Creemos que los neuroderechos son necesarios y urgentes y que también deben definirse explícitamente para evitar interpretaciones ambiguas. Nosotros interpretamos los neuroderechos como áreas de falta que tienen que ser cubiertas con un desarrollo específico de los tratados y regulaciones existentes de derechos humanos (Goering, Klein et al., 2021). Mas que nuevos derechos humanos, pensamos que se pueden incorporar con naturalidad como opiniones especiales a algunos de los tratados internacionales, como el Convenio de Derechos Civiles y Políticos, o el Convenio en contra de la Tortura.

Debemos evitar los errores que se produjeron con otras tecnologías como las redes sociales, cuyo crecimiento desregulado ha provocado importantes disrupciones en nuestra sociedad. Este problema de gobernanza queda bien reflejado en el llamado "dilema de Collingridge", según el cual las nuevas tecnologías, cuando se desarrollan por primera vez, son fáciles de regular pero no está claro qué impacto tendrán (Jobin, Ienca et al., 2019). Al mismo tiempo, cuando estas tecnologías están muy extendidas, sus efectos son obvios, pero están arraigadas en la sociedad y son muy difíciles de regular. Podemos ver claramente lo que nos espera en términos del impacto de la neurotecnología en la sociedad, por lo que es urgente establecer pautas éticas y sociales para que pueda crecer y desplegarse en consonancia con nuestra esencia humana.

5. PASOS HACIA LA IMPLEMENTACIÓN MUNDIAL DE NEURODERECHOS

Existen actualmente ya tres casos en el mundo donde se han incorporado protección a la actividad neuronal en distintas legislaciones. Un ejemplo notable de estas pautas es la aprobación unánime en noviembre del 2022 por parte del Parlamento chileno de una enmienda al artículo 19 de la constitución vigente que protege "la actividad neuronal y la información procedente de ella", como un derecho humano básico de la ciudadanía chilena (https://neurorightsfoundation.org/chile). Esta enmienda, pionera en la historia, ha dado lugar también al primer caso de jurisprudencia en el mundo sobre neurotecnología. En agosto del 2023, en el pleito "Girardi vs. Emotiv", la Corte Suprema de Chile fallo unánimemente a favor de un ciudadano chileno que demandó a una compañía neurotecnología norteamericana por usurpación de su derecho constitucional. El fallo

obliga a la compañía a borrar todos los neurodatos obtenidos del ciudadano y a someterse a la inspección por las autoridades de regulación sanitarias.

Otro caso pionero es el estado de Río Grande del Sur, en Brasil, donde el parlamento aprobó, también por unanimidad, una enmienda a su constitución en la que se protege la actividad cerebral de los ciudadanos y se fuerza a que todas las leyes futuras estén en concordia con este mandato (https://neurorightsfoundation.org/brazil).

Por último, destaca el caso reciente del estado de Colorado, en los EE. UU., donde su Cámara de Representantes y Senado acaban de aprobar, también por unanimidad, un proyecto de ley que define a los datos neuronales y los protege en la categoría de datos personales sensibles (https://neurorightsfoundation.org/).

El gobierno de España también está haciendo balance: la Secretaria de Estado de AI hizo pública una Carta de Derechos Digitales que incorpora los Neuroderechos como parte de los derechos ciudadanos para la nueva era digital (Digitales, 2021; Yuste, Quadra-Salcedo et al., 2023). Este documento orientativo, que no tiene valor legal, puede sin embargo dar lugar a la implementación de este mandato ético en legislaciones parecidas a las de Chile, Río Grande o Colorado.

Muchas organizaciones intergubernamentales también están considerando los neuroderechos como instrumentos útiles de gobernanza. Entre otras, la OCDE ha publicado una Recomendación para la innovación responsable en neurotecnología que incluye los neuroderechos a la privacidad mental y la libertad cognitiva (OECD-Council, 2019), mientras que el Consejo de Europa ha lanzado un Plan de acción estratégico de cinco años para explorar las implicaciones de la neurotecnología para los derechos humanos (Europe, 2019).

6. CONCLUSIONES

A medida que avanzamos rápidamente por las complejidades introducidas por las tecnologías emergentes, la implementación global de los neuroderechos nos parece una necesidad. Proteger la santidad de la mente humana, garantizar el acceso equitativo a los avances tecnológicos y preservar las libertades individuales son imperativos a medida que forjamos un futuro donde la tecnología y la humanidad coexistan armoniosamente. Ahora es el momento de actuar y adoptar un enfoque proactivo para defender la dignidad y los derechos de las personas frente a capacidades tecnológicas sin precedentes. Nos dirigimos hacia

un mundo nuevo, en el que cerebros y ordenadores estarán cada vez más entrelazados y que nos redefinirá como especie y depende de nosotros elegir qué tipo de especie queramos ser.

BIBLIOGRAFÍA

Alivisatos, A. P., Andrews, A. M., Boyden, E. S., Chun, M., Church, G. M., Deisseroth, K., Donoghue, J. P., Fraser, S. E., Lippincott-Schwartz, J., Looger, L. L., Masmanidis, S., McEuen, P. L., Nurmikko, A. V., Park, H., Peterka, D. S., Reid, C., Roukes, M. L., Scherer, A., Schnitzer, M., Sejnowski, T. J., Shepard, K. L., Tsao, D., Turrigiano, G., Weiss, P. S., Xu, C., Yuste, R. y Zhuang, X. (2013). "Nanotools for neuroscience and brain activity mapping", *ACS nano 7*(3): 1850-1866.

Alivisatos, A. P., Chun, M., Church, G. M., Greenspan, R. J., Roukes, M. L. y Yuste, R. (2012). "The brain activity map project and the challenge of functional connectomics", *Neuron 74*(6): 970-974.

Borbón, D. y Borbón, L. (2021). "A Critical Perspective on NeuroRights: Comments Regarding Ethics and Law", *Frontiers in Human Neuroscience*: 1-4.

Bublitz, C. (2022). "Novel Neurorights: From Nonsense to Substance", *Neuroethics 15*.

Carrillo-Reid, L., Han, Shuting, Yang, Weijian, Akrough, A. y Yuste, R. (2019). "Controlling Visually Guided Behavior by Holographic Recalling of Cortical Ensembles", *Cell 178*(2).

Crick, F. (1979). "Thinking about the brain", *Sci. Am. 241*(3): 219-232.

Digitales, C. D. (2021). https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Europe, C. O. (2019). "Committee on Bioethics of the Council of Europe, Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025)", adopted by the Committee on Bioethics (DH-BIO) at its 16th meeting (19-21 November 2019).

Fins, J. J. (2022). "The Unintended Consequences of Chile's Neurorights Constitutional Reform: Moving beyond Negative Rights to Capabilities", *Neuroethics 15*.

Foundation, N. (2023). "Market Analysis: Neurotechnology". https://neurorightsfoundation.org/.

Goering, S., Klein, E., Sullivan, L. S., Wexler, A., Arcas, B. A. Y., Bi, G. Q., Carmena, J. M., Fins, J. J., Friesen, P., Gallant, J., Huggins, J. E., Kellmeyer, P., Marblestone, A., Mitchell, C., Parens, E., Pham, M., Rubel, A., Sadato, N., Teicher, M., Wasserman, D., Whittaker, M., Wolpaw, J. y Yuste, R. (2021). "Recommendations for Responsible Development and Application of Neurotechnologies", *Neuroethics 14*(3): 365-386.

Herrmann, S., Yuste, R. y Genser, J. (2022). "Neurorights Foundation: Gap Analysis". https://static1.squarespace.com/static/60e5c0c4c4f37276f4d458cf/t/6275130256dd5e2e11d4bd1b/1651839747023/Neurorights+Foundation+PUBLIC+Analysis+5.6.22.pdf.

Huth, A. G., Lee, T., Nishimoto, S., Bilenko, N. Y., Vu, A. T. y Gallant, J. L. (2016). "Decoding the Semantic Content of Natural Movies from Human Brain Activity", *Front Syst Neurosci 10*: 81.

Ienca, M. y Andorno, R. (2017). "Towards new human rights in the age of neuroscience and neurotechnology", *Life Sci Soc Policy 13*(1): 5.

Insel, T. R., Landis, S. C. y Collins, F. S. (2013). "The NIH BRAIN Initiative", *Science 340*(6133): 687-688.

Jobin, A., Ienca, M. y Vayena, E. (2019). "The global landscape of AI ethics guidelines", *Nature Machine Intelligence 1*(9): 389-399.

Kandel, E. R. (2013). *Principles of neural science*. New York, McGraw-Hill.

Metzger, S. L., Littlejohn, K. T., Silva, A. B., Moses, D. A., Seaton, M. P., Wang, R., Dougherty, M. E., Liu, J. R., Wu, P., Berger, M. A., Zhuravleva, I., Tu-Chan, A., Ganguly, K., Anumanchipalli, G. K. y Chang, E. F. (2023). "A high-performance neuroprosthesis for speech decoding and avatar control", *Nature 620*(7976): 1037-1046.

OECD-Council (2019). OECD Recommendation on Responsible Innovation in Neurotechnology, Organisation for Economic Co-operation and Development.

Rainey, S. "Neurorights as Hohfeldian Privileges", *Neuroethics 16*.

Yuste, R. (2023). "Advocating for neurodata privacy and neurotechnology regulation", *Nat Protoc 18*(10): 2869-2875.

Yuste, R. (2023). *Lectures in Neuroscience,* Columbia University Press.

Yuste, R. y Bargmann, C. (2017). "Toward a Global BRAIN Initiative", *Cell 168*(6): 956-959.

Yuste, R. y Church, G. M. (2014). "The new century of the brain", *Scientific American 310*(3): 38-45.

Yuste, R., Goering, S., Arcas, B. A. Y., Bi, G., Carmena, J. M., Carter, A., Fins, J. J., Friesen, P., Gallant, J., Huggins, J. E., Illes, J., Kellmeyer, P., Klein, E., Marblestone, A., Mitchell, C., Parens, E., Pham, M., Rubel, A., Sadato, N., Sullivan, L. S., Teicher, M., Wasserman, D., Wexler, A., Whittaker, M. y Wolpaw, J. (2017). "Four ethical priorities for neurotechnologies and AI", *Nature 551*(7679): 159-163.

Yuste, R., Quadra-Salcedo, T. y Fernández, M. G. (2023). "Neurorights and New Charts of Digital Rights: A dialogue", *Indiana Journal of Global Legal Studies 30*: 1.

El estudio del impacto de la digitalización sobre la vida humana, lejos de mostrar signos de agotamiento, se muestra más vivo que nunca, evolucionando hacia nuevas áreas de interés. En este ámbito de investigación se observa ya una cierta madurez, lo que está dando pie a una nueva fase de análisis caracterizada por una mayor precisión en cuanto al objeto, sujetos, actividades o impactos alcanzados y, sobre todo, por una mayor concreción en el plano propositivo.

La presente obra no solamente avanza por esta senda, sino que lo hace desde una perspectiva multidisciplinar, abarcando todas las ramas del Derecho. Su especial valor descansa precisamente en aunar bajo una misma cubierta los estudios más avanzados acerca de la relación entre las distintas tecnologías integradas en la digitalización y el Derecho, de la mano de los especialistas más destacados y desde el particular prisma de todos y cada uno de los ámbitos que integran el saber jurídico.

María Emilia Casas Baamonde es Catedrática de Derecho del Trabajo y de la Seguridad Social de la Universidad Complutense de Madrid y miembro del Consejo Ciencias Sociales de la Fundación Ramón Areces, y **Daniel Pérez del Prado** es Profesor Titular de Derecho del Trabajo y de la Seguridad Social de la Universidad Carlos III de Madrid.