Nuevo paradigma en la garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial

Lorenzo Cotino Hueso, Catedrático de Derecho Constitucional, Universitat de Valencia, OdiseIA[1]

Versión previa a las pruebas de imprenta de
Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas, Aranzadi, Cizur Menor, 2022, España, pp. 69-105, ISBN: 978-84-1124-501-2

[1] El presente estudio es resultado de investigación del proyecto "Derecho, Cambio Climático y Big Data", Grupo de Investigación en Derecho Público y TIC como investigador de la Universidad Católica de Colombia. De igual modo, en el marco del proyecto MICINN Retos "Derechos y garantías frente a las decisiones automatizadas... (RTI2018-097172-B-C21); también "La regulación de la transformación digital …" grupo de investigación de excelencia Generalitat Valenciana "Algoritmic law" (Prometeo/2021/009, 2021-24) y estancia (AEST/2021/012).

Las tecnologías disruptivas, la IA y el uso intensivo de big data llevan a una *tormenta* de explotación e intercambio de datos frente a la que -hasta ahora- prácticamente sólo queda el *refugio* del RGPD[2]. Como señaló la Comisión Europea, la IA y el IOT implican una «enorme vulnerabilidad» respecto de la seguridad y protección de la privacidad.[3] Y de hecho supone una «nueva oleada de datos» (de 33 zetabytes en 2018 a una previsión de 175 zetabytes en 2025)[4]. En otros lugares me he centrado en los riesgos e impactos para derechos fundamentales[5], así como en el régimen general aplicable[6] a la IA. En el presente estudio me propongo fundamentar y profundizar en los nuevos enfoques jurídicos y dogmáticos en el tratamiento del derecho de protección de datos personales en particular y de los derechos fundamentales en general para dar respuesta a los impactos que genera la IA y las tecnologías disruptivas. Se trata de elementos que hace años adelanté en general para la IA y el big data[7] y en particular para el ámbito de protección de datos[8].

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 hable de la necesidad de una «Constitución del algoritmo» para «constitucionalizar el algoritmo y digitalizar la constitución»[9]. Se ha afirmado la necesidad de «un nuevo paradigma en la protección de los derechos fundamentales […] una reorientación a consecuencia de la naturaleza de las tecnologías de las que hablamos»[10]. En este trabajo intento apuntar o *apuntalar* los mimbres o estos elementos básicos para este nuevo paradigma o reorientación. Ciertamente dejo sin abordar cuestiones esenciales, como pueda ser adentrarse en los tipos de instrumentos regulatorios apropiados, así como el sistema instituciones y autoridades que van a intervenir en la gobernanza de la IA y sobre todo, para dotar de garantías efectivas de cumplimiento normativo.

---

[2] NI LOIDEAIN, N., "A Port in the Data-Sharing Storm: The GDPR and the Internet of Things", *King's College London Law School Research Paper* No. 2018-27, 2018.

[3] EUROPEAN COMMISSION, *Cybersecurity in the European Digital Single Markert*, *Report* 2017 (n 4), p. 76. https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf

[4] COMISIÓN EUROPEA, *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza*, COM(2020) 65 final, Bruselas, 19.2.2020, p. 5 https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

[5] "Riesgos e impactos del big data, la inteligencia artificial y la robótica y enfoques, modelos y principios de la respuesta del Derecho", BOIX PALOP, A. y COTINO HUESO, L. (coords.), *Monográfico Derecho Público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data RGDA Iustel*, nº 50, febrero 2019, https://bit.ly/37RifyJ

[6] "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, 2019, pp. 917-952, http://links.uv.es/BmO8AU7

[7] "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata. Revista Internacional de Éticas Aplicadas*, n º24, 2017., pp. 131-150. https://goo.gl/iERVha

[8] Encuesta sobre la Protección de Datos Personales, en *Teoría y Realidad Constitucional*, nº 46, 2020, Acceso a mi contribución específica en https://t.co/uZCKMjH4j2?amp=1 acceso a toda la encuesta en http://revistas.uned.es/index.php/TRC/article/view/29105

[9] BALAGUER CALLEJÓN, F., "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, 2021.

[10] SARRIÓN ESTEVE J., "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, 2020 (Retos en el siglo XXI / coord. por Romboli S.), pp. 321-334, p. 328.

1. La dignidad y los derechos: punto de partida jurídico y dogmático, no retórico

Ya desde la ética, ya desde el ámbito jurídico que es el que aquí interesa, para abordar los retos que deparan las tecnologías disruptivas el punto de partida no es otro que la dignidad y el libre desarrollo de la personalidad y, en consecuencia, de los derechos fundamentales que de ellos derivan. Obviamente hay otros enfoques jurídicos implicados como la propiedad (en su caso industrial o intelectual) y protección de los algoritmos y los datos (como secretos, por ejemplo) y su explotación, la responsabilidad por el uso de la IA o todo lo vinculado con el Derecho de la competencia. No obstante, incluso estos regímenes jurídicos han de quedar irradiados e inspirados por la dignidad y los derechos.

Afirmaciones generales no faltan. Como indicó el Parlamento de la Unión Europea en 2017 respecto de la robótica, la UE no puede renunciar a sus «valores humanistas intrínsecamente europeos y universales que caracterizan la contribución de Europa a la sociedad propios valores humanistas y principios basados en la dignidad y los derechos fundamentales»[11] La Comisión Europea apuesta por «garantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión y en consonancia con la Carta de los Derechos Fundamentales de la UE»[12].

Desde el inicio de la atención a estas cuestiones, especial acierto tuvo el Supervisor Europeo de Protección de datos[13] cuando afirmó que hay que situar a «La dignidad en el centro de una nueva ética digital», «un mayor respeto de la dignidad humana y una mayor salvaguardia de la misma podrían servir de contrapeso a la vigilancia generalizada y la asimetría de poder a la que se enfrentan las personas». En este sentido en 2020 el Parlamento Europeo ha subrayado la necesidad de una visión «antropocéntrica» y «antropogénica», que la dignidad sea el impulso de las obligaciones jurídicas y los principios éticos para el desarrollo, el despliegue y el uso de la IA, la robótica y las tecnologías conexas[14]. De hecho, el artículo 7 de la propuesta de reglamento de IA del Parlamento UE se titula «IA antropocéntrica y antropogénica»[15].

---

[11] 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 (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

[12] COMISIÓN EUROPEA. *IA para Europa. Comunicación de la Comisión al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.* COM(2018) 237 final{SWD(2018) 137 final} Bruselas, 25.4.2018. 4; pp. 14 y ss.

[13] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, SEPD, *Dictamen 4/2015. Hacia una nueva ética digital. Datos, dignidad y tecnología*, 11 de septiembre de 2015, pp. 14 y ss.

[14] 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))*, nº 2, y considerando 12. Su anexo incluye una propuesta de Reglamento regulatorio. Cabe recordar que el Parlamento Europeo no tiene competencias de propuestas regulatorias, que corresponden a la Comisión.

[15] Ello se traduce en que las tecnologías de alto riesgo "se desarrollarán, desplegarán y utilizarán de forma que se garantice en todo momento una supervisión humana integral." (art. 7.1º) y que "se pueda restablecer en todo momento el control humano cuando sea necesario, incluso mediante la alteración o la desactivación de dichas tecnologías." (art. 7.2º).

La más reciente Recomendación sobre la ética de la IA UNESCO[16] es sin duda un hito mundial en la materia aunque no cuente con valor normativo. La recomendación afirma al respecto que «las personas nunca deberían ser cosificadas, su dignidad no debería ser menoscabada de ninguna otra manera, y sus derechos humanos y libertades fundamentales nunca deberían ser objeto de violación o abusos» (nº 15). En la misma línea, afirma a la dignidad humana entre los «valores y principios» (III. 1 nº 13 y ss.), «valor» que debería ser respetado «por todos los actores durante el ciclo de vida de los sistemas de IA» y promovido «mediante modificaciones de las leyes, los reglamentos y las directrices empresariales» (10º).

Más allá de proclamaciones en ocasiones algo retóricas de las que están plagadas todas las declaraciones éticas de IA[17], desde el punto de vista jurídico y dogmático, hay que subrayar la importancia de la dignidad y los derechos fundamentales para guiar y abordar los retos que se plantean. Como recientemente recuerdan Milione y Cárdenas especialmente para el ámbito europeo, del concepto de dignidad han ido germinando nuevos derechos y nuevas situaciones jurídico-subjetivas merecedoras de protección y tutela. Asimismo, jurisprudencialmente supone una cláusula abierta que dota de margen de apreciación a los altos tribunales para extender el umbral de protección de derechos en el marco del CEDH, la UE o en la arena nacional si es el caso. Considero que el impacto de la IA y las tecnologías disruptivas exige la actualización de facultades que integran el contenido de diversos derechos, así como garantías y acciones efectivas para proteger los derechos. Si ello no fuera suficiente, y sólo en su caso, sería preciso el reconocimiento de nuevos derechos.[18] Y en todos los casos cabe apoyarse en la proyección jurídica de la dignidad y la dimensión objetiva de los derechos.

A mismo tiempo, la jurisprudencia europea emplea la categoría de la dignidad para indicar jurídicamente los límites, las barreras infranqueables que no se deben sobrepasar si no quieren contribuir a la autodestrucción del ser humano. De igual modo en el ámbito de la UE, de la dignidad se derivan los valores inspiradores y las tradiciones constitucionales de los países miembros, como criterio interpretativo y como verdadero derecho fundamental.[19] Todo ello, tiene especial incidencia y utilidad

---

[16] Conferencia General 41ª reunión - París, 41 C/73, 22 de noviembre de 2021. Anexo. https://unesdoc.unesco.org/ark:/48223/pf0000379920_spa

[17] La bibliografía es muy abundante, por no decir que excesiva, una destilación de los principios éticos de la IA y un mapeo global y en la UE puede seguirse en mi trabajo "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* nº 58 (junio 2019). http://dx.doi.org/10.2436/rcdp.i58.2019.3303 Y 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, No. 2020-1, https://cyber.harvard.edu/publication/2020/principled-ai

[18] 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 p. 99 y ss. Asimismo, Masferrer, A., "Derechos de nueva generación", en Enríquez, J. M. , *Derechos humanos: un análisis multidisciplinar de su teoría y praxis*, 2017, págs. 331-358.

[19] MILIONE, C. y CÁRDENAS CORDÓN, A., "Dignidad humana y derechos fundamentales", *Derechos y libertades*, nº 42, 2020, pp. 233-265, en especial pp. 262-263. DOI: 10.14679/1159. Sobre la dignidad cabe remitir, entre otros, a CHUECA RODRÍGUEZ, R. L., (dir.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015 y GÓMEZ SÁNCHEZ, Y., "Dignidad y Ordenamiento jurídico", *Revista de Derecho Constitucional Europeo* (*ReDCE*) 4 (julio-diciembre 2005), pp. 219-254.

para el tratamiento jurídico de la IA al tiempo de la dimensión objetiva de los derechos.

De un lado, en sentido positivo, la dignidad como elemento estructural debe orientar las soluciones jurídicas y normativas que se adopten respecto de la IA y el big data. También en sentido positivo, el uso de la IA y las tecnologías disruptivas ha de orientarse al logro efectivo de la dignidad y los derechos de las personas. Igualmente, de la dignidad pueden derivarse los valores y principios tanto jurídicos como éticos relativos a la IA. Del otro lado, desde el punto de vista negativo, hay que dotar de garantías ante los riesgos e impactos en la dignidad y los derechos por la IA y el big data. Y como se ha adelantado, la dignidad es el límite jurídico claro frente a los peligros estructurales de los derechos o de la propia humanidad. Asimismo, de la dignidad pueden derivarse en su caso nuevos derechos fundamentales o nuevos contenidos y garantías de los ya existentes.

2. La dimensión objetiva de los derechos como catalizador jurídico constitucional para el tratamiento de la IA

Conjunta y paralelamente con la proyección jurídico constitucional de la dignidad de la persona, resulta útil –al menos en los países donde se maneja esta categoría- subrayar la dimensión objetiva de los derechos fundamentales. La misma deriva asimismo del reconocimiento constitucional de la dignidad humana. La doble dimensión subjetiva y objetiva de los derechos es una categoría de largo predicamento en la jurisprudencia alemana. Siguiendo las 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. La dimensión objetiva obliga a mirar la realidad efectiva de los derechos fundamentales. También se traduce en la creación de instituciones o institutos específicos de protección del derechos fundamentales. La dimensión objetiva de los derechos fue adoptada por la jurisprudencia[20] y doctrina[21] constitucional españolas, siguiendo a la alemana.

La dimensión objetiva de los derechos es también el recurso jurídico y dogmático especialmente útil ante las necesidades que se derivan en razón del impacto

[20] 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.

[21] No se trata de una materia excesivamente trabajada con rigor. Además de los trabajos que luego se mencionan de de Otto o en la obra que coordina Bastida, me permito destacar especialmente los análisis de SALVADOR MARTÍNEZ, M., "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, 2001, pp. 199-219; ALGUACIL GONZÁLEZ-AURIOLES, J., "Objeto y contenido de los Derechos Fundamentales: presupuestos e implicaciones de una nueva diferenciación dogmática", en *Teoría y realidad constitucional*, nº 18, 2006, pp. 305-320, en particular pp. 314 y ss. y de GAVARA DE CARA, J. C., "La vinculación positiva de los poderes públicos a los derechos fundamentales", *Teoría y realidad constitucional*, nº 20, 2007, pp. 277-320.

de la IA. Así, la dimensión objetiva se traduce en la proyección de los derechos como valores (y de ahí una clara conexión con la ética de la IA).

Los riesgos y amenazas que supone la IA para los derechos fundamentales son respecto las personas individualmente consideradas, pero como se expondrá, afectan a grandes colectivos, incluso pueden alcanzar al conjunto de la ciudadanía y de la humanidad y al género humano. Esta variabilidad de sujetos genera dificultades jurídicas desde la estructura y fórmulas de garantía clásica de los derechos que están muy ceñidas al individuo. Algunas de estas dificultades pueden abordarse mejor desde la dignidad humana y la necesidad de preservarla a nivel individual, colectivo o sectorial, de la ciudadanía o global. Asimismo a partir de la dignidad se facilita tener en cuenta los derechos de las próximas generaciones.

Asímismo, los derechos fundamentales como principios objetivos pasan a ser elementos inspiradores del ordenamiento jurídico, ya para el legislador (cuando regule la IA), ya en la interpretación del Derecho aplicable a la IA por autoridades sectoriales (como AEPD u otras) o los jueces. Y este papel inspirador resulta especialmente importante además teniendo en cuenta las lagunas regulatorias en la materia. De igual modo y como se verá, la irradiación del régimen de protección de datos al ámbito de la IA, big data, datos no personales, etc. es de especial importancia.

Igualmente, acudir a la dimensión objetiva facilita dar forma jurídica a la obligación de hacer efectivos los derechos especialmente entre los sujetos privados. Ello es algo especialmente importante en razón del peso esencial que en la materia tienen las grandes plataformas y desarrolladores privados. La dimensión objetiva se traduce en obligaciones de eficacia de los derechos fundamentales en las relaciones entre particulares. Las obligaciones de los derechos para el sector privado deben articularse a través de la regulación o bien como mandatos de interpretación de las normas entre particulares. Ello tiene especial importancia, como luego se insiste, dado el peso específico de las grandes tecnológicas en la materia.

Asimismo, a partir de la dimensión objetiva de los derechos también se legitima jurídicamente la creación, articulación y dotación de instituciones o institutos específicos de protección de derechos fundamentales, como por ejemplo las autoridades de protección de datos o las autoridades de IA de las que habla la propuesta de Reglamento de IA de la UE de 2021 y la reciente Agencia Española de Supervisión de la IA en España.

También de la dimensión objetiva de los derechos derivan obligaciones de actuación por los poderes públicos para hacer efectivos los derechos. Permite fundamentar la necesidad de trascender de la mera eficacia, eficiencia y búsqueda de intereses particulares en el uso y desarrollo de la IA. Y ello para fundamentar la necesidad de la llamada IA para el bien común, la búsqueda de intereses mundiales, nacionales, generales, así como el derecho de las personas a participar de los beneficios del progreso científico y tecnológico (art. 27. 1º DUDH), una dimensión beneficiosa especialmente subrayada desde el punto de vista constitucional por Barrilao[22]. Las obligaciones generales que dimanan de la dimensión objetiva incluso pueden acabar adoptando forma de derechos; también obligaciones de prestación y

[22] Desde una perspectiva jurídica, sobre los beneficios de la tecnología como objeto de protección jurídica puede seguirse a lao en sus diversos trabajos, afirmando la cláusula de progreso tecnológico como derecho humano. SÁNCHEZ BARRILAO, J. F., "Los fundamentos del «progreso informático» en la Unión Europea" *Revista de derecho político*, Nº 98, 2017, pp. 335-368. En especial 342 y ss. DOI: 10.5944/rdp.98.2017.18658 y "El Derecho constitucional … cit. pp. 243 y ss.

subvención (como puede articularse toda la actual financiación del avance de la IA con garantías, alfabetización y formación, IA inclusiva, etc.).

También estas categorías de dignidad y la dimensión objetiva de los derechos pueden servir para facilitar, fundamentar, adecuar y agregar nuevos contenidos de los derechos preexistentes así como en su caso, para fundamentar el reconocimiento de nuevos derechos fundamentales, si es que se considera preciso.

Hoffmann-Riem también acude a la dimensión objetiva del derecho, en este caso de protección de datos personales, para extender el modelo de extraterritorialidad en la aplicación del RGPD «este principio no debería limitarse a un derecho de protección de datos, si no extenderse también a otros riesgos ligados a la digitalización que afectan a los bienes jurídicos, incluyendo el menoscabo de bienes jurídicos colectivos» [23]. En este punto cabe señalar que la propuesta de Reglamento de IA de la UE de 2021 sigue en general este esquema extraterritorial.

Esta dimensión objetiva del derecho viene a quedar como añadido al derecho fundamental subjetivo en sí, elemento externo al contenido del derecho subjetivo que si bien impone obligaciones a los poderes públicos, tales obligaciones no se articulan como facultades exigibles del derecho subjetivo[24]. Si en general el derecho subjetivo cabe concebirlo como regla, esta dimensión objetiva puede considerarse como norma de principio por su más que relativo grado de exigibilidad jurídica. En cualquier caso, la dimensión objetiva puede ser una palanca de impulso jurídico, normativo y jurisprudencial frente a los retos que se plantean. La dimensión objetiva impulsa necesariamente una «política de derechos fundamentales», definida en sus líneas generales por el legislador en la regulación del ejercicio de los mismos, como señala Aláez[25] e inicialmente de Otto[26] (1988, 163 y ss.). En esta dirección Sánchez Barrilao para el ámbito de la IA apunta a la necesidad de un nuevo enfoque «potenciando la dimensión político-normativa del Derecho constitucional, frente a la meramente judicial y conflictual que hoy tiende a prevalecer». Se trata precisamente de un nuevo paradigma jurídico por el que aquí se apuesta, que puede canalizarse a mi juicio acudiendo a esta dimensión objetiva.[27]

3. Dignidad y dimensión objetiva de los derechos para la protección entre particulares, las «big tech» y la reorientación del Derecho de la competencia

El Parlamento de la UE en su propuesta de octubre de 2020 «Destaca la asimetría entre quienes emplean tecnologías de IA y quienes interactúan con ellas y se encuentran sujetos a éstas» (nº 3). No pueden desconocerse las graves asimetrías, la

[23] HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, Civitas, Madrid, 2019, p. 98.

[24] BASTIDA, F. J. y otros, *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2004. Sobre la dimensión objetiva en particular me remito al Capítulo 2, pp. 50-56 (M. A. Presno); Capítulo 5 (I. Villaverde), pp. 112-115 y Capítulo 8 (B. Aláez Corral), pp. 182 y ss.). La referencia lo es a la p. 43. versión disponible en internet. https://www.unioviedo.es/constitucional/miemb/pdf/librodf.PDF

[25] *Ibídem*, 182 y ss.

[26] MARTÍN RETORTILLO, L. y de OTTO Y PARDO, I., *Derechos fundamentales y Constitución*, Civitas, Madrid, 1988, pp. 163 y ss.

[27] SÁNCHEZ BARRILAO, J. F., "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, Nº. 2, 2016, pp. 225-258. p. 256.

hegemonía y el protagonismo esencial que tienen los sujetos privados respecto de la IA. En especial -aunque no sólo- las grandes plataformas y empresas tecnológicas y de telecomunicaciones. Esta situación deja a la ciudadanía por lo general desprotegida e incluso limita mucho las capacidades de actuación de los poderes públicos. A decir de Balaguer «las grandes compañías tecnológicas que convierten en letra muerta gran parte de las previsiones constitucionales relativas a los derechos fundamentales de la persona.»[28] A su juicio se está produciendo una «cosificación» de los derechos, que se integran dentro de ecosistemas creados por las compañías tecnológicas. Los derechos fundamentales a su juicio ya no expresan la dignidad de la persona sino la inserción del individuo como una pieza más dentro de un contexto económico. Ello provoca para Balaguer que los derechos a proteger son cada vez más los de los consumidores y usuarios frente a las grandes compañías. Apunta así el proceso por el cual hay una hipertrofia del Derecho de los consumidores pero que persigue la continuidad de los nuevos procesos económicos.[29]. Y ciertamente en este estudio se pretende lo contrario, que la «Constitución del algoritmo» se reformule para lograr los objetivos de la Constitución analógica. Y cabe advertir que precisamente el camino apuntado sí que requiere limitar y mucho una visión subjetivista de los derechos que interfieren en el logro de aquellos objetivos. Asimismo, se apuesta por técnicas que ya se dan en la protección de consumidores como cierto paternalismo de ignorar la voluntad del consumidor o la apuesta por vías protección de intereses difusos. Esta «Constitución del algoritmo» quedaría lejos del camino señalado por Balaguer de cosificación y protección de los intereses de los nuevos agentes tecnológicos, sino precisamente lo contrario.

Pues bien, acudir a la dignidad y la dimensión objetiva de los derechos fundamentales puede servir como palanca legitimadora para actuar en el sector privado para cumplir con el deber de protección de individuos y colectivos en las políticas, acciones institucionales y regulación. En esta dirección Hoffmann-Riem[30] subraya la necesidad de proteger espacios de libertad colectivos, proteger a los titulares teniendo en cuenta las asimetrías del poder. Es por ello que señala las insuficiencias de los derechos individuales por lo que cabe acudir al principio del Estado social y Democrático de derecho. Y también señala la necesidad de acudir a la eficacia horizontal desde los derechos particulares frente a empresas como en el caso de las comunicaciones[31] y para ello acude también a la dimensión objetiva de los derechos fundamentales y ello lo conecta con los mandatos de Derecho objetivo.[32]

Quintiá también ha mostrado particular atención a esta perspectiva, como punto de partida afirma que las grandes plataformas se sitúan ya en la infraestructura y cementos de la sociedad y nuestras vidas: *bajo los adoquines* está el monopolio, esto es, en palabras de Srnicek: «lejos de ser simples propietarios de información, estas

[28] BALAGUER CALLEJÓN, F., "Crisis sanitaria y Derecho Constitucional en el contexto global", *Teoría y Realidad Constitucional*, núm. 46, 2020, pp. 121-140, p. 123. Antes, con más profundidad «Redes sociales, compañías tecnológicas y democracia», *Revista de Derecho Constitucional Europeo*, n.º 32, julio-diciembre de 2019. Sobre las limitaciones del Derecho constitucional en el ámbito tecnológico, también el ya mencionado SÁNCHEZ BARRILAO, J. F. "El Derecho constitucional *… cit*.

[29] En especial se sigue ahora BALAGUER CALLEJÓN, F., "Los derechos constitucionales en el contexto global y digital. Transformación del sujeto y conversión en objeto", en ROTHENBURG, W. C. (Org.) *Direitos fundamentais, dignidade, constituição: estudos em Homenagem a Ingo Wolfgang Sarlet*, Thoth, Londrina, 2021.

[30] HOFFMANN-RIEM, W., *Big Data… cit.* p. 92.

[31] *Ibídem*, pp. 79 y ss.

[32] *Ibídem*, p. 81.

empresas se están convirtiendo en propietarias de las infraestructuras de la sociedad. Por ello, las tendencias monopolísticas de estas plataformas deben tenerse en cuenta en cualquier análisis que se haga de sus efectos en la economía en general» [33]. A partir de lo cual considera Quintiá que «Los efectos sobre el equilibrio entre los poderes públicos y el sector privado. No se trata simplemente, de una posición dominante en el mercado, que afecte a la calidad o al precio de bienes y servicios. Se trata de una posición dominante sobre los medios que rigen nuestra vida privada y diaria.»[34] Así, «el interés general queda aparentemente desprotegido en estos mercados donde las plataformas ponen reglas» [35]. Para el ámbito de la IA proyecta a Ferraioli y ante la ineficacia de los derechos sociales en tanto que títulos subjetivos, propone una revisión del constitucionalismo. A su juicio es necesario «repensar el Derecho para una nueva garantía social», se trata de transformar esa arquitectura, hay que dotarla de nuevas capacidades.» Y para esta revisión menciona la dimensión objetiva de los derechos como posible palanca para una cambio correlativo en el Derecho a partir de los derechos, dado que el Derecho de la competencia no es suficiente frente a tal asimetría.

Como señala Hoffmann-Riem[36] el Derecho de la competencia es una herramienta muy importante frente al poder hegemónico de las grandes compañías. No obstante, la finalidad del Derecho de la competencia es garantizar la funcionalidad de los mercados económicos e impedir el abuso de una posición de dominio del mercado. En principio ni la protección de derechos, si otros objetivos de bien común como limitar poderes políticos culturales sociales, el principio democrático u otros son objetivos del derecho de la competencia. No obstante, acudir a la dignidad y dimensión objetiva de los derechos fundamentales permite vincular el Derecho de la competencia al logro de la dignidad y los derechos fundamentales, reorientando sus objetivos.

4. «Es el impacto social, estúpido». La necesidad de superar una visión subjetivista del derecho de protección de datos personales

Como se diría de la causa del éxito del presidente Clinton en 1992 «¡es la economía, estúpido¡» («*It's the economy, stupid*»). Pues permítaseme tomar aquellas palabras para expresar la idea fuerza de que por encima de una visión reduccionista centrada en el derecho subjetivo y la visión individualizada de los derechos, hay que afrontar el importante impacto social y colectivo que implica de la IA y el big data.

Siguiendo a Petit[37] se pueden distinguir los impactos discretos, sistémicos y existenciales que generan la IA. Los impactos discretos resuelven ex post de modo reactivo a través de las reglas actuales del Derecho. En buena medida harían referencia a violaciones puntuales de derechos fundamentales. Ahí, la visión tradicional de los derechos fundamentales como derechos subjetivos reactivos es suficiente. Sin

[33] QUINTIÁ PASTRANA, A. "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, 2019, pp. 105-126, p. 111. Cita p. 112.

[34] *Ibídem*, P. 116.

[35] *Ibídem*, PP. 116-117.

[36] HOFFMANN-RIEM, W., *Big Data… cit.* p. 102.

[37] PETIT, N., *Law and Regulation of Artificial Intelligence and Robots - Conceptual Framework and Normative Implications*. Working paper, 2017 pp. 26-27 https://ssrn.com/abstract=2931339 or http://dx.doi.org/10.2139/ssrn.2931339

embargo, lo más habitual con la IA y el big data es que se generen impactos sistémicos o estructurales que afectan significativamente a la sociedad. De ahí que hay un interés público ya en juego que exige la planificación, la evaluación[38] la regulación previa y la experimentación. Asimismo no hay que descuidar, aunque no exagerar, los riesgos existenciales de la IA que pueden poner en peligro la existencia misma de la humanidad.

Pues bien, el daño individual producido por el big data y la IA puede ser imperceptible para un derecho fundamental desde la perspectiva del individuo titular del derecho, pero su uso bien puede impactar masivamente a los derechos fundamentales de sectores o conjuntos de la sociedad de una manera relevante en esta dimensión colectiva. Este pequeño o micro daño, un *small or micro damage*, puede ser un macro daño o daño masivo (big damage). La relevancia del peligro o daño debe apreciarse en una perspectiva mucho más amplia que la de cada individuo. Ello, como a continuación se expone obliga a que haya que trabajar con una dimensión o enfoque supraindividual o colectivo de los derechos que no es el habitual.

Inicialmente la doctrina no subrayó esta cuestión respecto del big data, sólo en alguna medida respecto de la privacidad.[39] Con una percepción más práctica, el Parlamento UE ha subrayado la necesidad de garantizar efectivamente e incluso judicialmente a través de diversos derechos fundamentales el uso del big data, siempre que repercuta de manera relevante en las personas (Consideración 5º)[40].

Pronto percibió en cierto modo el problema el Supervisor Europeo cuando –respecto de la privacidad y la protección de datos señala 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.»[41] Siguiendo este ejemplo del Supervisor, se puede concluir que al final del camino, *miguita a miguita*, el derecho a la protección de datos queda como una *corteza* vacía. Concluye el Supervisor que la ««inteligencia colectiva» socava la elección individual y la igualdad de las oportunidades.

Este fenómeno se aprecia especialmente con la protección de datos. Los datos que se manejan muchas veces no son datos estructurados ni vinculables a personas concretas; muchos de los tratamientos se realizan sobre datos anonimizados o seudonimizados. Formalmente, no queda afectado ni el derecho de protección de datos ni posiblemente otros derechos individualmente, a nivel *micro*, por decirlo de algún modo; pero materialmente las decisiones públicas y privadas que se adoptan sí que impactan -a nivel *macro*- en la sociedad en general, en grandes colectivos y en su protección de datos y otros derechos fundamentales y en bienes constitucionales esenciales para el Estado social y democrático de Derecho. Sin embargo, estos impactos no están siendo guarnecidos por un derecho bajo la reduccionista perspectiva de derecho subjetivo que captura toda la atención. Destacan especialmente los análisis

[38] *Ibídem*, p. 28.

[39] DE TULLIO, M. F. "La privacy e i big data verso una dimensione costitizionale collettiva", *Politica del diritto*, Vol. 47, Nº. 4, 2016, pp. 637-696.

[40] PARLAMENTO EUROPEO. *Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)). 2017 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES

[41] SEPD, *Dictamen 4/2015… cit.* p. 15.

de gran calado en esta dirección de Hoffmann-Riem[42] y especialmente Mantelero[43], con apoyo de Vedder, Rodotà, Peña Gangadharan, Crawford, Faleiros, Luers, Meier, Perlich y Thorp. El uso de los datos afecta al derecho de protección de datos personales va más allá de la dimensión individual y adquiere una dimensión colectiva.

Hoffmann-Riem recuerda que además de los derechos en juego, hay que proteger de bienes jurídicos colectivos como la protección general de las libertades, la operatividad de la democracia, el ordenamiento plural de las comunicaciones, la protección frente a la manipulación de la información, impedir asimetrías de poder, evitar la fragmentación social y efectos intimidatorios que puede generar la vigilancia. Para el autor «el derecho de protección de datos tal como se ha desarrollado para el derecho de protección individual no es capaz de lograrlo»[44], el derecho de protección de datos queda sobrepasado. Se afirma que el derecho individual y subjetivo de protección de datos es insuficiente frente al poder efectivo que implica el enorme poder real que confiere el manejo masivo de datos. «En la medida en que el manejo de datos permite el desarrollo del poder político social de un modo que resulta problemático bajo aspectos del Estado social democrático de derecho, es importante que se establezcan mecanismos eficaces para contrarrestarlo jurídicamente.» [45] El derecho de protección de datos no está orientado al tratamiento de datos no personales ni a las intervenciones que pudieran producirse, y menos aún específicamente a la protección de bienes comunes colectivos o a la protección frente a un abuso de poder. «El nuevo reglamento europeo […] ya no es suficiente» la digitalización desencadena consecuencias sociales que sobrepasan incluso el ámbito del individuo interesado. Es necesario ampliar la visión, tanto con un propósito de política social, jurídico».[46]

La protección de datos se basa en el modelo del derecho subjetivo, mientras que la dimensión colectiva emergente de protección con respecto al tratamiento en el contexto del big data no se limita necesariamente a hechos o datos que se relacionan directamente con una persona específica, sino que también incluye grupos de individuos no reconducibles a la tradicional noción sociológica de grupo. Así pues, cabe entender que lo que está en juego no es sólo la simple y en ocasiones irrisoria o no identificable afectación a derechos e intereses individuales[47]. Ni tan siquiera la suma de los cientos, miles o millones de mínimas afectaciones, sino intereses públicos en razón de bases colectivas. Está en juego es, en palabras del autor, la «decisión misma de transformar la sociedad en una representación mediatizada por modelos matemáticos, así como la identificación de los valores introducidos en tales modelos para tomar decisiones por parte de quien crea los algoritmos». [48]

---

[42] HOFFMANN-RIEM, W., *Big Data…cit.*

[43] 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. «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, n.º 2, (2016), pp. 238-255, 2016 DOI:10.1016/j.clsr.2016.01.014 y MANTELERO, A., «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, 2017. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

[44] *Ibídem*, cita de la p. 47, cabe seguir pp. 75 y ss y 119 y ss. 75 y ss y 119 y ss.

[45] *Ibídem*, p. 121.

[46] *Ibídem*, p. 139.

[47] MANTELERO, A. *El big data… cit.* p. 24.

[48] *Ibídem*, p. 24.

A decir de Jaume, «El individualismo metodológico inherente de las normas y leyes occidentales y los algoritmos y la IA no entienden al individuo; y las democracias, desde su perspectiva dogmática jurídica, no entienden a los colectivos. Las culturas occidentales en sus culturas o jurídicas son individualistas en la metodología y antropocéntricas en su ontología». «Centrarse en los derechos individuales dentro de ese contexto sociotécnico es irónicamente detrimental para los derechos individuales porque deja el Marco social fuera de la evaluación». «El daño social, al igual que el daño medioambiental, son problemas existentes que no se dejan evaluar desde un enfoque individual». [49]. También tienen propósitos sociales, no obstante sus correspondientes instrumentos normativos están menos desarrollados. La aplicación de la IA requiere un pensamiento social y una clara definición de cómo equilibrar lo social con las libertades e intereses.

Como una de las consecuencias, procede recalibrar los análisis relativos a los derechos fundamentales. Al momento de valorar la relevancia jurídica y constitucional del riesgo, daño, afectación o restricción del, los análisis jurídicos, test y ponderaciones para cada caso concreto hay que valorar no sólo el caso concreto que se analiza, sino los miles o millones de afectaciones masivas que se dan o se pueden dar de permanecer actuando el algoritmo, el sistema de IA o el tratamiento de datos masivos de que se trate.

Por ejemplo, para el caso de la garantía del debido proceso ante la aplicación automatizada de la ley por poderes públicos, y del alcance y profundidad de la revisión judicial de cada situación concreta, Citron señala que el balance debe ser «recalibrado»[50]. No se tratará de analizar el coste que supone introducir garantías para un caso individual y aislado de aplicación, sino que habrá de medirse también el peligro y potencialidad que supone un error o sesgo masivo así como el beneficio significativo de evitar errores en innumerables casos futuros. No se tratará de una decisión pública en concreto a controlar, sino de miles o millones de decisiones. Además, debe tenerse en cuenta que si el error no se controla, analiza y en su caso se corrige, las decisiones erróneas pasarán a ser big data que alimentará a los futuros algoritmos haciendo que el sesgo se multiplique.

Se trata de cuestiones que pueden tener una gran relevancia teórica, pero también práctica y procedimental y determinar la admisión y las posibilidades efectivas de actuación ante las autoridades garantes y ante los tribunales y las posibilidades de actuación ante ellas de los legitimados activos.

5. De intereses y derechos subjetivos clásicos a la tutela de intereses supraindividuales, difusos o colectivos en las últimas generaciones de derechos

Tradicionalmente el ordenamiento jurídico continental europeo a partir de los principios individualistas del Derecho romano y la doctrina privatista parten del

[49] JAUME PALASÍ, L., "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, 2020, pp. 27-39, pp. 32 y 34.

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

interés subjetivo del titular como elemento medular del derecho subjetivo[51]. Incluso desde el Derecho público, como expone Medina[52], el nuevo constitucionalismo subjetivó el Derecho administrativo y el proceso contencioso-administrativo. La norma que obliga a la administración pasó a ser, sencillamente, el derecho subjetivo de quien resulta perjudicado por su incumplimiento. El lenguaje del derecho y la protección volvió a generalizarse, dejando de ser patrimonio exclusivo de civilistas.

No hay nada completamente nuevo *bajo el sol* y la necesidad de superar un enfoque subjetivista de los derechos no es del todo nueva. Los derechos fundamentales de las llamadas primera y segunda generaciones de derechos[53] esencialmente eran derechos subjetivos. Sin embargo, ya con los importantes cambios y transformaciones tecnológicas y sociales de los siglos XX y XXI y los generalmente llamados derechos de tercera generación, se ha hecho más difícil sostener este carácter esencialmente subjetivo de los derechos como mecanismos de protección de un interés particular. Así, especialmente los derechos relacionados con el medio ambiente o la protección de consumidores han llevado a que se desarrollen –especialmente desde el Derecho anglosajón- conceptos, instrumentos y técnicas de garantía de los intereses «difusos», «supraindividuales», «colectivos», «transpersonales», de «grupo», etc.[54]. Se habla también de la protección de intereses en «serie», esto es, de los consumidores, de los contribuyentes, de los usuarios de los servicios públicos o de colectivos recientes unidos a la producción de masa de bienes y servicios que se da en la sociedad postcapitalista[55]. La tutela de la dignidad de la persona y su libre desarrollo sigue estando en el centro del que dimanan los derechos, si bien el titular se hace difuso, supraindividual. Además, como ya se ha señalado anteriormente, se tiene presente a un titular futuro con los derechos de las futuras generaciones que por principio de responsabilidad hay que proteger.

Así viene sucediendo desde el siglo XX, aunque en particular en las últimas décadas. Además de legislación y técnicas procesales, en medio ambiente o consumo se ha ido pasando de un derecho de daños a un derecho de riesgos para no tener que esperar a que se dé el daño que afectaría a la colectividad y en su caso al individuo[56]. Y como infra se analiza este enfoque de riesgos y diseño es esencial para la IA.

Entre los llamados derechos de cuarta o última generación, se hace referencia a respuestas frente a los últimos e incesantes retos que depara la sociedad postindustrial y digital[57]. En esta última generación van cristalizando o se van afirmando nuevos

---

[51] HERNÁNDEZ MARTÍNEZ, M. P., *Mecanismos de tutela de los intereses difusos y colectivos*. Instituto de Investigaciones Jurídicas, Serie G: Estudios Doctrinales, núm. 184, UNAM, México, 1997, p. 107.

[52] MEDINA ALCOZ, L. "Historia del concepto de derecho subjetivo en el Derecho administrativo español", *Revista de Derecho Público: Teoría y Método*, Vol. 1, 2021 pp. 7-52, p. 46 DOI:10.37417/RPD/vol_1_2021_531

[53] BOBBIO, N., *El tiempo de los derechos*, (trad. Rafael de Asís Roig), Sistema, Madrid, 1991, pp. 18 y ss. Sobre las generaciones de derechos y los nuevos derechos, MASFERRER, A., "Derechos de nueva generación", cit.

[54] GIDI, A. y FERRER MAC-GREGOR, E... *Procesos colectivos. La tutela de los derechos difusos, colectivos e individuales en una perspectiva comparada*, México, Porrúa, 2003, p. 203.

[55] HERNÁNDEZ MARTÍNEZ, M. P., *Mecanismos de tutela… cit.* pp. 155 y ss.

[56] ARIAS, A., "Los derechos colectivos y su relación con las acciones populares", *Derecho Constitucional. Revista Jurídica, Facultad de Derecho Universidad Católica de Guayaquil*, 1999, pp. 105-129, p. 113.

[57] BUSTAMANTE DOMAS, J., "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica". *Revista Interamericana de Ciencia, Tecnología, Sociedad e Innovación* (septiembre de 2001 /diciembre). 2001 y RIOFRÍO MARTÍNEZ-VILLALBA, J. C. , "La cuarta ola

«derechos digitales»[58]. Expresión de ello es la reciente Carta de Derechos digitales adoptada en España julio de 2021[59], sin valor normativo. No obstante, antes de caer en la tentación de apuntarse al reconocimiento de nuevos derechos, me interesa subrayar ahora que para la defensa de los derechos fundamentales ya existentes hay que tener en cuenta estos conceptos, categorías y técnicas de protección de derechos e intereses supraindividuales, colectivos o difusos. En respuesta a la IA y el big data no sólo hay que tener en cuenta al sujeto individual de los derechos clásicos que hay que proteger. Ante los riesgos existenciales puede tratarse de la garantía de la humanidad presente y de las futuras generaciones. Asimismo, un enfoque supraindividual también puede ser necesario respecto de riesgos o daños sistémicos o incluso riesgos o daños puntuales que se generan. En estos supuestos, la afectación de la dignidad o de los concretos derechos no sólo se limita al amplísimo colectivo de usuarios de nuevas tecnologías (más de la mitad de la humanidad, nueve de cada diez ciudadanos en algunos países más avanzados), de destinatarios de servicios, etc. Los derechos e intereses a proteger son tanto del conjunto, incluso de quienes no aportan sus datos o no utilizan las TIC. Todos somos potenciales sujetos de muchas decisiones y medidas adoptadas gracias a los macrodatos y la IA. Baste recordar que, como se ha sostenido infra, aplicar estas técnicas de protección para los derechos fundamentales en los nuevos contextos digitales, lejos de ser una operación para «cosificarlos» y desvirtuarlos (Balaguer), es, precisamente, el camino que se considera adecuado para hacerlos efectivos.

Señala Hernández[60] que el problema con los intereses colectivos o supraindividuales puede dividirse en dos dimensiones. De un lado, desde la tutela individual, no es sencillo reconocer al sujeto la tutela fraccionada e individualizada de fracciones del interés general. El interés del individuo es que se respete la norma objetiva o el interés público y general. Del otro lado, por cuanto a la tutela supraindividual, las dificultades se dan especialmente en residenciar en diferentes sujetos colectivos o instituciones su legitimación y la posibilidad de representar los intereses supraindividuales o en serie. Hernández[61] ya afirmaba la necesidad de reconocer en algunos casos una legitimidad para cualquier sujeto por «la emergencia de los intereses difusos por lesión a los valores constitucionales».

Así pues, sobre estas dificultades, se exigen regulaciones concretas respecto de las acciones colectivas, públicas e individuales aplicables y la legitimación requerida. También habrá que afinar las necesidades de prueba del daño o amenaza concreta al

---

de derechos humanos: los derechos digitales". *Revista Latinoamericana de Derechos Humanos* Volumen 25 (1), I Semestre 2014, pp. 15-45.

[58] Entre otros, RALLO LOMBARTE, A., "Una nueva generación de derechos digitales", *Revista de Estudios Políticos*, nº 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. *España constitucional (1978-2018). Trayectorias y perspectivas*, Vol. III. CEPC, Madrid, 2018, pp. 2347- 2361. Acceso en www.cotino.es

[59] GOBIERNO DE ESPAÑA-DE LA QUADRA, T. (coord.), *Carta de Derechos digitales*, julio de 2021. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf Próximamente, COTINO HUESO, L. (coord..), *La Carta de Derechos Digitales*, Tirant lo Blanch, Valencia, 2022.

[60] HERNÁNDEZ MARTÍNEZ, M. P., *Mecanismos de tutela… cit.* pp. 116-117.

[61] *Ibídem*, pp. 117-118.

derecho fundamental del que se trata y el nexo causal con la acción u omisión por el causante.[62]

6. Las (nuevas) acciones colectivas para la protección de datos de colectivos y el uso de IA

La extensión al ámbito de la protección de datos de las acciones colectivas parece que va a ser una realidad muy próxima. Señalaba Plaza que «sería conveniente extender a este ámbito el ejercicio de acciones colectivas.» Y ello pese a que «Puede parecer una paradoja el carácter personalísimo del derecho de la personalidad del afectado con la posibilidad de que se pueda ejercitar por otra persona o representante, pero si repercute en beneficio del protegido tampoco debiera observarse como un sistema incongruente […] tiene sentido que consideramos a estos afectados como consumidores o usuarios.»[63].

Las acciones colectivas ya se daban en el ámbito de consumo, si bien dudosamente alcanzaba la protección de datos. Así, 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[64]; 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). Respecto del alcance de estas acciones para la protección de datos, lo cierto es que la (derogada) Directiva 2009/22/CE, de 23 de abril de 2009, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores no incluía la protección de datos. Sin embargo, la nueva 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 (nº 56). Así las cosas, se podrá colectivamente impugnar la introducción o el uso continuo de un sistema de IA susceptible de vulnerar los derechos de los consumidores o subsanar, cesar y resarcir una violación de derechos. Así lo ha recordado el Parlamento Europeo en octubre 2020[65]. Esta Directiva de 2020 debe suponer un impulso de mejora regulatoria en España para hacer efectiva y práctica esta garantía colectiva de los derechos de los colectivos afectados y, en defecto de regulación, se aplicada directamente. Su proyección a los tratamientos de datos con IA en el sector privado al menos, es clara.

Esta directiva puede ser un impulso o mejora a la actual regulación del RGPD. Cabe recordar que el artículo 80 RGPD sobre «representación de los interesados»

---

[62] Al respecto, respecto de la tutela individual o colectiva en supuestos de "*afectaciobes generalizada o común para muchas personas afectadas*", Corte Constitucional colombiana, entre otras, Sentencia T-1205 de 2001 o Sentencia T-659 de 2007.

[63] PLAZA PENADÉS, J., "Aspectos legales del Big Data y la Inteligencia Artificial", PEDREÑO, A. y otros, *Big Data e Inteligencia Artificial : una visión económica y legal de estas tecnologías disruptivas*, Fundació Parc Científic Universitat de València, 2019, pp. 28-43, p. 33 https://www.researchgate.net/publication/334517305_Big_Data_e_Inteligencia_Artificial_una_vision_economica_y_legal_de_estas_tecnologias_disruptivas Sobre el tema, también GARCÍA PÉREZ, Rosa M. (2016). "La protección de datos de carácter personal del consumidor en el mercado único digital". *Revista de Derecho Mercantil*, 301 (julio- septiembre), 199-251.

[64] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

[65] PARLAMENTO EUROPEO, *Resolución de 20 de octubre de 2020… cit.* p. 35.

suponía un primer reconocimiento del papel potencial de las asociaciones y la sociedad civil[66]. En la línea del RGPD, la regulación nacional de datos expresamente permitía la representación legal o voluntaria. Así, el artículo 12.1 Ley Orgánica 3/2018, de 5 de diciembre, en virtud del cual los derechos reconocidos en los artículos 15 a 22 RGPD pueden ejercerse directamente o por medio de representante legal o voluntario. En el ámbito criminal y policial la más reciente Ley Orgánica 7/2021, de 26 de mayo en su artículo 55 también permitía la representación a entidades o asociaciones sin ánimo de lucro con objeto en la defensa de los derechos fundamentales, como el derecho de protección de datos personales. Sin embargo, la vía del artículo 80 queda algo constreñida por los requisitos exigibles pues era necesario conferir la representación y, en cualquier caso, lo cierto es que no parece que su uso sea aún relevante. La propuesta de RGPD por la Comisión de 25 de enero de 2012 era más generosa y su artículo 73. 3º reconocía a las entidades el «derecho a presentar una reclamación ante una autoridad de control» ante cualquier violación de protección de datos sin que fuera necesaria la reclamación de un interesado. Ahora bien, como se ha señalado, la línea más restrictiva del artículo 80 RGPD evita el incentivo económico a la hora de la representación y la acción[67]. Habrá que ver, pues, la evolución general de las acciones colectivas con el impulso que supone la nueva Directiva y sus efectos más concretos en el ámbito de protección de datos.

Apunta Palma[68] que aun indirectamente, podría resultar un impulso a la garantía colectiva de los derechos el futuro Reglamento de gobernanza de datos. En este punto, los futuros «Proveedores de servicios de intercambio de datos» tienen como objetivo principal mejorar las acciones individuales y el control de las personas sobre los datos que les conciernen. Ello puede ser posible especialmente desde un punto de vista práctico en la medida en la que se institucionalicen instrumentos que pueden generalizarse y están especializados en la gestión de los datos de las personas desde la perspectiva también de sus derechos e intereses. Así, respecto de estos proveedores cabe tener en cuenta que su actuación puede quedar dentro del ejercicio de los derechos del RGPD y pueden intermediar para facilitar datos (art. 9. 1 b) y art. 11. 10º) Propuesta de Reglamento relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) de 25 de noviembre[69].

---

[66] "El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro […] para que presente en su nombre la reclamación, y ejerza en su nombre los derechos" (art. 80. 1º) y deja en manos de los Estados que "pueda presentar una reclamación ante la autoridad de control […] si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento." (Art. 80. 2º). Sobre el tema, entre otros, RAMOS, PASCUAL, D. "Reflexiones sobre el artículo 80 del Reglamento Europeo de Protección de datos", *La Ley privacidad*, Nº 7, 2021 y FERNÁNDEZ-SAMANIEGO y PIÑAR GUZMÁN, J, "Las acciones colectivas en el marco del RGPD: una perspectiva desde el Derecho Civil español. *Diario La Ley*, Nº 26, Sección Ciberderecho, 11 de Febrero de 2019.

[67] En este sentido, ROIG I BATALLA, A., *Las garantías frente a las decisiones automatizadas del Reglamento general de Protección de Datos a la gobernanza algorítmica* , J.M. Bosch, Barcelona, 2021, p.128. sigo por PALMA ORTIGOSA, Adrián, *Régimen jurídico de la toma de decisiones automatizadas y el uso de sistemas de inteligencia artificial en el marco del derecho a la protección de datos personales*, Tesis doctoral Universidad de Valencia, 2021, p. 558.

[68] PALMA ORTIGOSA, A., *Régimen jurídico de la toma de decisiones … cit.,* p. 560.

[69] Así, respectivamente se recogen los "Servicios de intermediación entre los interesados que, en el ejercicio de los derechos previstos en el Reglamento (UE) 2016/679, deseen facilitar sus datos personales y los usuarios potenciales de los datos, incluida la facilitación de los medios técnicos o de otro tipo necesarios para habilitar tales servicios." Y "los proveedores que ofrezcan servicios a interesados actuarán

Para el ámbito laboral también Todolí ha apostado por la dimensión colectiva en la protección de los derechos de los trabajadores por parte de los representantes[70]. A su trabajo en esta misma obra cabe también remitir.

7. Las limitaciones de la protección de datos personales para dar respuesta a las nuevas necesidades de la IA y el big data

La IA atrae casi por defecto la aplicación del régimen de la protección de datos. Y en ocasiones, es casi el único régimen jurídico hoy día claramente aplicable. En muchos casos la IA implica la elaboración de perfiles, esto es, evaluación automatizada de personas por cuanto su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física, etc. (art. 4. 4º RGPD-UE). Asimismo, la IA supone también en muchos casos decisiones automatizadas aplicadas a personas concretas basadas en datos directos, observados o inferidos de las personas[71]. Para que sea aplicable el régimen de protección de datos debe darse la premisa de que los variados macrodatos que *alimentan* la IA sean datos de personas identificadas o identificables, o reidentificables. No se aplicará la normativa de protección de datos si se da una anonimización que garantice que los datos no vuelvan a ser personales. A este respecto hay que seguir especialmente el Dictamen 5/2014, de 10 de abril, del Grupo del Artículo 29 sobre anonimización. Y, de hecho, el régimen de protección de datos es en muchas ocasiones el único régimen jurídico aplicable al contexto de la IA, big data y tecnologías disruptivas.

Sin embargo, ello pugna con el hecho de que algunos elementos del régimen de protección de datos presenta dificultades estructurales para proyectarse a estos contextos. Por ejemplo, se da una grave dificultad para el cumplimiento de los principios básicos de la protección de datos. Así, la finalidad (art. 5.1.b RGPD) de los tratamientos de datos masivos se *desvía* hacia el descubrimiento de nuevas correlaciones, etc., cuando no para usos comerciales de los fabricantes, aplicaciones y plataformas. De igual modo, resulta muy difícil prever ulteriores usos de los datos captados pues precisamente estos procesos de uso y descubrimiento de nuevas correlaciones son los que determinarán usos posteriores y son en buena medida impredecibles. También, la limitación del plazo de conservación (art. 5.1.e RGPD) suele ser compleja dado que es natural que se encadenen unas y otras investigaciones a partir de los hallazgos de la anterior. Igualmente, el principio esencial de la minimización de datos (art. 5.1.c RGPD) va en contra del mismo concepto de big data o macrodatos que se generan por el uso de IA o IOT, así como contra la necesidad de mayores cantidades de datos para la mayor calidad de la investigación[72].

---

en el mejor interés de estos al facilitarles el ejercicio de sus derechos, en particular asesorándolos sobre los posibles usos de los datos y las condiciones generales asociadas a dichos usos".

[70] TODOLÍ SIGNES, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: big data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", *Revista de derecho social*, Nº 84, 2018, pp. 69-88.

[71] 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.

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

Además de las dificultades de los principios de la protección de datos, el presupuesto de la legitimación y consentimiento para la licitud del tratamiento de datos quedan muy modulados en el contexto de IA o IOT. Hablar de consentimiento informado y las finalidades determinadas para las que tratar los datos pasa a ser casi una entelequia frente a usos futuros que no se pueden prever. El consentimiento ha sido la columna vertebral del derecho subjetivo de protección de datos. Y la realidad es que otorgar el consentimiento ha devenido en una absoluta rutina masiva. Una sociedad infantilizada y cautivada por la tecnología *ha vendido su alma al diablo* a través de facilitar el consentimiento y de hecho lo que era una garantía ha sido totalmente contraproducente. Se llega a afirmar que «la legislación de protección de datos que resulta desactivada por el consentimiento», como sucedió con el Derecho de consumo ya hace décadas, debe caminarse hacia la imposición de normas obligatorias[73] que incluso ignoren paternalistamente la voluntad de los sujetos afectados. Como luego se apunta, considero que un enfoque basado en la evaluación del riesgos y la adopción de medidas proactivas es mucho más interesante para el ámbito de la IA y el big data. Y respecto de los múltiples derechos (acceso, rectificación, supresión, oposición, etc.) lo cierto es que su ejercicio por la ciudadanía ha sido irrisorio y en modo alguno se ha demostrado una garantía eficaz.

Como recuerda Soriano, se da la llamada «paradoja de la privacidad» [74]. Pese a que las encuestas suelen expresar preocupación y voluntad de proteger su privacidad y datos de carácter personal, las actuaciones efectivas no se corresponden, en muchos casos, con dicha voluntad. Las recompensas a corto plazo llevan a no valorar racionalmente los peligros y daños futuros. Además, nadie quiere quedar relegado de la sociedad digital y por lo general sólo queda la elección de acceder o no acceder en absoluto a los servicios a cambio de los datos. Y, por supuesto, una visión individualizada no permite apreciar el general impacto que se produce socialmente y en colectivo.

De igual modo, es muy difícil cumplir con las obligaciones de transparencia e información al interesado (art. 5.1.a y 14.5.b RGPD) frente a usos insospechados al momento de la captación del consentimiento. La transparencia sin duda sigue siendo una garantía muy importante, pues es también un mecanismo preventivo. No obstante, la facilitación de información para efectuar un tratamiento se convertido en un ritual rutinario para la ciudadanía. Mantelero subraya la falta de conocimiento y capacidad de las personas y su asimetría frente a plataformas y grandes empresas para entender la afectación de derechos, valorar riesgos o negociar el tratamiento de datos, «las partes interesadas tienen una percepción muy limitada de las implicaciones potenciales que pueden afectarlas de forma colectiva» [75]. Como luego se expone, una vía de superación de la cuestión es una aceptación de finalidades mucho más laxas pero acompañada de la referida evaluación del riesgo y medidas garantistas efectivas.

---

[73] HUERGO LORA, A. J., "Una aproximación a los algoritmos desde el derecho administrativo", en HUERGO LORA, A. J. (dir.), DÍAZ GONZÁLEZ, G. M. (coord.) *La regulación de los algoritmos*, Aranzadi Thomson Reuters, Cízur, 2020, pp. 23-87, p. 55.

[74] SORIANO ARNANZ, A., "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, nº. 56, 2021, http://laadministracionaldia.inap.es/noticia.asp?id=1511706. Remite a ATHEY, S., CATALINI, C. y TUCKER, C., "The digital privacy paradox: small money, small costs, small talk", *MIT Sloan Research Paper* No. 5196-17, 2017.

[75] MANTELERO, A. *El big data… cit.* p. 28.

El régimen jurídico de la protección de datos ha servido en Europa para colmar las enormes lagunas de regulación frente a los diferentes fenómenos tecnológicos en los últimos treinta años. Como señala Huergo, «ha sido la primera respuesta jurídica al fenómeno»[76]. Los principios de la protección de datos y la regulación han pasado ampliamente la «prueba del algodón» del paso del tiempo y con excelente nota. Muchos de los drásticos cambios tecnológicos en este tiempo se han podido reconducir jurídicamente bajo el régimen de la protección de datos. Y prueba de ello es que las autoridades de protección de datos siguen derivando de estos principios normas y muy concretas obligaciones jurídicas para la IA y el big data[77]. Las nuevas propuestas regulatorias para la IA, de hecho, siguen girando alrededor de los principios estructurales de la protección de datos y el modelo de la responsabilidad proactiva.

Ahora bien, no se pueden pedir peras al olmo ni seguir estirando la goma de la protección de datos para cubrir tantas lagunas. E incluso para seguir aplicando el régimen de protección de datos es necesario reconducir algunos de los principios y regulaciones al nuevo contexto tecnológico. Y, especialmente, el Derecho objetivo de protección de datos puede utilizarse para el ámbito de la IA y big data, pero si se distancia de algún modo del derecho subjetivo de protección de datos. No se trata de agradecer los servicios prestados y reiniciar un nuevo régimen, sino de aprovechar y potenciar los muchos elementos estructurales que se pueden derivar de este Derecho al tiempo de limitar una visión reduccionista del derecho subjetivo que, de modo contraproducente, lastra las garantías efectivas frente al desarrollo de la IA y el big data.

8. La creación dinámica de grupos algorítmicos, la privacidad colectiva y de grupo

Las vías para intentar eludir el régimen de protección de datos son muy amplias, así como hay indefiniciones de si es aplicable el régimen de protección de datos u otro régimen de protección.

Una de las novedades que implica la IA es la creación dinámica de grupos y colectivos humanos que no comparten en principio rasgos tradicionales, sino que es precisamente el algoritmo el que no cesa de configurar tales colectivos por afinidades y patrones del perfilado automatizado. Ello además sin que los interesados percibamos ni la inclusión en estos grupos ni las implicaciones que puede tener. Y lo cierto es que la aprehensión jurídica de este fenómeno y la posibilidad de proyectar como garantía el régimen de protección de datos es cuestionable, de ahí que se proclame la privacidad colectivo o la de grupo.

Recuerda con acierto Jaume[78] la naturaleza infraestructural de la IA. Los algoritmos clasifican a las personas en grupos granulares. La identidad de los individuos no es relevante, aunque se perciba como un procedimiento técnico de

[76] HUERGO LORA, A. J., "Una aproximación a los algoritmos … *cit.* p. 52.

[77] Entre otros, sobre la proyección de los elementos estructurales de la protección de datos a la IA, MARTÍNEZ MARTÍNEZ Ricard, "Inteligencia artificial, Derecho y derechos fundamentales", DE LA QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J. L. (dirs.), *Sociedad Digital y Derecho*, Boletín Oficial del Estado, Ministerio de Industria, Comercio y Turismo y Red.es, Madrid, 2018, pp. 259-278, en concreto, 275-276. También, CASTELLANOS CLARAMUNT, J., "La gestión de la información en el paradigma algorítmico: IA y protección de datos", *Métodos de Información*, 11(21), 2020, pp. 59-82.

[78] JAUME PALASÍ, L., "Cómo la inteligencia artificial… *cit.* p. 28.

individualización, técnicamente la personalización no implica individualización alguna. Además, esta granularidad implica la creación de grupos fuera de las categorías sociales convencionales de una cultura, e incluso al margen de los grupos tradicionalmente discriminados respecto de las que nuestro Derecho constitucional antidiscriminatorio refuerza sus garantías.

Floridi y el grupo de Tilburg, que abordan especialmente la «privacidad de grupo en la era de los datos»[79] exponen -y así lo recuerda también la AEPD[80]-, que la mayoría de las personas no están perfiladas individualmente, sino como miembros de un grupo específico. De hecho, es muy posible que se generen colectivos y perfiles dinámicos sin tratamiento de datos personales. Así, se pueden definir grupos por el tipo de adquisiciones, nivel adquisición, mismo contenido online, barrio o afinidad geográfica y un casi infinito etcétera. Estos grupos ad-hoc, como señala la AEPD no tienen un listado de miembros y sus integrantes no son siempre conscientes de la pertenencia a los mismos. Yendo más allá, estos grupos dinámicos pueden establecerse sin que medie acción alguna por los sujetos, sino por la agrupación de la IA según un conjunto de datos. Estos colectivos o grupos perfilados se pueden alimentar con datos agregados, es decir, datos no vinculados a personas (open data, apps, Iot, navegación, geolocalización, etc.). Asimismo estos perfiles y colectivos dinámicos pueden enriquecerse a partir del rastreo y análisis de personas especialmente seleccionadas asignados a dichos grupos, cuyos resultados se extrapolan a todo el grupo. En consecuencia, los datos empleados para generar el perfil de estos colectivos o grupos podrían no tener la consideración de datos personales y, afirma la AEPD, «no están establecidos como tal y no están sujetos a ninguna forma jurídica». El perfilado y las inferencias sobre estos grupos «carecerían de cualquier protección legal.»[81] Ciertamente no lo considero así en tanto en cuanto estas clasificaciones, aunque no supongan tratamiento de datos personales, pasan a serlo en el momento que desprenden efectos sobre personas concretas. En el momento en el que se aplican a una persona concreta se da un tratamiento por vinculación de datos e información a un sujeto. Asimismo, y como luego se sostiene, en muchos casos serán supuestos de tratamiento de datos inferidos respecto de los que sí que procede aplicar el régimen de protección de datos.

También cabe señalar el fenómeno por el que el uso de IA puede suponer que se eludan las especiales garantías respecto de los datos especialmente protegidos del artículo 9 RGPD. Así, a partir de datos *proxies* o indirectos, esto es, datos que en principio no son datos sensibles especialmente protegidos, el perfilado automatizado de big data y algoritmos pueden derivar en factores especialmente prohibidos o datos especialmente protegidos. Hay que vigilar y analizar posibles «enmascaramientos» y la elección intencional de factores que están cerca de los prohibidos o de datos afines a los especialmente protegidos[82]. Apunta Van der Sloot en esta línea que los datos no personales pueden convertirse en datos sensibles en una fracción de segundo y que el

---

[79] 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

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

[81] *Ibídem*.

[82] Entre otros, TERRY NICOLAS, "Big Data Proxies and Health Privacy Exceptionalism", en *Health Matrix nº 24*, pp. 65-108, 2014. Sobre el enmascaramiento de datos especialmente prohibidos, BAROCAS, S. y SELBST, A. D., *Big Data's Disparate Impact*, 104 *CAL. L. REV.* 671, 692-93, 2016.

procesamiento de datos no personales puede tener un impacto mayor en la vida de las personas que el procesamiento de datos personales sensibles. Es por ello que basar la protección jurídica en la naturaleza de los datos «no es la mejor manera de avanzar». [83]

Es más, recuerda Soriano el fenómeno aparentemente contrario. La prohibición del tratamiento de datos especialmente protegidos como la religión o la raza para la toma de decisiones se da el efecto contraproducente de que se hace «mucho más complicado determinar si el algoritmo infiere las categorías protegidas de otros datos». Es por ello, que al menos como mecanismo debe autorizarse que los algoritmos empleen las categorías sospechosas para poder determinar hasta qué punto dichas categorías condicionan el resultado del algoritmo. Señala la autora que «es más sencillo enseñar a los sistemas automatizados a no discriminar con base en las categorías sospechosas si dichos datos se introducen y consideran expresamente».[84]

9. Garantías del tratamiento de los datos no personales y de los datos producidos o inferidos por la IA

Como a continuación se sostiene, dado su impacto tanto en las personas concretas como en la sociedad, hay que dotar de protección a los tratamientos de datos no personales, datos agregados, datos compuestos, datos inferidos, a metadatos y datos de contenido, datos sensibles e insensibles, datos estadísticos, datos anónimos y anonimizados[85].

Ha de haber un marco básico para proteger a las personas de los tratamientos de datos no personales. Y como se expone, se puede hacer a partir de la irradiación del Derecho de protección de datos para los datos no personales, así como aplicando la protección de otros derechos fundamentales, como la vida privada.

Una vía jurídica pasa por recurrir la dimensión objetiva del derecho de protección de datos personales y su valor objetivo. Así, para Hoffmann-Riem «la garantía del derecho fundamental irradia espectacularmente sobre la protección de datos que no sean de carácter personal» [86]. De este modo, los elementos básicos de protección de este derecho pueden proyectarse para los datos no personales. Este autor ha llegado a afirmar que deben clasificarse como datos personales aquellos que no son recogidos de una persona concreta pero que pueden utilizarse para filtrar personas concretas y someterlas a determinadas medidas. Y precisamente hace referencia a ello respecto de la aplicación de efectos a personas por asignarlas a los referidos grupos generados por el análisis de big data.

De especial interés son las propuestas de Van der Sloot[87]. Apuesta por proyectar el régimen de protección de datos a los datos no personales. Así, los principios del RGPD (art. 5) pasan a ser fuente de inspiración para los datos no personales. Especialmente, supone proyectar los deberes generales de cuidado y estándares para

---

[83] 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 version SSRN.

[84] SORIANO ARNANZ, A., "Decisiones automatizadas… cit.

[85] Especialmente cabe seguir, VAN DER SLOOT, B., "Regulating non-personal data… cit. y en España recientemente a POLO ROCA, A., "Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos*". Estudios de Deusto: revista de la Universidad de Deusto*, Vol. 69, nº. 1, 2021, pp. 165-194, DOI: 10.18543/ed-69(1)-2021

[86] HOFFMANN-RIEM, W., *Big Data… cit.*, p. 90.

[87] VAN DER SLOOT, B., "Regulating non-personal data … *cit.* p. 16.

el buen gobierno de los datos. También el principio de minimización debe proyectarse a los datos no personales y exigir una finalidad específica para su procesamiento; «limitar el uso de los datos a ese propósito específico parece un requisito básico en la era de Big Data»[88]. Asimismo, dada la creciente relevancia de las decisiones que se adoptan con datos no personales, hay que garantizar que esos datos agregados sean correctos, completos y actualizados y los requisitos para garantizar la transparencia parecen vitales. También se propone «una evaluación de impacto que también tenga en cuenta intereses sociales más amplios». A ello cabe añadir las medidas de seguridad técnicas y organizativas adecuadas, incluso se aboga por la prohibición de la transferencia de datos no personales a otras jurisdicciones, salvo que se apliquen normas similares al tratamiento de datos no personales. Asimismo, se afirma la prohibición de uso de big data para eludir las reglas de protección de datos agregando datos temporalmente o eliminando un conjunto de datos de identificación.

Otras vías de solución respecto de estos tratamientos de datos por IA pasan esencialmente por no limitarse a la protección que brinda el derecho de protección de datos personales y acudir a otros derechos concurrentes, su dimensión objetiva y a la misma protección de la dignidad de la persona. Como señala Polo no se trata de proteger los datos, sino a las personas que hay detrás del dato[89].

Llevamos décadas de expansión de la protección de datos, que incluso ha fagocitado a sus «hermanos» derechos de la personalidad. Sin embargo, recuerda Hoffmann-Riem que el «derecho de protección de datos no es un derecho general sobre libertades ni de protección de autonomía personal»[90]. El impacto que puede darse por el tratamiento de datos no personales bien puede bajo quedar la protección y garantías de la vida privada y familiar. En esta línea, el Consejo de Derechos Humanos de Naciones Unidas señala que «la agregación de la información comúnmente conocida como «metadatos» puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada»[91]. Como punto de partida al respecto, cabe recordar que el derecho de protección de datos personales derivó de la protección de la vida privada y familiar (art. 8 CEDH). En el ámbito del CEDH y el TEDH la protección se ha brindado respecto de «datos relativos a la vida privada y familiar», así respecto de informaciones, comunicaciones, imágenes, filmaciones, sonidos, etc.[92] Los tratamientos de datos no relativos a una persona identificable pueden quedar bajo la protección de la vida privada. Y ello también bajo el Derecho de la UE. No hay que obviar que la Carta de los derechos fundamentales protege la vida privada y familiar y la intimidad (art. 7) y el derecho de protección de datos personales (art. 8). Para ello, siguiendo especialmente el análisis de Polo cabe tener en cuenta la línea marcada por la STJUE Digital Rights Ireland de 2014[93]. En aquel supuesto se abordaron los datos de comunicaciones electrónicas que bien podían ser datos personales o no. «Estos datos, *considerados en su conjunto*, pueden permitir extraer conclusiones muy

[88] *Ídem.*

[89] POLO ROCA, A., "Datos, datos, datos… cit. p. 234.

[90] HOFFMANN-RIEM, W., *Big Data… cit.*, p. 139.

[91] NACIONES UNIDAS, *Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital*, de 30 de junio de 2014, A/HRC/27/37, nº 19.

[92] Por ejemplo, STEDH, de 24 de junio de 2004, asunto Von Hannover c. Alemania.

[93] STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros.

precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan» (ap. 27).[94] Así, como sostiene Polo[95], datos personales y también no personales «considerados en su conjunto» merecen la protección de la vida privada. Debería profundizarse en esta línea -sólo- apuntada por el TJUE para reforzar la protección jurídica respecto de estos tratamientos de datos.

Señala este autor que surge así la noción del dato personal compuesto o teoría del perfil: un dato personal construido a partir de distintos datos no personales (de su combinación), una especie de «dato personal no personal»[96]. De igual modo sucede respecto de la anonimización (irreversible por definición), cualquier resquicio de reidentificación debe llevar a la aplicación del RGPD.

Ya existen tibias regulaciones sobre los datos no personales, especialmente por cuanto a su libre circulación (Reglamento (UE) 2018/1807). Sin embargo, como recuerda Van der Sloot el enfoque en modo alguno es el de la protección de las personas, sino que no se restrinja la disponibilidad, transferencia y tratamiento de datos no personales.[97]

Jurisprudencial y normativamente cabe esperar que se fortalezcan y aseguren garantías preventivas para el manejo del big data aun cuando no implique tratamiento de datos personales, especialmente en la línea de los principios, minimización, publicidad y transparencia de los tratamientos y evaluaciones de impacto social con incorporación de los sectores y sociedad civil implicados.

Mención a parte merecen los *datos inferidos*, a los que Palma ha prestado especial atención[98]. Hablamos de los datos, información o conocimiento sobre una persona física que no procede de la recogida o mera observación de datos que aporta el interesado, sino que se infieren u obtienen a partir de tratar sus datos, por lo general con sistemas automatizados y de IA. El tema tiene enorme relevancia. Pensemos por ejemplo en toda la información generada gracias al procesamiento de datos con sistemas de IA (por ejemplos, perfiles de personalidad efectuados por una red social, plataforma comercial, etc.). Por lo general, de estos datos no se tiene conocimiento por el interesado al tiempo que pueden fluir a terceros. Estos datos inferidos son ciertamente los que tienen valor para quienes los manejan, y no tanto lo datos personales de origen.

Pues bien, sin duda alguna para el Grupo del Artículo 29 estos datos relativos a una persona son datos personales, aunque no hayan sido facilitados el interesado[99]. Sin embargo, Soriano recuerda que el régimen de protección de datos se centra en los datos introducidos en los sistemas y no tanto en los resultados obtenidos. El RGPD no articula mecanismos de protección frente a las inferencias obtenidas del procesamiento de datos, sino que la protección se centra en la corrección y precisión

---

[94] También, STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Secretary of State for the Home Department y otros, ap. 99.

[95] Ver en general POLO ROCA, A., "Datos, datos, datos… *cit.* y en particular pp. 222 y ss.

[96] *Ibídem*, p. 28.

[97] VAN DER SLOOT, B., "Regulating non-personal data… cit., p. 16-17.

[98] Sobre el tema, PALMA ORTIGOSA, A., *Régimen jurídico de la toma de decisiones … cit.,* , pp. 185 y ss. Sobre la noción, WACHTER, S. y MITTELSTADT, B. D., "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, vol. 2019, No. 2, 2019, pp. 494-620, p. 2 versión https://ssrn.com/abstract=3248829

[99] GRUPO DEL ARTÍCULO 29, *Directrices sobre decisiones… cit.* p.10.

de los datos introducidos inicialmente en el sistema y la forma en que estos son procesados[100]. Asimismo, como recuerda Palma, para el TJUE no es tan claro que respecto de estos datos inferidos pueda ejercerse el derecho de acceso o rectificación. Sin embargo, como señala el autor, se trata de datos personales respecto de los que procede el acceso y en su caso la rectificación o supresión. Ahora bien, ello sin perjuicio de que concurran causas que modulen, delimiten o limiten estos derechos, como pueda ser por ejemplo los secretos empresariales [101]

Considero que no puede dudarse que los datos, información o conocimiento que se vinculen a una persona particular son datos personales respecto de los que procede proyectar el régimen jurídico de protección de datos. Ello es así ya sean generados con sistemas algorítmicos, bien a partir de datos de la propia persona, bien por su combinación con otros datos, e incluso cuando, como exponía, cuando los algoritmos clasifican a las personas en grupos granulares y proyecten sus efectos en sujetos particulares. Ahora bien, para ello posiblemente sea necesario una regulación o criterios interpretativos de las autoridades regulatorias o judiciales al respecto. Esto que se sostiene no aplica al derecho a la portabilidad, que tiene otra lógica e incluso diferente naturaleza, por cuanto el Grupo del Artículo 29 también claramente señala que sólo hay derecho a solicitar y recibir los datos aportados por el interesado, no a los inferidos a partir de éstos[102].

10. «Más vale prevenir que curar». El cumplimiento normativo en el diseño y los estudios de impacto: del RGPD a la IA «made in Europe»

Como es sabido, el RGPD apuesta por mecanismos proactivos y preventivos en vez de reactivos, en otras palabras, más vale prevenir que curar. Se trata la filosofía del *compliance* o cumplimiento normativo, de corte anglosajón en buena medida ajena al Derecho continental europeo. En esencia se trata de identificar posible riesgos y posibles daños en la entidad u organización para estimular todos los mecanismos preventivos y proactivos para evitar que ocurran, supone establecer controles y una supervisión y evaluación continua de los mismos para adoptar decisiones a tiempo. El sistema acaba implicando cambios en la propia organización y la gobernanza de la misma así como en la cultura y formación de sus miembros. Estas técnicas se van incorporando en ámbitos como la lucha contra la corrupción, o en ámbitos como el tributario, laboral. Y por lo que ahora interesa, este sistema preventivo es esencial el ámbito de la protección de datos y todo indica que se va a exportar de modo natural al sector de la IA y tecnologías conexas.

El RGPD ha subrayado la obligación de actuación en defensa y prevención de riesgos a través de la llamada *accountability* o deber proactivo (principio del art. 5, Considerando 78)[103]. Ello se traduce en anticiparse y no ser reactivo, que se integre

[100] SORIANO ARNANZ, A., "Decisiones automatizadas… cit.

[101] 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.

[102] GRUPO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos*. Adoptadas el 13 de diciembre de 2016. Revisadas 5 de abril de 2017, pp. 11 y 12.

[103] Sobre el tema, en general, BAJO ALBARRACÍN, J.C., "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *Compliance*", LÓPEZ CALVO,

por defecto en el sistema la privacidad si esperar a que se elija, en adoptar medidas ordenadas a garantizar el cumplimiento normativo, procesos del diseño basado en privacidad, o el desarrollo de metodologías de análisis de riesgos o *Privacy Impact Assessment*. Así, se impone la protección de datos desde el diseño y por defecto (art. 25) antes del inicio del tratamiento de datos. También se exige la diligente elección de un encargado del tratamiento (por ejemplo, proveedor de servicios de nube) para que ofrezca las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas (art. 28). De igual modo, la designación de un delegado de protección de datos figura esencial para el cumplimiento normativo (art. 36). También se articulan garantías como la necesidad de un registro interno de las actividades del tratamiento identificando el análisis del riesgo en cada tratamiento (art. 30, art. 31 Ley Orgánica 3/2018, de 5 de diciembre, o en conexión con el inventario de actividades en el sector público, art. 77.1º). Asimismo, la proactividad implica la necesidad de decidir qué medidas técnicas y organizativas son las adecuadas según los riesgos (art. 32 RGPD). De igual modo, la notificación de una violación de la seguridad a las autoridades (art. 33) y su comunicación a los interesados (art. 34). Y precisamente una de las medidas más significativas, son las evaluaciones de impacto, esto es, el análisis y descripción de todas las operaciones, su necesidad y la proporcionalidad y la evaluación de los riesgos[104]. Como luego se detalla, el uso de decisiones algorítmicas y perfilados respecto de humanos en buena medida efectuar la evaluación de impacto de protección de datos (art. 35 RGPD), otro de los instrumentos básicos de este modelo.

Pues bien, el modelo de la gestión del riesgo, la responsabilidad proactiva y el diseño para el cumplimiento normativo tiene singular relevancia en el ámbito de la IA y el big data[105]. Así se aprecia en la actividad de la AEPD respecto de la IA[106]. Considero que se trata de los elementos que se *toman prestados* del régimen de protección de datos de mayor importancia práctica y por los que hay que apostar. Cabe mencionar en este sentido el acierto de Carta de derechos digitales de 2021 cuando generaliza la importancia de este principio para todos los ámbitos: «Se 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.» (art. I. 4º).

Pues bien, es precisamente en la UE donde se apuesta una Ética confiable de la IA en el diseño y «Made in Europe», para posicionarse frente a Estados Unidos y

---

J. (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Barcelona, Bosch, 2019, pp. 973-981. MARTÍNEZ MARTÍNEZ R., "El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto", en GARCÍA MAHAMUT, R. y TOMÁS MALLÉN, B. (eds.) El *Reglamento General de Protección de Datos: un enfoque nacional y comparado*, 2019, Tirant lo Blanch, Valencia, pp. 311-342.

[104] GRUPO DEL ARTÍCULO 29, *Directrices sobre decisiones… cit.* pp. 3 y ss.

[105] Sobre la aplicación del principio de responsabilidad proactiva y el diseño para el ámbito de la IA y el big data, ALBERTO GONZÁLEZ, P., "Responsabilidad proactiva en los tratamientos masivos de datos", Dilemata, Nº. 24, 2017 (Ejemplar dedicado a: Ética de datos, sociedad y ciudadanía), pp. 115-129. NAVAS NAVARRO, Susana, "Derecho e inteligencia artificial desde el diseño. Aproximaciones", NAVAS NAVARRO, S. (coord..). *Inteligencia artificial: tecnología, derecho*, Tirant lo Blanch, Valencia, 2017, pp. 23-72 y MARTÍNEZ MARTÍNEZ, Ricard. "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista catalana de dret públic*, nº 58, 2019, pp. 64-81.

[106] 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.

especialmente China, que no conceden tal importancia a la cuestión. El mayor distintivo de esta marca Europa es el «*Ethics & Rule of law by design* X-by design»[107]. El alto grupo de expertos de la UE elaboró una lista exhaustiva de evaluación, aún de plena validez[108]. También, la Conferencia internacional de protección de datos afirma un «enfoque general de 'ética por diseño»[109]. El Libro Blanco de 2020 insiste en esta línea. Y este enfoque es la base del régimen de la propuesta de Reglamento de IA de 2021[110]: la mayor imposición de obligaciones y garantías cuanto mayor riesgo implique el tratamiento de datos o el sistema de IA. Como se expone en el propio texto, se «sigue un enfoque basado en el riesgo e impone cargas reglamentarias sólo cuando es probable que un sistema de IA plantee riesgos elevados para los derechos fundamentales y la seguridad». De este modo, a los sistemas de IA de alto riesgo se determinan «los requisitos de datos de alta calidad, documentación y trazabilidad, transparencia, supervisión humana, exactitud y solidez, son estrictamente necesarios para mitigar los riesgos para los derechos fundamentales y la seguridad que plantea la IA y que no están cubiertos por otros marcos jurídicos existentes.»

El modelo de evaluación de riesgos y aplicación de garantías compensatorias que es la médula del RGPD, se erige como el más efectivo frente a los problemas ya señalados que implican los consentimientos vacíos respecto de finalidades desconocidas al momento de recabar los datos. Destaca especialmente Mantelero[111] cuando apuesta por la evaluación de los riesgos y beneficios debería pensar siempre menos en los individuos, mediante el mecanismo de consentimiento informado, y en su lugar adoptarse un sistema transparente y general de análisis de los riesgos que fuera capaz de garantizar una gestión de datos sin causar perjuicios al individuo ni a la sociedad. En esta línea señala que hay que reemplazar el principio de finalidad por un amplio concepto de interés legítimo.

Ello permitiría a los sujetos privados dar las garantías oportunas a los riesgos de cada tratamiento a través de evaluaciones de riesgo y de impacto generalizadas. No olvidemos que la aceptación del interés legítimo como base de legitimación va directamente vinculada a un enfoque de riesgos y de garantías compensatorias (art. 6 RGPD). Y no sólo para casos particulares como actualmente. Apunta el autor «la aceptación de la idea de que los datos se recogen para propósitos múltiples y cambiantes que se pueden definir solo de manera genérica cuando empieza el tratamiento».[112] Así las cosas, y al menos para el ámbito de la IA y big data que aquí interesa, esta propuesta se traduce en una generalización del análisis de impacto

[107] Un análisis exhaustivo en mi estudio "Ética en el diseño… cit.

[108] COMISIÓN EUROPEA - GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL, *Directrices éticas para una IA fiable*, 2019, en especial Capítulo III y listado, pp. 33-41.

[109] ICDPPC (INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS), *Resolución sobre Big Data. Las amenazas del big data.* 36th International Conference, Mauritius, 2014 ap. 4º http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-Spanish-version.pdf

[110] Un primer análisis del mismo en España puede seguirse en COTINO HUESO, L. y otros, "Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)", *iario La Ley*, 2 de julio de 2021, Wolters Kluwer. https://links.uv.es/2FK3xc4

[111] MANTELERO, A. *El big data… cit.* pp. 20 y ss., p. 20 remite particularmente a 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.

[112] *Ídem*.

incluso en los usos de big data e IA que no reúnan todos estos requisitos del artículo 35. 3º RGPD. Así, «la evaluación del riesgo se convierte en el medio para definir mejor los fines específicos de cada uso de los datos y reducir los posibles efectos negativos del tratamiento» [113] y el consentimiento queda razonablemente relegado a favor de un modelo centrado en el riesgo.

La realización de estudios de impacto es el instrumento más importante del modelo de evaluación de riesgos. Ciertamente hoy puede entenderse que la explotación masiva de datos y el uso de IA exige por defecto de estudios de impacto por cuanto quedan bajo el artículo 35. 3º RGPD al tratarse de «evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas». Al respecto, la AEPD en 2019 concretó bastante los supuestos en los que procede el estudio de impacto, siempre que se dieran dos presupuestos de un listado. Y en nuestro ámbito es muy fácil que se den al menos dos de los siguientes presupuestos: 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[114].

11. El impacto social o colectivo y la participación social en la evaluación de riesgos y los estudios de impacto de la IA

La evaluación de riesgos del uso de la IA no debe ceñirse a una visión individual ceñida al impacto respecto del afectado concreto, ni sólo en el datos personales, sino respecto del impacto en bienes colectivos y en los derechos humanos se afirma en los documentos internacionales. Debe apostarse por un sistema obligatorio de evaluación de riesgos múltiples (*multiple-risks assessment*) teniendo en cuenta las repercusiones sociales y éticas del uso de estos sistemas[115]. Recientemente lo recuerda la Unesco: «debería garantizarse la aplicación de procedimientos de evaluación de riesgos y la adopción de medidas para impedir que ese daño se produzca», nº 25). Y al momento de decidir el uso de un sistema IA debe justificarse que no supone «una violación o un abuso de los derechos humanos» (Unesco nº 26 b). Se insiste en que el «aprendizaje sobre el impacto de los sistemas de IA», «el enfoque y la comprensión de los sistemas de IA deberían basarse en el impacto de estos sistemas en los derechos humanos» (Unesco nº 45). Asimismo, en estas evaluaciones de impacto hay que tener particularmente en cuenta a personas «en situación de vulnerabilidad, los derechos laborales, el medio ambiente y los ecosistemas, así como las consecuencias éticas y sociales, y facilitar la participación ciudadana» (Unesco nº 50) y ello, en todas las etapas del ciclo IA (Unesco nº 51). Se afirma el compromiso de «la elaboración de una metodología de la UNESCO de evaluación del impacto ético de las tecnologías de la IA basada en una investigación científica rigurosa y fundamentada en el derecho internacional de los derechos humanos» (Unesco nº 131).

---

[113] MANTELERO, A. *El big data… cit.* p. 22.

[114] Afirma que se han de dar al menos dos de estos supuestos. AEPD, *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

[115] MANTELERO, A., «From group privacy… cit., p.187 y ss.

En esta dirección, se indica que los sistemas de prevención, atenuación y seguimiento de riesgos deben «determinar las repercusiones en los derechos humanos y el medio ambiente, así como las consecuencias éticas y sociales» (Acción 11, nº 95). Y que los gobiernos han de establecer un marco regulador de estas evaluaciones de impacto y que tales mecanismos deben «facilitar la participación de los ciudadanos y hacer frente a los problemas de la sociedad». «Esa evaluación también debería ser multidisciplinaria, multicultural, pluralista e inclusiva y contar con múltiples interesados». En esta perspectiva de la dimensión colectiva, puede resultar también de sumo interés acudir a indicadores para afinar mucho mejor las evaluaciones y estudios de seguimiento e impacto de todas las políticas relativas a la ética de la IA (nº 104)[116]. Y todo ello con «amplia participación de las partes interesadas pertinentes» (nº 105).

Se ha adelantado la importancia de las *Directrices éticas* para una IA fiable de los expertos de la Comisión[117]. De entre las mismas, cabe destacar aquéllas de interés social y colectivo. Así, cabe cuestionarse si «¿ha llevado usted a cabo una evaluación del impacto sobre los derechos fundamentales? ¿Ha identificado y documentado los posibles equilibrios entre los diferentes principios y derechos?». Hay que tener en cuenta las cuestiones sobre el «Bienestar social y ambiental». De igual modo, el análisis de «impacto social» general «más allá del que tenga sobre el usuario (final), como, por ejemplo, las partes interesadas que pueden verse indirectamente afectadas por dicho sistema». Se hace referencia asimismo a la necesidad de «algún mecanismo para identificar los intereses y valores que implica el sistema de IA y los posibles equilibrios entre ellos» y que existan procesos para decidir sobre los equilibrios necesarios y que queden documentados. En particular, se afirma la conveniencia de evaluar el riesgo de pérdida de puestos de trabajo o de descualificación de la mano de obra y cuestionarse ¿Qué pasos se han dado para contrarrestar esos riesgos?

Ya en el marco concreto de la actual normativa de protección de datos, la evaluación de riesgos no se limita sólo al impacto que puede tener el sistema IA en el concreto derecho de protección de datos, sino en todos los derechos y libertades. A partir de esta obligación actual y existente, la AEPD insiste en el análisis de proporcionalidad y necesidad: «un análisis y gestión del riesgo para los derechos y libertades de los interesados que introduce en el tratamiento el procesamiento de los datos mediante el componente IA». Ello conlleva la obligación en evaluar y documentar que se han tenido en cuenta todas las opciones posibles para el menor impacto en todos los derechos y libertades afectados. Antes de optar por nuevos sistemas IA, valorar sistemas más probados que minimizan datos o hacen un sistema menos intensivo de explotación de datos. Si hay que abordar nuevos problemas, justificar el uso mismo de IA que pueda afectar derechos. [118] Estos análisis deben darse también en la fase de pruebas (y se insiste en la protección de los derechos en una visión amplia[119]), como desde el punto de vista de seguridad[120].

[116] Nº 104: "Deberían elaborarse instrumentos e indicadores adecuados para medir la eficacia y la eficiencia de las políticas relativas a la ética de la IA en función de las normas, prioridades y objetivos acordados, incluidos objetivos específicos para los grupos desfavorecidos y vulnerables. Ello podría comportar evaluaciones de instituciones públicas y privadas, proveedores y programas, incluidas autoevaluaciones, así como estudios de seguimiento y la elaboración de conjuntos de indicadores."

[117] COMISIÓN EUROPEA, *Directrices éticas … cit.* pp. 33-41.

[118] AEPD, *Requisitos para Auditorías … cit.*, p. 17.

[119] *Ibídem*, p.27.

[120] *Ibídem*. P. 31.

Los nuevos modelos de análisis de riesgos deben integrar a la sociedad civil, se debe identificar mejor los grupos de personas potencialmente afectadas por los riesgos. Asimismo, cabe integrar a expertos, auditores externos. El papel de las autoridades independientes de protección de datos para este enfoque es esencial. Mantelero señala[121] que las autoridades de protección de datos pueden hacer participar a los diferentes interesados que representan los intereses colectivos afectados por proyectos específicos de tratamiento de datos, en el análisis de riesgos.

Y más allá de los análisis de riesgos, en general, la IA exige nuevos modos de gobernanza, así como de regulación[122]. Y en los mismos hay que garantizar la participación social. La Recomendación de Unesco integra transversalmente por la participación de la sociedad civil y los colectivos afectados en la gobernanza de la IA, en la evaluación de riesgos y elaboración de indicadores, elaboración de políticas o la implementación de la propia recomendación. Se apuesta por «La participación de las diferentes partes interesadas a lo largo del ciclo de vida de los sistemas de IA es necesaria para garantizar enfoques inclusivos de la gobernanza de la IA, de modo que los beneficios puedan ser compartidos por todos, y para contribuir al desarrollo sostenible. […] Deberían adoptarse medidas para tener en cuenta los cambios en las tecnologías y la aparición de nuevos grupos de partes interesadas y para permitir una participación significativa de las personas, las comunidades y los grupos marginados y, si procede, en el caso de los pueblos indígenas, el respeto de su autonomía en la gestión de sus datos.» (nº 47) También de especial interés es la recomendación de que «las entidades públicas, las empresas del sector privado y las organizaciones de la sociedad civil a que incorporen a diferentes partes interesadas a su gobernanza en materia de IA y consideren la posibilidad de añadir una función de responsable independiente de la ética de la IA o algún otro mecanismo para supervisar las actividades relacionadas con la evaluación del impacto ético, las auditorías y el seguimiento continuo, así como para garantizar la orientación ética de los sistemas de IA.» (nº 58).

Será necesario detallar esta integración de mecanismos de control y defensa de intereses colectivos en los diferentes procedimientos y regulaciones públicos y privados, al momento de concretar los requisitos de gobernanza, gestión de datos, análisis de riesgos, estudios de impacto, auditorías, etc. y en el marco de la autorregulación (y la autorregulación regulada). Las posibilidades de participación de la sociedad civil son muy amplias.

12. Para concluir

En el presente estudio he sostenido diversos elementos básicos para el tratamiento jurídico desde los derechos fundamentales para dar respuesta al impacto de la IA y las tecnologías disruptivas. El marco actual, esencialmente proyección de la normativa de protección de datos, ya ha dado mucho de sí y puede seguir haciéndolo, pero es difícil seguir *abusando* de este marco jurídico sin una reconfiguración y nuevo enfoque.

---

[121] MANTELERO, A., «From group privacy… cit. p. 188.

[122] Sobre los modos de regulación, COTINO HUESO, L., "Riesgos e impactos del big data, la inteligencia… cit. pp. 11 y ss. y sobre los enfoques éticos normativos y las posibilidades de regulación internacional, ROBLES CASTILLO, M. "La gobernanza de la inteligencia artificial:: contexto y parámetros generales", *Revista electrónica de estudios internacionales (REEI)*, nº. 39, 2020, pp. 1-27, DOI: 10.17103/reei.39.07

En las muchas declaraciones sobre la ética de la IA son abundantes y por lo general vacuas las afirmaciones de la importancia de la dignidad y los derechos. Sin embargo, en el presente estudio se parte del alcance jurídico de la dignidad así como de la dimensión objetiva de los derechos fundamentales. Estas categorías jurídicas sirven para afianzar los cimientros del tratamiento jurídico básico de la IA y el big data. Así, la dignidad y la dimensión objetiva de los derechos facilitan el tratamiento internacional bajo la lengua de los derechos; la dimensión axiológica de la dignidad y los derechos permite un nexo de la ética con el Derecho de la IA; facilita la actualización de los derechos actuales ante las tecnologías disruptivas, el reconocimiento legal y especialmente jurisprudencial de nuevos contenidos y garantías de los derechos clásicos en el entorno digital; el mandato de maxificación de la eficacia de los derechos obliga a dotar de garantías efectivas a los derechos en el nuevo contexto de la IA, también en su caso a adoptar regulaciones y nuevos criterios jurisprudenciales. El alcance jurídico de la dignidad y la dimensión objetiva de los derechos facilita la superación de un enfoque individualista que es el que prima con los derechos subjetivos, siendo que la IA y el big data afectan esencialmente a la sociedad y colectivos sin que se aprecie el impacto individualmente en los supuestos más importante. También acudir a la dignidad y la dimensión objetiva de los derechos facilita conformar jurídicamente la obligación de que todas las ramas del Derecho, como el Derecho de la competencia u otros, incluyan entre sus objetivos el logro de los derechos. De igual modo, permite dotar de cobertura jurídica a los objetivos sociales del uso de la IA, IA for good, sostenibilidad, etc. Asimismo, acudir a estas categorías implica dotar de garantías frente a los riesgos que supone la IA para toda la sociedad, para grupos y colectivos y a generar y regular respuestas y mecanismos de tutela efectivos, entre otros mecanismos de acción colectiva de protección de intereses difusos o colectivos. De igual modo, el alcance jurídico de la dignidad es útil para exigir jurídicamente que la IA no ponga en riesgo a las futuras generaciones y a la humanidad. La dignidad y la dimensión objetiva de los derechos también legitiman jurídicamente la intervención pública con políticas y regulaciones dirigidas al sector privado, de tanta relevancia para la IA, así como impulsar fenómenos de autorregulación y códigos de conducta para garantizar y hacer efectivos los derechos fundamentales desde los sectores industriales, tecnológicos y profesionales del ámbito de la IA y el big data.

A lo largo del estudio, se ha insistido especialmente en la necesidad de superar una visión subjetivista del derecho de protección de datos personales, así como de otros derechos de especial proyección para la IA. Para ello se ha subrayado especialmente la importancia de apreciar el impacto de las tecnologías disruptivas en toda la humanidad, sociedad, colectivos o grupos. Y ello choca de natural con la estructura jurídica de los derechos subjetivos fundamentales, lógica y tradicionalmente centrada en las personas individuales. La aplicación del régimen de protección de datos se dificulta y se hace dudosa y vidriosa muy habitualmente en entornos de big data e IA en supuestos habituales en los que la IA genera colectivos y perfiles dinámicos sin tratamiento de datos personales, así como respecto de los tratamientos de datos anonimizados, seudonimizados, agregados, no personales, compuestos. También a los tratamientos de los datos que son producto o que se generan o infieren gracias a la IA. A este respecto se ha intentado asentar que lo importante no es tanto la naturaleza del dato, personal o no, sino las garantías para los derechos de las personas que hay detrás de los datos. Así, se hacen diversas propuestas

sobre el régimen aplicable a los tratamientos de los datos no personales, así como los datos que son inferidos por los sistemas de IA, que parecen en cierto limbo jurídico. Y la solución pasa, en buena medida, por proyectar los principios y elementos básicos del régimen de protección de datos a modo de irradiación de la dimensión objetiva de este derecho.

De igual modo, se ha analizado la dificultad que tiene la garantía y tutela de los intereses supraindividuales, difusos o colectivos en las últimas generaciones de derechos. Especialmente se ha analizado la proyección de las *class actions*, acciones colectivas para el ámbito concreto de la protección de datos de grupos y la IA. Sin duda que la Directiva (UE) 2020/1828, de 25 de noviembre de 2020 puede suponer un cambio importante en la materia en los próximos años, pudiendo pasar a ser una verdadera garantía frente a las grandes corporaciones tecnológicas. Se ha efectuado un examen de otras barreras y problemas importantes del régimen de protección de datos cuando se proyecta a la IA y el big data. Así sucede con la casi nula garantía que implica el consentimiento, que llega a desactivar o hacer casi inútiles las garantías y derechos. Lo que era la garantía esencial de un derecho fundamental se ha convertido en la vía de agua abierta que ha hecho naufragar en muy buena medida todas las garantías. Y este problema se da esencialmente respecto del desarrollo de la IA en el sector privado. Así, se ha de seguir pasando a un derecho más imperativo. También se ha reparado en dificultades estructurales para hacer efectivos algunos principios de la protección de datos cando se trata del contexto de la IA y las tecnologías disruptivas, como por ejemplo, la minimización de los macrodatos, o la práctica imposibilidad de determinar finalidades de tratamientos que están por venir.

Más allá de estos límites, desde el punto de vista de las respuestas, se ha centrado la atención en la importancia del «Más vale prevenir que curar» que rige en la nueva protección de datos: responsabilidad proactiva, análisis de riesgos, estudios de impacto, cumplimiento normativo en el diseño son las herramientas maestras del régimen jurídico de la IA (la «AI made in Europe»). Y estos elementos procedentes de la protección de datos en su paso al ámbito de la IA deben *purgarse* de una visión individualista y reduccionista del derecho subjetivo de la protección de datos, así como ampliar su espectro a otros derechos fundamentales. Finalmente, se ha centrado la atención en indicadores y elementos a tener en cuenta en análisis de riesgos, auditorías y estudios de impacto social o colectivo de la IA, así como la necesidad de integrar a la sociedad civil en estos instrumentos.

Bibliografía

AEPD:

- *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020.

- *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

- *Privacidad de grupo*, 19 de octubre de 2020, https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo

- *Requisitos para Auditorías de Tratamientos que incluyan IA*, 2021.

ALBERTO GONZÁLEZ, P., «Responsabilidad proactiva en los tratamientos masivos de datos», Dilemata, Nº. 24, 2017 (Ejemplar dedicado a: Ética de datos, sociedad y ciudadanía), pp. 115-129.

ALGUACIL GONZÁLEZ-AURIOLES, J., «Objeto y contenido de los Derechos Fundamentales: presupuestos e implicaciones de una nueva diferenciación dogmática», en *Teoría y realidad constitucional*, nº 18, 2006, pp. 305–320.

ARIAS, A., «Los derechos colectivos y su relación con las acciones populares», *Derecho Constitucional. Revista Jurídica, Facultad de Derecho Universidad Católica de Guayaquil*, 1999, pp. 105-129.

BAJO ALBARRACÍN, J.C., «Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *Compliance*», en LÓPEZ CALVO, J. (coord.). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Barcelona, Bosch, 2019, pp. 973-981.

BALAGUER CALLEJÓN, F.:

- «Redes sociales, compañías tecnológicas y democracia», *Revista de Derecho Constitucional Europeo*, n.º 32, julio-diciembre de 2019.

- «Crisis sanitaria y Derecho Constitucional en el contexto global», *Teoría y Realidad Constitucional*, núm. 46, 2020, pp. 121-140.

- «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, 2021.

- «Los derechos constitucionales en el contexto global y digital. Transformación del sujeto y conversión en objeto», en Rothenburg, W. C. (Org.) *Direitos fundamentais, dignidade, constituição: estudos em Homenagem a Ingo Wolfgang Sarlet*, Thoth, Londrina, 2021.

BAROCAS, S. y SELBST, A. D., *Big Data's Disparate Impact*, 104 *CAL. L. REV.* 671, 692-93, 2016.

BASTIDA, F. J. y otros, *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2004.

BOBBIO, N., *El tiempo de los derechos*, (trad. Rafael de Asís Roig), Sistema, Madrid, 1991.

BUSTAMANTE DOMAS, J., «Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica». *Revista Interamericana de Ciencia, Tecnología, Sociedad e Innovación* (septiembre de 2001 /diciembre).

CASTELLANOS CLARAMUNT, J., «La gestión de la información en el paradigma algorítmico: IA y protección de datos», *Métodos de Información*, 11(21), 2020, pp. 59-82.

CHUECA RODRÍGUEZ, R. L., (dir.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015.

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

COMISIÓN EUROPEA:

- GRUPO INDEPENDIENTE DE EXPERTOS DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL, *Directrices éticas para una IA fiable*, 2019.

- *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

- *IA para Europa. Comunicación de la Comisión al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones.* COM(2018) 237 final{SWD(2018) 137 final} Bruselas, 25.4.2018. 4.

COTINO HUESO, L. y otros, «Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Artificial Intelligence Act)», *iario La Ley*, 2 de julio de 2021, Wolters Kluwer. https://links.uv.es/2FK3xc4

COTINO HUESO, L.:

-»Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales», *Dilemata. Revista Internacional de Éticas Aplicadas*, n º24, 2017., pp. 131-150. https://goo.gl/iERVha

- «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* nº 58 (junio 2019). http://dx.doi.org/10.2436/rcdp.i58.2019.3303

- «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, 2019, pp. 917-952, http://links.uv.es/BmO8AU7

- «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, 2018, pp. 2347- 2361. Acceso en www.cotino.es

- «Riesgos e impactos del big data, la inteligencia artificial y la robótica y enfoques, modelos y principios de la respuesta del Derecho», BOIX PALOP, A. y COTINO HUESO, L. (coords.), *Monográfico Derecho Público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data RGDA Iustel*, nº 50, febrero 2019, https://bit.ly/37RifyJ

- Encuesta sobre la Protección de Datos Personales, en *Teoría y Realidad Constitucional*, nº 46, 2020, Acceso a mi contribución específica en https://t.co/uZCKMjH4j2?amp=1 acceso a toda la encuesta en http://revistas.uned.es/index.php/TRC/article/view/29105

DE TULLIO, M. F. «La privacy e i big data verso una dimensione costitizionale collettiva», *Politica del diritto*, Vol. 47, Nº. 4, 2016, pp. 637-696.

ESCOBAR ROCA, G., *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid, 2018, en especial p. 99 y ss.

EUROPEAN COMMISSION, *Cybersecurity in the European Digital Single Markert*, *Report* 2017 (n 4), p. 76. https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf

FERNÁNDEZ-SAMANIEGO y PIÑAR GUZMÁN,J, «Las acciones colectivas en el marco del RGPD: una perspectiva desde el Derecho Civil español. *Diario La Ley*, Nº 26, Sección Ciberderecho, 11 de Febrero de 2019.

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, No. 2020-1, https://cyber.harvard.edu/publication/2020/principled-ai

GARCÍA PÉREZ, Rosa M. «La protección de datos de carácter personal del consumidor en el mercado único digital». *Revista de Derecho Mercantil*, 301 (julio-septiembre), 2016199-251.

GAVARA DE CARA, J. C., «La vinculación positiva de los poderes públicos a los derechos fundamentales», *Teoría y realidad constitucional*, nº 20, 2007, pp. 277-320.

GIDI, A. y FERRER MAC-GREGOR, E... *Procesos colectivos. La tutela de los derechos difusos, colectivos e individuales en una perspectiva comparada*, México, Porrúa, 2003.

GOBIERNO DE ESPAÑA-DE LA QUADRA, T. (coord.), *Carta de Derechos digitales*, julio de 2021. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf Próximamente, COTINO HUESO, L. (coord..), *La Carta de Derechos Digitales*, Tirant lo Blanch, Valencia, 2022.

GÓMEZ SÁNCHEZ, Y., "Dignidad y Ordenamiento jurídico", *Revista de Derecho Constitucional Europeo* (*ReDCE*) 4 (julio-diciembre 2005), pp. 219-254.

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.

- *Directrices sobre el derecho a la portabilidad de los datos*. Adoptadas el 13 de diciembre de 2016. Revisadas 5 de abril de 2017.

HERNÁNDEZ MARTÍNEZ, M. P., *Mecanismos de tutela de los intereses difusos y colectivos*. Instituto de Investigaciones Jurídicas, Serie G: Estudios Doctrinales, núm. 184, UNAM, México, 1997.

HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, Civitas, Madrid, 2019.

HUERGO LORA, A. J., «Una aproximación a los algoritmos desde el derecho administrativo», en HUERGO LORA, A. J. (dir.), DÍAZ GONZÁLEZ, G. M. (coord.) *La regulación de los algoritmos*, Aranzadi Thomson Reuters, Cízur, 2020.

ICDPPC (INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS), *Resolución sobre Big Data. Las amenazas del big data.* 36th International Conference, Mauritius, 2014 http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-Spanish-version.pdf

JAUME PALASÍ, L., «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, 2020, pp. 27-39, pp. 32 y 34.

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, https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

MANTELERO, A.:

- «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, n.º 2, (2016), pp. 238-255, 2016 DOI:10.1016/j.clsr.2016.01.014

- *El big data en el marco del Reglamento General de Protección de Datos*, marzo, UOC, Barcelona, pp. 1-46.

- «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, 2017. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

-«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.

MARTÍN RETORTILLO, L. y de OTTO Y PARDO, I., *Derechos fundamentales y Constitución*, Civitas, Madrid, 1988, pp. 163 y ss.

MARTÍNEZ MARTÍNEZ R.:

- «El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto», en GARCÍA MAHAMUT, R. y TOMÁS MALLÉN, B. (eds.) El *Reglamento General de Protección de Datos: un enfoque nacional y comparado*, 2019, Tirant lo Blanch, Valencia, pp. 311-342.

- «Inteligencia artificial, Derecho y derechos fundamentales», DE LA QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J. L. (dirs.), *Sociedad Digital y Derecho*, Boletín Oficial del Estado, Ministerio de Industria, Comercio y Turismo y Red.es, Madrid, 2018, pp. 259-278.

- «Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo», *Revista catalana de dret públic*, nº 58, 2019, pp. 64-81.

MASFERRER, A., "DERECHOS DE NUEVA GENERACIÓN", EN ENRÍQUEZ, J. M. , *DERECHOS HUMANOS: UN ANÁLISIS MULTIDISCIPLINAR DE SU TEORÍA Y PRAXIS*, 2017, PÁGS. 331-358.

MEDINA ALCOZ, L. «Historia del concepto de derecho subjetivo en el Derecho administrativo español», *Revista de Derecho Público: Teoría y Método*, Vol. 1, 2021 pp. 7-52, p. 46 DOI:10.37417/RPD/vol_1_2021_531

MILIONE, C. y CÁRDENAS CORDÓN, A., «Dignidad humana y derechos fundamentales», *Derechos y libertades*, nº 42, 2020, pp. 233-265, en especial pp. 262-263. DOI: 10.14679/1159.

NACIONES UNIDAS, *Informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital*, de 30 de junio de 2014, A/HRC/27/37, nº 19.

NAVAS NAVARRO, S., «Derecho e inteligencia artificial desde el diseño. Aproximaciones», NAVAS NAVARRO, S. (coord..). *Inteligencia artificial: tecnología, derecho*, Tirant lo Blanch, Valencia, 2017, pp. 23-72.

NI LOIDEAIN, N., «A Port in the Data-Sharing Storm: The GDPR and the Internet of Things», *King's College London Law School Research Paper* No. 2018-27, 2018.

PALMA ORTIGOSA, Adrián, *Régimen jurídico de la toma de decisiones automatizadas y el uso de sistemas de inteligencia artificial en el marco del derecho a la protección de datos personales*, Tesis doctoral Universidad de Valencia, 2021.

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 (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)).*

- *Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)). 2017

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES

PETIT, N., *Law and Regulation of Artificial Intelligence and Robots - Conceptual Framework and Normative Implications*. Working paper, 2017 https://ssrn.com/abstract=2931339 or http://dx.doi.org/10.2139/ssrn.2931339

PLAZA PENADÉS, J., «Aspectos legales del Big Data y la Inteligencia Artificial», PEDREÑO, A. y otros, *Big Data e Inteligencia Artificial : una visión económica y legal de estas tecnologías disruptivas*, Fundació Parc Científic Universitat de València, 2019, pp. 28-43 https://www.researchgate.net/publication/334517305_Big_Data_e_Inteligencia_Artificial_una_vision_economica_y_legal_de_estas_tecnologias_disruptivas

POLO ROCA, A., «Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos». *Estudios de Deusto: revista de la Universidad de Deusto*, Vol. 69, nº. 1, 2021, pp. 165-194, DOI: 10.18543/ed-69(1)-2021.

QUINTIÁ PASTRANA, A. «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, 2019, pp. 105-126.

RALLO LOMBARTE, A., «Una nueva generación de derechos digitales», *Revista de Estudios Políticos*, nº 187, pp. 101-135. https://doi.org/10.18042/cepc/rep.187.04

RAMOS, PASCUAL, D. «Reflexiones sobre el artículo 80 del Reglamento Europeo de Protección de datos», *La Ley privacidad*, Nº 7, 2021.

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

RIOFRÍO MARTÍNEZ-VILLALBA, J. C. , «La cuarta ola de derechos humanos: los derechos digitales». *Revista Latinoamericana de Derechos Humanos* Volumen 25 (1), I Semestre 2014, pp. 15-45.

ROBLES CASTILLO, M. «La gobernanza de la inteligencia artificial:: contexto y parámetros generales», *Revista electrónica de estudios internacionales (REEI)*, nº. 39, 2020, pp. 1-27, DOI: 10.17103/reei.39.07

ROIG I BATALLA, A., *Las garantías frente a las decisiones automatizadas del Reglamento general de Protección de Datos a la gobernanza algorítmica* , J.M. Bosch, Barcelona, 2021.

SALVADOR MARTÍNEZ, M., «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, 2001, pp. 199-219

SÁNCHEZ BARRILAO, J. F.:

- «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, Nº. 2, 2016, pp. 225-258. p. 256.

«Los fundamentos del «progreso informático» en la Unión Europea» *Revista de derecho político*, Nº 98, 2017, pp. 335-368. DOI: 10.5944/rdp.98.2017.18658

SARRIÓN ESTEVE J., «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, 2020 (Retos en el siglo XXI / coord. por Romboli S.), pp. 321-334.

SORIANO ARNANZ, A., «Decisiones automatizadas y discriminación: aproximación y propuestas generales», *Revista General de Derecho Administrativo*, nº. 56, 2021, http://laadministracionaldia.inap.es/noticia.asp?id=1511706.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, SEPD, *Dictamen 4/2015. Hacia una nueva ética digital. Datos, dignidad y tecnología*, 11 de septiembre de 2015.

TERRY NICOLAS, «Big Data Proxies and Health Privacy Exceptionalism», en *Health Matrix nº 24*, pp. 65-108, 2014.

TODOLÍ SIGNES, A., «La gobernanza colectiva de la protección de datos en las relaciones laborales: big data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos», *Revista de derecho social*, Nº 84, 2018, pp. 69-88.

UNESCO, *Recomendación sobre la ética de la IA*. Conferencia General 41ª reunión - París, 41 C/73, 22 de noviembre de 2021. Anexo. https://unesdoc.unesco.org/ark:/48223/pf0000379920_spa

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., «A right to reasonable inferences: re-thinking data protection law in the age of big data and AI», *Columbia Business Law Review*, vol. 2019, No. 2, 2019, pp. 494-620, p. 2 versión https://ssrn.com/abstract=3248829