

# DERECHO Y TECNOLOGÍAS

María Emilia Casas Baamonde  
(Directora)

Daniel Pérez del Prado  
(Coordinador)

frA HAND  
books



FUNDACIÓN  
RAMÓN ARECES

**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](mailto:cerasa@cerasa.es)

[www.cerasa.es](http://www.cerasa.es)

© FUNDACIÓN RAMÓN ARECES

Vitruvio, 5 – 28006 MADRID

[www.fundacionareces.es](http://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

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 3

# CÓMO ABORDAR JURÍDICAMENTE EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LOS DERECHOS FUNDAMENTALES<sup>1</sup>

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”<sup>2</sup>. Se ha afirmado la necesidad de “un nuevo paradigma

---

<sup>1</sup> 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 “Algorithmic 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).

<sup>2</sup> 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”<sup>3</sup>. 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<sup>4</sup>. No se entra ahora en lo que sería la parte especial relativa a cada derecho fundamental o sector específico,<sup>5</sup> 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<sup>6</sup>.

---

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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.

<sup>6</sup> “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<sup>7</sup>.

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

---

<sup>7</sup> 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<sup>8</sup>. 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 gobernarán a los hombres, no sería necesario ningún control, ni externo ni interno, sobre el gobierno”<sup>9</sup>. Trasladando esta afirmación al ámbito del Derecho, es indudable que este tiene un papel crucial frente a los nuevos riesgos<sup>10</sup>.

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

---

<sup>8</sup> 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>

<sup>9</sup> 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>

<sup>10</sup> “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<sup>11</sup>, en su Considerando 48<sup>12</sup> 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)<sup>13</sup>.

## 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<sup>14</sup>,

---

<sup>11</sup> 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](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.

<sup>12</sup> 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.

<sup>13</sup> 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](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680aee411)

<sup>14</sup> 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”<sup>15</sup>. 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”<sup>16</sup>. La Carta de Derechos Digitales de España, adoptada en julio de 2021<sup>17</sup>, menciona explícitamente la dignidad en su introducción y el apartado XXV.1<sup>18</sup>. La UNESCO también ha resaltado esta perspectiva<sup>19</sup>. 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<sup>20</sup> 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>

<sup>15</sup> 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.

<sup>16</sup> Hoffmann-Riem, W. (2019). *Big Data. Desafíos también para el Derecho*, Civitas, Madrid, p. 98.

<sup>17</sup> 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](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.

<sup>18</sup> 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 XXVI *dispone* que “La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad”.

<sup>19</sup> Conferencia General 41ª reunión - París, 41 C/73, 22 de noviembre de 2021. Anexo. [https://unesdoc.unesco.org/ark:/48223/pf0000379920\\_spa](https://unesdoc.unesco.org/ark:/48223/pf0000379920_spa) Entre otros, ver núm. 15, III. 1, núm. 13 y ss. y 10º.

<sup>20</sup> 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<sup>21</sup> y doctrina constitucional española<sup>22</sup>, siguiendo la alemana<sup>23</sup>. 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<sup>24</sup> 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

---

<sup>21</sup> 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.

<sup>22</sup> 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-Auriol, 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.

<sup>23</sup> 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.

<sup>24</sup> Milione, C. y Cárdenas Córdón, 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”<sup>25</sup>. 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”<sup>26</sup>. 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<sup>27</sup> e inicialmente Otto<sup>28</sup>.

### 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<sup>29</sup>. En tales casos, además, se aplican las garantías específicas

---

<sup>25</sup> 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.

<sup>26</sup> 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.

<sup>27</sup> 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.unioviado.es/constitucional/miemb/pdf/librodf.PDF>

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

<sup>29</sup> 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<sup>30</sup>.

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<sup>31</sup>. 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<sup>32</sup>, Floridi y el grupo de Tilburg<sup>33</sup> y con profundidad Castillo<sup>34</sup>, 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

---

<sup>30</sup> 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.

<sup>31</sup> 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>

<sup>32</sup> Jaume Palasí, L. “Cómo la inteligencia artificial...” *cit.* p. 28.

<sup>33</sup> 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>

<sup>34</sup> 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<sup>35</sup>, 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), infringiendo 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<sup>36</sup>. Apunta Van der Sloot que hoy día basar la protección jurídica en la naturaleza de los datos “no es la mejor manera de avanzar”<sup>37</sup>.

Y quizá la cuestión más importante: la IA genera datos de salida, datos inferidos que pueden revelar información personal de manera indirecta o detallada<sup>38</sup>. 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<sup>39</sup>. Sin embargo, el RGPD se centra más en los datos de entrada<sup>40</sup> y el TJUE no es tan claro que respecto de estos datos

---

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

<sup>36</sup> 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.

<sup>37</sup> 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.

<sup>38</sup> 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>

<sup>39</sup> Grupo del Artículo 29, *Directrices sobre decisiones... cit.* p. 10.

<sup>40</sup> Soriano Arnanz, A. *Decisiones automatizadas... cit.*

inferidos pueda ejercerse el derecho de acceso o rectificación<sup>41</sup>. 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<sup>42</sup>. A este respecto, hay que tener en cuenta la muy valiosa posición del Grupo del Artículo 29<sup>43</sup> desde hace años o la doctrina<sup>44</sup>. La reciente STJUE del 7 de diciembre de 2023 (caso SCHUFA c. Alemania) que he analizado<sup>45</sup> 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

---

<sup>41</sup> 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.

<sup>42</sup> 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”.

<sup>43</sup> En especial hay que tener en cuenta Grupo del Artículo 29, *Directrices sobre decisiones individuales...cit.*

<sup>44</sup> 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>.

<sup>45</sup> 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/V14YNLI>

sencillo ni superponer las dos normas, ni gestionar el cumplimiento conjunto de las mismas<sup>46</sup>.

#### 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*<sup>47</sup> y más notablemente con el Libro Blanco de la IA<sup>48</sup> 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*<sup>49</sup> de 2022 dentro de la *Artificial Intelligence and Data Act*, “AIDA”<sup>50</sup>. En diciembre de 2022, Brasil comenzó a tramitar el proyecto de ley núm. 2338 en el Senado para regular la IA<sup>51</sup>, mientras que el Reino Unido ha adoptado un enfoque de regulación más laxo post-Brexit<sup>52</sup>.

---

<sup>46</sup> 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.*

<sup>47</sup> Se sigue la evolución en “Ética en el diseño...” *cit.*

<sup>48</sup> *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>

<sup>49</sup> <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>

<sup>50</sup> 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>

<sup>51</sup> *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](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>

<sup>52</sup> 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<sup>53</sup>. Canadá anunció en septiembre de 2023 el “Código de Conducta Voluntario para el Desarrollo y Gestión Responsable de Sistemas Generativos Avanzados de IA”<sup>54</sup>. 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<sup>55</sup>. 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<sup>56</sup>. Con carácter más parcial, el 3 de enero de 2024 California ha regulado su *Artificial Intelligence Accountability Act*<sup>57</sup> o Illinois cuenta con su *Artificial Intelligence Video Interview Act* (820 ILCS 42/)<sup>58</sup>. En Iberoamérica existen múltiples propuestas legislativas<sup>59</sup>.

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<sup>60</sup>. Su elaboración comenzó con el Comité Ad hoc sobre IA

---

<sup>53</sup> [http://www.cac.gov.cn/2023-07/13/c\\_1690898327029107.htm](http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm)

<sup>54</sup> 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>

<sup>55</sup> <https://www.mofa.go.jp/files/100573473.pdf>

<sup>56</sup> *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/>

<sup>57</sup> California Senate Bill 896, <https://legiscan.com/CA/text/SB896/id/2868456>

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

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

<sup>60</sup> 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)<sup>61</sup> 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<sup>62</sup>, con unos “Términos de Referencia del CAI”<sup>63</sup> para crear un “instrumento jurídico vinculante de carácter transversal”<sup>64</sup> 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<sup>65</sup>. Hubo un “Borrador Cero” de 6 de enero 2023<sup>66</sup>, un Borrador consolidado de 7 de julio de 2023<sup>67</sup>, un Proyecto base de 18 de diciembre de 2023<sup>68</sup> 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<sup>69</sup>.

---

*Ciudadanía*, 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.

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

<sup>62</sup> <https://www.coe.int/en/web/artificial-intelligence/cai>

<sup>63</sup> 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>

<sup>64</sup> 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/>

<sup>65</sup> Parte II y III. 11. CAHAI, *Possible elements... cit.*

<sup>66</sup> 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>

<sup>67</sup> 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>

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

<sup>69</sup> [https://search.coe.int/cm/pages/result\\_details.aspx?objectid=0900001680aee411](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<sup>70</sup>. 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,

---

<sup>70</sup> 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<sup>71</sup>. A través de más de treinta declaraciones internacionales y corporativas analizadas en Harvard<sup>72</sup>, 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

---

<sup>71</sup> 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”).*

<sup>72</sup> 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)<sup>73</sup> 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

---

<sup>73</sup> 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<sup>74</sup>. Van cristalizando o se van afirmando nuevos “derechos digitales”<sup>75</sup>. 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<sup>76</sup> o la Carta Iberoamericana de Principios y Derechos en Entornos Digitales, de 25 de marzo de 2023<sup>77</sup>.

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

---

<sup>74</sup> 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.

<sup>75</sup> 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, CEPCC, Madrid, pp. 2347-2361. Acceso en [www.cotino.es](http://www.cotino.es)

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

<sup>77</sup> Aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. [https://www.segib.org/wp-content/uploads/Carta\\_iberamericana\\_derechos\\_digitales\\_ESP\\_web.pdf](https://www.segib.org/wp-content/uploads/Carta_iberamericana_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](https://www.fundacioncarolina.es/wp-content/uploads/2023/03/DERECHOS-DIGITALES_FC-2.pdf)

<sup>78</sup> 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<sup>79</sup>, 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<sup>80</sup>, 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”.

---

<sup>79</sup> 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.

<sup>80</sup> 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<sup>81</sup>, 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.<sup>82</sup> 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

---

<sup>81</sup> 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*).

<sup>82</sup> 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<sup>83</sup>.

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

---

<sup>83</sup> 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”<sup>84</sup> 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)<sup>85</sup>. Este recurso debe permitir que una autoridad independiente, no necesariamente judicial, examine el fondo de la petición y, si procede, otorgue la reparación adecuada<sup>86</sup>. 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”<sup>87</sup>. 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<sup>88</sup>. 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

---

<sup>84</sup> Así, cabe seguir el ya referido estudio de Harvard, Fjeld y otros: “Principled Artificial Intelligence... cit.

<sup>85</sup> 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>

<sup>86</sup> La sentencia TEDH, de 3 de abril de 2001, Keenan contra Reino Unido, párr. 122 resume el contenido de este precepto.

<sup>87</sup> En la versión de 18 de diciembre se señala la letra c) como posibilidad (en color rojo).

<sup>88</sup> 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<sup>89</sup>, 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<sup>90</sup>. 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<sup>91</sup>, 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

---

<sup>89</sup> 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.*

<sup>90</sup> Ver “Nuevo paradigma en las garantías ...cit. Sobre el tema recientemente, Castillo Parrilla, J. A.: “Privacidad de grupo...cit.

<sup>91</sup> 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”<sup>92</sup>. Como afirma Jaume “El daño social, al igual que el daño medioambiental, son problemas existentes que no se dejan evaluar desde un enfoque individual”<sup>93</sup>. Con este enfoque destacan especialmente los análisis de gran calado en esta dirección de Hoffmann-Riem<sup>94</sup> y especialmente Mantelero<sup>95</sup>, de Tullio<sup>96</sup> 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”<sup>97</sup>, 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”<sup>98</sup>, inspirado en parte por Mantelero<sup>99</sup>. La Recomendación

---

<sup>92</sup> 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.

<sup>93</sup> 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.

<sup>94</sup> Hoffmann-Riem, W.: *Big Data...cit.*

<sup>95</sup> 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>

<sup>96</sup> De Tullio, M. F. (2016). “La privacy e i big data verso una dimensione costituzionale collettiva”, *Politica del diritto*, Vol. 47, núm. 4, pp. 637-696.

<sup>97</sup> 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](http://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2)

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

<sup>99</sup> 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<sup>100</sup>. 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<sup>101</sup>. Asimismo, se están reforzando las garantías y regulaciones para acciones colectivas efectivas del consumidor<sup>102</sup>, 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<sup>103</sup>.

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)<sup>104</sup>. 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.

---

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

<sup>101</sup> 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.

<sup>102</sup> 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).

<sup>103</sup> 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, I asunto C 701/20.

<sup>104</sup> 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<sup>105</sup>. 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

---

<sup>105</sup> *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<sup>106</sup>. España ha sido el primer país de la UE en establecer una Autoridad Española de Supervisión de la IA, AESIA<sup>107</sup>.

Cabe plantearse la necesidad de independencia de estas autoridades de IA, especialmente cuando 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.

---

<sup>106</sup> 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.

<sup>107</sup> 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”<sup>108</sup>. 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. 23.1°).

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<sup>109</sup>. El RGPD establece una regulación muy exhaustiva<sup>110</sup>, 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,

---

<sup>108</sup> “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”.

<sup>109</sup> Artículo 8 Carta de derechos fundamentales UE, “3. El respeto de estas normas estará sujeto al control de una autoridad independiente”.

<sup>110</sup> 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<sup>111</sup>. 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”<sup>112</sup>.

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

---

<sup>111</sup> 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>

<sup>112</sup> 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”<sup>113</sup>. 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<sup>114</sup>, y extendiéndose para incluir la discriminación algorítmica pública. Este modelo se generaliza en la UE en diversos ámbitos digitales<sup>115</sup>

---

<sup>113</sup> 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, Cizur, 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, Cizur, 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.

<sup>114</sup> 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.

<sup>115</sup> 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)<sup>116</sup>. 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<sup>117</sup>, 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](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)

<sup>116</sup> “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”.

<sup>117</sup> 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<sup>118</sup> 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<sup>119</sup> y españolas<sup>120</sup> 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”<sup>121</sup>, que fundamenta las políticas y normativas de IA en la UE<sup>122</sup>. Además, el alto grupo de expertos de la UE adoptó un modelo

---

<sup>118</sup> 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>

<sup>119</sup> 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>

<sup>120</sup> 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/](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.lodpencastellon.com/wp-content/uploads/2018/02/Gu%C3%ADa-Evaluaci%C3%B3n-de-impacto-protecci%C3%B3n-de-datos.pdf>

<sup>121</sup> HLEG, *op.cit.*, en versión 2018, pp. 19, 21, 29.

<sup>122</sup> Un análisis exhaustivo en mi estudio “Ética en el diseño... *cit.*”

de ética en el diseño con su exhaustiva lista de evaluación<sup>123</sup>, su modelo ALTAI de evaluación o FUTURE-AI para salud<sup>124</sup>. 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<sup>125</sup> y Simón en España<sup>126</sup> 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

---

<sup>123</sup> HLEG, *Directrices éticas para una IA fiable, 2019, en especial Capítulo III y listado*, pp. 33-41.

<sup>124</sup> Portal ALTAI <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal>

<sup>125</sup> 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>

<sup>126</sup> Simón Castellano, Pere (2023). *La evaluación de impacto algorítmico en los derechos fundamentales*, Aranzadi, Cizur. 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)<sup>127</sup>. 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<sup>128</sup>, 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).

---

<sup>127</sup> 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.*

<sup>128</sup> 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.LI 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<sup>129</sup> relacionadas con los derechos fundamentales previas al RIA<sup>130</sup>, 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<sup>131</sup>.

---

<sup>129</sup> Por ejemplo, HRESIA o EISDH (evaluación de impacto social, ético y de los Derechos Humanos), la PIA (*Privacy Impact Assessment*) o DPIA (*Data Privacy Impact Assessment*), la SIA (*Social Impact Assessment*) y la *EtIA Ethical Impact Assessment*).

<sup>130</sup> Como recuerda Chaveli, existen ciertas metodologías como el *Algorithmic Impact Assessment 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.

<sup>131</sup> En particular, Álvarez García, V. J. y Tahiri 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<sup>132</sup>.

---

<sup>132</sup> 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.lpdencastellon.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/](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). “Comments 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](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](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](http://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 Ciudadanía*, 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/V14YNLI>

- (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 costituzionale 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](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 (DPLA) 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, Cizur, 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.
- Quintía Pastrana, A. (2019). “Reforma del derecho y revolución digital. Las garantías sociales en la economía de plataformas”, en Puentes Cociña, B. y Quintía 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* n° 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.*