DERECHO CONSTITUCIONAL E INTELIGENCIA ARTIFICIAL

María Mercedes Serrano Pérez
Doctora en Derecho y profesora de Derecho Constitucional de la Universidad de Castilla-La Mancha

Celia Fernández Aller
Doctora en Derecho y profesora de la ETSISI (Escuela Técnica Superior de Ingeniería en Sistemas Informáticos) de la Universidad Politécnica de Madrid

1. INTRODUCCIÓN

No hay ámbito jurídico que no se vaya a ver profundamente transformado en la Cuarta Revolución industrial en la que estamos inmersos. El potencial de la inteligencia artificial (en adelante, IA) es único en la historia. Ha posibilitado asistentes personales activados por voz, redes neuronales que navegan sin descanso por el big data en busca de patrones que puedan ayudar a predecir deseos, programas de IA que están transformando la Medicina, la Economía, la Educación, la Justicia, etc. Hasta ahora esta tecnología no ha alcanzado la capacidad de la inteligencia humana, pero no se descarta el momento en que la supere, llegándose al punto de no retorno tecnológico, o *singularidad*[1].

En este sentido, la Comisión Europea[2] recuerda que IA se está desarrollando rápido. Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir. Al mismo tiempo, la IA conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos.

Se vive un momento clave en el ámbito europeo, puesto que la Comisión trabaja en las conclusiones de su Libro Blanco para formular alternativas políticas que permitan el desarrollo de la IA de forma compatible con los intereses económicos y los derechos fundamentales. Lo cierto es que los lobbies empresariales están presionando a favor de los primeros, defendiendo un enfoque auto-regulador, que contrasta con un enfoque de regulación general que permita mitigar los riesgos enormes que plantea la IA para los derechos de las personas.

La Unión Europea (en adelante, UE) está preocupada por generar confianza como requisito previo para la adopción de la IA, y ello supone una oportunidad para Europa, dada su estrecha vinculación con los valores y el Estado de Derecho y su capacidad demostrada de crear productos seguros, fiables y sofisticados en sectores que van desde la aeronáutica a la energía, pasando por la automoción y los equipos médicos.

---

[1] A las diferentes acepciones de la expresión "inteligencia artificial" y las limitaciones de lo que ahora se entiende por ella, se dedica la investigación de Smith, B. C., (2019) *The promise of artificial intelligence. Reckoning and judgment*, The MIT Press, Cambridge (Massachusets). Además, es muy descriptivo el texto de Tegmark, Max (2017) *Life 3.0. Being human in the age of Artificial Intelligence*. Vintage.

[2] COMISIÓN EUROPEA. 19.2.2020 COM(2020) 65 final *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*. Disponible en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

Un ámbito en el que se ha regulado el uso de la IA que incluya tratamiento de datos personales es el de la protección de datos. El Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD)[3] ha introducido un enfoque basado en los riesgos, en el que las autoridades de protección de datos ven su función reguladora debilitada significativamente. El enfoque basado en el riesgo debe ser implementado por los responsables (grandes empresas) a través de las evaluaciones de impacto en la protección de datos (que evocan los estudios de impacto ambiental) y la notificación de las infracciones, entre otros procedimientos. Se determinarán grupos de datos cuyo nivel de riesgo sea alto, y a esos se les aplicarán medidas más exigentes de protección. Este enfoque dista mucho de ser un enfoque de protección reforzada de la privacidad[4]. En el mismo sentido se pronuncian otros autores[5].

Para superar estas limitaciones, resulta esencial reconocer que la Etica tiene un papel clave en el momento de orientar el avance de las legislaciones. Además, urge generalizar la utilización de los estudios de impacto en la ética.

Las Directrices éticas para una AI fiable[6] pueden servir como documento base para conseguir una IA centrada en el ser humano: este enfoque se esfuerza por garantizar que los valores humanos sean siempre la principal consideración, y nos obliga a tener en cuenta que el desarrollo y el uso de la IA no debe considerarse como un medio en sí mismo, sino con el objetivo de aumentar el bienestar de los ciudadanos.

La IA confiable tiene dos componentes: 1) su desarrollo, despliegue y utilización deben cumplir con los derechos fundamentales y la reglamentación aplicable, así como respetar los principios y valores fundamentales, garantizando un "propósito ético", y 2) debe ser técnicamente robusta y fiable.

Para ello, es necesario:

Desarrollar, desplegar y utilizar los sistemas de IA respetando los principios éticos de: respeto de la autonomía humana, prevención del daño, equidad y explicabilidad. Reconocer y abordar las tensiones que pueden surgir entre estos principios.

---

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

[4] "The risk-based approach under the new EU data protection regulation: a critical perspective" *Journal of Risk Research*. VOL. 23, NO. 2, 139–152. https://doi.org/10.1080/13669877.2018.1517381.

[5] E. Harcourt, Bernard (2010). "Risk as a proxy for race". *Criminology and Public Policy*; Macenaite, Milda (2016). "The "Riskification" of European Data Protection Law through a two-fold Shift". *European Journal of Risk Regulation*, 8 (2017), pp. 506–540 © Cambridge University Press ; Niels van Dijk, Raphaël Gellert, Kjetil Rommetveit (2016). "A risk to a right? Beyond data protection risk assessments". *Computer Law and Security review.*

[6] Grupo de expertos de alto nivel sobre inteligencia artificial (Unión Europea) (2019). Directrices éticas para una Inteligencia artificial fiable (cursiva) ISBN 978-92-76-11994-4.

Prestar una atención especial a las situaciones que afecten a los grupos más vulnerables, como los niños, las personas con discapacidad y otras que se hayan visto históricamente desfavorecidas o que se encuentren en riesgo de exclusión, así como a las situaciones caracterizadas por asimetrías de poder o de información

Reconocer y tener presente que, pese a que aportan beneficios sustanciales a las personas y a la sociedad, los sistemas de IA también entrañan determinados riesgos y pueden tener efectos negativos, algunos de los cuales pueden resultar difíciles de prever, identificar o medir (por ejemplo, sobre la democracia, el Estado de Derecho y la justicia distributiva, o sobre la propia mente humana).

Garantizar que el desarrollo, despliegue y utilización de los sistemas de IA cumpla los requisitos para una IA fiable: 1) acción y supervisión humanas, 2) solidez técnica y seguridad, 3) gestión de la privacidad y de los datos, 4) transparencia[7], 5) diversidad, no discriminación y equidad, 6) bienestar ambiental y social, y 7) rendición de cuentas.

Para garantizar el cumplimiento de estos requisitos, se deberá estudiar la posibilidad de emplear tanto métodos técnicos como no técnicos.

Además, habrá que impulsar la investigación y la innovación.

Otra prioridad debe ser comunicar información a las partes interesadas, de un modo claro y proactivo, sobre las capacidades y limitaciones de los sistemas de IA, posibilitando el establecimiento de expectativas realistas, así como sobre el modo en que se cumplen los requisitos.

Se debe facilitar la trazabilidad y la auditabilidad de los sistemas de IA, especialmente en contextos o situaciones críticos.

Otra sugerencia es la adopción de una evaluación de la fiabilidad de la IA al desarrollar, desplegar o utilizar sistemas de IA, y adaptarla al caso de uso específico en el que se aplique dicho sistema.

Por otro lado, hay que tener presente que este tipo de listas de evaluación nunca pueden ser exhaustivas. Garantizar la fiabilidad de la IA no consiste en marcar casillas de verificación, sino en identificar y aplicar constantemente requisitos, evaluar soluciones y asegurar mejores resultados a lo largo de todo el ciclo de vida del sistema de IA, implicando a las partes interesadas en el proceso.

Existen muchas iniciativas de establecimiento de principios éticos de la IA, como los Principios de Asilomar (https://futureoflife.org/ai-principles/), los de IEEE (https://ethicsinaction.ieee.org/), la Unión Europea (*Ethical Framework for a Good*

[7] La Nueva Ley de Servicios digitales en tramitación en Europa va a suponer un avance en este asunto de la transparencia, puesto que obligará a las plataformas grandes a informar sobre los sistemas de recomendación algorítmica y posibilidades de elección de los usuarios para el acceso a la información.

AI Society, propuesto por el AI4People en diciembre de 2018; *Ethics Guidelines for Trustworthy AI del High-Level Expert Group on Artificial Intelligence* de la Comisión Europea de abril de 2019), WWW Consortium (que tiene también su propuesta ética) o ITU (https://aiforgood.itu.int/).

Como recuerdan algunos autores[8], es cierto que grandes empresas tecnológicas como Google han hecho esfuerzos por dotarse de códigos éticos, como el relativo a la IA. Estos esfuerzos de las empresas por pensar en los asuntos éticos y comprometerse a ciertas pautas son muy deseables. Pero el interés privado no puede marcar el rumbo de los consensos éticos, al faltarle la imparcialidad. Tal y como ha señalado recientemente Nemitz[9], debemos estar muy vigilantes con las actividades de los "temibles 5", que son quienes moldean nuestra experiencia con las tecnologías digitales, incluida la IA: Google, Facebook, Microsoft, Apple y Amazon. Estas corporaciones son extremadamente ricas, lo que les garantiza acceso desproporcionado a legisladores y gobiernos. Además, financian todo tipo de actividades, incluidas la ciencia y la investigación. Estas empresas están presentes en todos los campos, tanto político, como de la sociedad civil, ciencia, periodismo, negocios, lo que les permite ganarse la simpatía en torno a los asuntos que les preocupan. Cualquier análisis crítico debe comenzar por la comprensión de esta acumulación de poder tecnológico, económico y político en las manos de las referidas empresas, que lideran el desarrollo tecnológico de la IA y su transformación en servicios de interés comercial[10].

Las formulaciones éticas de las empresas suelen ser muy amplias y se produce en ocasiones una selección del código ético por parte de las mismas que se adapta a sus necesidades sin un proceso de consultas y acuerdo entre las partes interesadas. En otras palabras, habrían de evitarse los peligros de los que alerta Floridi[11]:

a) *Ethics shopping*, que supone que una organización elija, entre las muchas iniciativas que hay de códigos éticos muy dispersos, el que mejor se adapte a su forma de hacer, justificando así sus intenciones, poco coherentes con la ética en ocasiones.

b) *Ethics dumping,* que consiste en la conducta de exportar prácticas no éticas a países donde hay más laxitud o diferencia de criterios.

c) *Ethics lobbying,* o la práctica de algunos actores privados de usar autorregulación en temas como la ética de la Inteligencia Artificial para hacer lobb-

---

[8] Fernández-Aller (2020) "Salud digital, salud global y ética. Una mirada desde el enfoque de derechos humanos". *Revista Diecisiete*.

[9] Nemitz (2018) "Constitutional democracy and technology in the age of artificial intelligence". *Philosophical Transactions R. Soc. A* 376: 20180089. http://dx.doi.org/10.1098/rsta.2018.0089.

[10] Ibid., p. 2.

[11] Floridi, Luciano (2019). "Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical". *Philosophy and Technology*.

ying en contra de la introducción de normas con fuerza jurídica, sometidas estas últimas a mecanismos más exigentes en caso de incumplimiento.

d) *Bluewashing,* como concepto proveniente de la ética de la Ecología *-greenwashing-*, que es la mala práctica de una organización pública o privada que busca aparecer socialmente como más verde, sostenible y comprometida de lo que en realidad es.

Lo cierto es que el crecimiento económico sostenible y el bienestar social presentes y futuros de Europa se valen cada vez más de los valores creados por los datos. La IA es una de las partes más importantes de la economía de los datos[12]. Hoy en día, la mayor parte de los datos son relativos a los consumidores y se almacenan y tratan en infraestructuras ubicadas en nubes centralizadas. Frente a esto, una enorme proporción de los datos del futuro, que serán mucho más abundantes, procederá de la industria, las empresas y el sector público, y se almacenará en diversos sistemas, entre los que destacan los dispositivos informáticos que operan en el borde de la red. Este hecho ofrece nuevas oportunidades a Europa, que cuenta con una posición sólida en la industria digitalizada y las aplicaciones de comunicación empresarial, pero con una posición relativamente frágil en las plataformas de consumidores.

En otras palabras, la IA es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática. Los avances en computación y la creciente disponibilidad de datos son, por tanto, un motor fundamental en el pronunciado crecimiento actual de la IA. Europa puede aunar su potencial tecnológico e industrial con una infraestructura digital de gran calidad y un marco regulador basado en sus valores fundamentales para convertirse en líder mundial de la innovación en la economía de los datos y sus aplicaciones, tal como se establece en la Estrategia Europea de Datos.

Como conclusión a lo dicho hasta aquí, hay que reconocer que existe la necesidad de lograr una gobernanza de la IA, y esto no puede conseguirse sólo con ética, cuyo papel es esencial sin duda, sino con principios jurídicos fuertes[13]. A entender estos principios y su aplicación en el ámbito constitucional va dirigido este capítulo.

Este texto pretende contribuir a la creación de IA, puesto que el pensamiento jurídico no es sólo "inteligencia aplicada" sino creación de inteligencia (Jonas, 1995). La inteligencia jurídica es uno de los grandes logros del pensamiento humano. El Derecho es tanto el origen como el resultado de una forma peculiar de inteligencia. Pero ante un desarrollo sin precedentes de la Ciencia y de la Tecnología corremos el peligro de que se quede atrás. Si el Derecho no se da prisa y deja de ser un actor residual de la transformación de la realidad estamos arriesgando demasiado. Esto exige

[12] Serrano Pérez, Mª M., y Fernández Aller, Mª C., (2020). *El valor del dato en la Economía digital.* Nº: 21/2020. 02-07-2020. Ed. Fundación Alternativas.

[13] Robles Carrillo, Margarita (2020) Human Rights Law as the principal legal framework for the regulation of AI. "Artificial Intelligence: from ethics to law". *Telecommunications Policy*.

un Derecho cada vez más inteligente y en condiciones de tratar con las nuevas formas de inteligencia que protagonizan las sociedades avanzadas. Para ello es preciso abandonar una visión meramente regulativa. El Derecho no se limita a regular la realidad. No podemos conformarnos con decir que va a remolque de la sociedad. El Derecho es constructor de realidad. La tecnología jurídica es capaz de crear realidades artificiales que transforman el mundo.

Un campo que merece atención es el del impacto de la IA en los derechos fundamentales de las personas. Este capítulo se dedicará precisamente a estudiar las interrelacciones existentes entre los derechos de las personas y la AI, desde el punto de vista del Derecho constitucional, que necesitará una nueva mirada, otras orientaciones, y con toda seguridad, nuevas regulaciones.

2. LA INTELIGENCIA ARTIFICIAL DESDE UN ENFOQUE CONSTITUCIONAL

La IA tiene un papel transformador esencial en la sociedad a través de la combinación de datos, lo que puede representar una intromisión en la vida de los ciudadanos. Por la afectación de estos procedimientos a los individuos y potencialmente a sus derechos fundamentales es necesario regular y someter a criterios jurídicos los tratamientos de IA. Aunque todavía es pronto para su generalización, la extensión de la IA originará ventajas en el día a día de los individuos y de las sociedades, así debería ocurrir en la mayoría de las ocasiones. Los avances en IA no tienen otro sentido que mejorar las condiciones de vida de la humanidad. Pero también pueden producirse situaciones que lastren la libertad y los derechos de los sujetos[14]. Esas dos razones, en especial y sobre todo la segunda, justifican por sí solas la perspectiva constitucional para estructurar y dar consistencia jurídica al máximo nivel a un elemento que provocará (ya lo hace) una revolución a todos los niveles imaginables.

Junto a estos poderosos argumentos, mejorar las condiciones de vida y la protección de los derechos de los ciudadanos, la IA es un fenómeno ligado a la tecnología y al tratamiento de los datos personales, en la medida en que los procesos de IA utilicen informaciones personales para extraer conclusiones[15], elementos ambos, la tecnología y el tratamiento de datos personales, que hace tiempo quedaron interesados por un enfoque jurídico. Ambos fenómenos forman parte de un mundo globalizado en el que la regulación jurídico constitucional a la que recurrimos y en la que buscamos

[14] Tal y como refleja el *Libro Blanco sobre inteligencia artificial*..., ob. cit., pág. 1, "…la inteligencia artificial (IA) conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos", disponible en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

[15] Según el *Libro Blanco sobre inteligencia artificial*…, ob. cit., pág. 2, "la inteligencia artificial es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática".

apoyo y justificación se mueve en torno a parámetros que van más allá del entorno constitucional estatal y por tanto de la influencia de las constituciones de todos y cada uno de los países implicados, que por otro lado comparten los elementos constitucionales fundamentales entre los que han de moverse las tecnologías y los datos. Debido a la globalización también en el campo tecnológico, hay que buscar en los valores constitucionales comunes las habilitaciones y limitaciones precisas para que el desarrollo de la IA, como de cualquier tecnología, no constituya una amenaza para el ser humano. Pero además, la perspectiva no solo ha de ser jurídica, sino que es preciso ahondar en los criterios éticos comúnmente aceptados, tal y como hemos apuntado ya, para ofrecer un modelo de regulación completo y útil.

Abordar la regulación de la IA desde postulados éticos y jurídicos compartidos exige, por tanto, el compromiso conjunto de Europa y de sus Estados miembros. Diseñar la IA desde un marco constitucional, legal y ético, es una obligación de los poderes públicos en un Estado social y democrático de Derecho, que han de desarrollar y sostener dicha regulación sobre la base del respeto a los derechos y deberes de los ciudadanos y a los principios y criterios constitucionales, y además con una visión social y colectiva de beneficio para todos[16]. Solo construida sobre esos cimientos constitucionales, la IA generará confianza en la sociedad y en los ciudadanos y se convertirá en una herramienta de progreso y mejora de la calidad de vida de los individuos[17]. Por otro lado, afrontar la normación de la IA en perspectiva jurídica exclusivamente ofrecería una visión parcial del fenómeno, por lo que hay que complementar la regulación del Derecho con planteamientos éticos, económicos, sociales, etc.

Desde la UE la construcción de un espacio común de los datos es el objetivo perseguido a través de las normas y documentos sobre la IA. Una eventual legislación fraccionada por parte de los Estados miembros supondría un riesgo para el espacio común y para el mercado único digital, por el que ha apostado fuerte la UE como elemento de desarrollo. Por ello, en Europa, se ha ido elaborando un cuerpo normativo desde hace ya algunos años con el objetivo de alcanzar una confianza digital que facilite el crecimiento económico y afiance la posición de Europa en el mundo tecnológico. El RGPD, *el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea*[18] *y la Ley de Ciberseguridad (CSA)*[19], son algunos

[16] Sobre el valor colectivo de los algoritmos y la privacidad, Turégano Mansilla, I., "La dimensión social de la privacidad en un entorno virtual", *Era digital, sociedad y Derecho*, tirant lo blanch, Valencia 2020, pág. 34.

[17] Ha de asentarse sobre la dignidad humana y la privacidad, *Libro Blanco sobre inteligencia artificial…*, ob. cit., pág. 2. Las referencias a estos valores y al resto es un constante en todos los documentos europeos sobre la IA.

[18] DOUE L 303.

[19] *Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo de 17 de abril de 2019*, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguri-

ejemplos de la labor legisladora asumida por los órganos comunitarios para alcanzar un horizonte común en materia de IA.

Por tanto, la perspectiva constitucional de la IA en un entorno europeo común habrá de tener en cuenta los principios que derivan del Estado social y del Estado de Derecho, en especial la consecución del interés general y la protección de los derechos de los ciudadanos. La regulación armónica de la IA constituye uno de los grandes retos del Derecho constitucional en el siglo XXI.

3. LA REGULACIÓN DE LA UNIÓN EUROPEA SOBRE INTELIGENCIA ARTIFICIAL. MARCO NORMATIVO

La preocupación de la UE por la tecnología ha sido una constante desde hace ya décadas. La estrategia digital y la adaptación de Europa al nuevo modelo de sociedad digital conforma una de las seis prioridades de la Comisión para el periodo 2019-2014, además de constituir un elemento transversal para el desarrollo del resto de objetivos. La IA constituye una de las acciones esenciales de la Europa digital.

Desde la regulación de la protección de datos hasta los comienzos de normación de la IA, la idea de mercado único digital ha constituido el soporte y la meta que han conducido a los órganos legislativos europeos a desarrollar una legislación homogénea y sólida alrededor de la tecnología. Ahora bien, la consecución del mercado digital y su relación con la IA entronca con las normas que protegen el derecho a la protección de datos, que aun extramuros de las competencias de la UE constituye una materia asumida parcialmente por los órganos comunitarios, ante la necesidad de asegurar una legislación uniforme en toda la Unión que protegiera la libre circulación de los datos. Por tanto, con la sustracción efectuada al legislador nacional, al menos parcialmente, se procura equilibrar el derecho a la protección de datos con la libre circulación de los mismos, esta ultima libertad fuera de la órbita competencial estatal, pero necesaria para afianzar el mercado común, no solo en su versión última de mercado único digital. Pero la IA también maneja datos no personales, por lo que requiere una normativa específica que regule su uso, siempre en beneficio del ser humano.

En el año 2018, la Comisión publica el *Plan coordinado sobre Inteligencia Artificial*[20], en cumplimiento del documento *Estrategia Europea* de abril del mismo año[21].

---

dad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).

[20] *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan coordinado sobre la inteligencia artificial*, en adelante el Plan coordinado, COM (2018) 795 final, disponible en https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-795-F1-ES-MAIN-PART-1.PDF, pág. 1.

[21] *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Inteligencia artificial para Europa*, en adelante

La *Estrategia Europea* señalaba que "el término "inteligencia artificial" se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía- con el fin de alcanzar objetivos específicos"[22].

El documento señalaba la importancia de la IA en nuestro modo de vida y la necesidad de que la UE adoptara un planteamiento coordinado para aprovechar de la mejor manera las oportunidades que brinda la IA, disponiendo de los siguientes recursos: "investigadores, laboratorios, empresas emergentes, mercado único digital, un conjunto elevado de datos en la industria, investigación y sector público". De este modo Europa se proponía ser competitiva en IA, potenciar su capacidad tecnológica e industrial e introducir la IA en la todos los sectores económicos[23], cuestión principal -la economía-, en la UE, que está presente en todas las acciones de la Unión. Ser, en definitiva, líder en transformación digital, pero teniendo como referencia ética y jurídica los valores de la UE, en concreto el respeto al contenido del RGPD en lo que a datos de carácter personal se refiere[24]. La ambiciosa meta marcada por la UE, con el fin de no desperdiciar las oportunidades que brinda la IA, exige una actuación coordinada desde la Unión dirigida a todos los Estados miembros.

La coordinación a que aspira la UE se proyectaría, según la *Estrategia Europea*, a través de la consolidación de un marco ético y jurídico adecuado, un marco de confianza que además obligue a la rendición de cuentas por los actores implicados. La Estrategia recuerda el marco normativo sólido sobre el que se debe asentar la inteligencia artificial, en concreto los valores consagrados en el art. 3 TUE, así como en la CDFUE. En lo que respecta a los datos, el RGPD garantiza un elevado nivel de protección de los datos desde el diseño y por defecto. La garantía de la protección de

---

La *Estrategia Europea*, COM (2018) 237 final, disponible en https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF

[22] La *Estrategia Europea* menciona ejemplos diarios que utilizan IA, traducir de un idioma, bloquear el correo no deseado, en sanidad, en agricultura, cit., pág. 2.

[23] La integración de la inteligencia artificial en todos los sectores económicos no solo abarca las grandes empresas, sino que Europa propone la digitalización de las pequeñas y medianas empresas por lo que es imprescindible incrementar la inversión privada. La Comisión se propone la captación de más inversión privada en IA a través del Fondo Europeo para Inversiones Estratégicas en el periodo de 2018-2020. Aunque el marco financiero plurianual del 2021-2027 contempla un abanico de espacios propuestos por la Comisión para la captación de inversiones, *La Estrategia*…, ob. cit., https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF, pág. 12.

[24] En lo que respecta a la utilización de datos, la Comisión ha presentado iniciativas para ampliar el espacio de los datos. En concreto ha presentado "una actualización de la Directiva sobre la información del sector público (tráfico, meteorología, datos económicos y financieros, o registros mercantiles); directrices sobre la puesta en común de datos del sector privado en la economía; actualización de la Recomendación relativa al acceso a la información científica y a su preservación; y una Comunicación sobre la transformación digital de la sanidad y la asistencia sanitaria", https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF, pág. 14.

los datos de carácter personal y de la libre circulación de los datos resultan imprescindibles para poder extender las oportunidades de la IA. La libre circulación de los datos abarca la elaboración de perfiles cuya técnica concede al sujeto el derecho a recibir información sobre la lógica que sostiene dichas decisiones (art. 13, apartado 2, letra f), at. 14,2, g) y art. 15,1, letra h) RGPD. La libre circulación de los datos favorecerá la consolidación del mercado único digital, que se alcanzará también con la libre circulación de datos no personales, cuya normativa se está ultimando, así como el Reglamento sobre privacidad y comunicaciones electrónicas[25] y el Reglamento sobre Ciberseguridad ya aludido.

La batería normativa desarrollada desde los órganos europeos conseguirá (es su pretensión) que, tanto los ciudadanos como las empresas, alcancen la confianza necesaria en la IA para emplearla sin temor al riesgo que puede entrañar para los derechos de los individuos.

Pero la UE es consciente que las herramientas jurídicas no serán suficientes para crear un clima adecuado al desarrollo de la IA, por lo que la Comisión también la elaboración de directrices éticas teniendo en cuenta la CDFUE. Así pues, "el proyecto de directrices abordará cuestiones tales como el futuro del trabajo, la equidad, la seguridad, la protección, la inclusión social y la transparencia de los algoritmos. En términos más generales, en él se examinará el impacto en los derechos fundamentales, en particular, a la intimidad, la dignidad, la protección de los consumidores y la lucha contra la discriminación. Se basará en el trabajo que desarrolla el Grupo europeo de ética de la ciencia y de las nuevas tecnologías y se inspirará en otras iniciáticas similares"[26]. En este sentido la Agencia de los Derechos Fundamentales de la UE llevará a cabo una evaluación para constatar el impacto que los desafíos actuales de la tecnología pueden representar para los derechos fundamentales. Como consecuencia del ritmo de desarrollo de la IA, la Comisión se propone, con indudable acierto, la revisión de los marcos jurídicos actuales para su adaptación a los retos planteados y garantizar en todo momento evolutivo el respeto a los valores básicos y los derechos fundamentales de la UE.

Por tanto, de la *Estrategia Europea* sobre IA destaca la exigencia, resaltada por la propia UE, de actuar de manera conjunta para implicar a todos los ciudadanos en la transformación digital, dedicar los recursos suficientes para impulsar la IA y trasladarla a todo el entramado económico. Todo ello con el respeto a los valores y derechos fundamentales de la Unión[27].

---

[25] *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE* (Reglamento sobre la privacidad y las comunicaciones electrónicas) COM/2017/010 final - 2017/03 (COD), disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[26] *Estrategia Europea*…, ob. cit., pág. 18.

[27] *Estrategia Europea*…, ob. cit., pág. 23.

Tras la *Estrategia Europea* y de acuerdo con sus postulados, la Comisión elabora a finales del 2018 el *Plan coordinado sobre inteligencia artificial* entre todos los Estados miembros en el que alienta a los Estados a fijar un plan nacional de acuerdo con los documentos europeos[28], incluyendo el desarrollo de estrategias nacionales de IA para el año 2019, con planes de inversión y medidas de implementación. La Comisión solicita a los colegisladores la adopción de medidas para la implantación del mercado único digital y por supuesto medidas financieras. El Consejo Europeo aprobó el *Plan coordinado sobre inteligencia artificial* e instó a trabajar en la línea de la innovación digital[29]. Junto al Plan coordinado señalado, el Anexo posterior al mismo[30] constituye la primera edición del Plan y contiene las actividades que se fijan para el intervalo temporal de 2019 y 2020 (aunque la pandemia de estos años ha priorizado irremediablemente otras iniciativas), poniendo el acento en las actividades planificadas desde la UE en el marco financiero actual. La previsión de ejecución del Plan se extiende hasta 2027.

La *Estrategia Europea de Datos*, de 19 de febrero de 2020[31] es coetánea con la comunicación titulada "Modelar el futuro para digital de Europa" y con el *Libro Blanco sobre inteligencia artificial*, documentos en los que se recoge la manera en que la Comisión debe apoyar y promover tanto el desarrollo como el empleo relacionado con la IA en toda Europa. La Estrategia de 2020 insiste en el valor central del ser humano y en la importancia de los datos como bien social y económico[32].

Ya sabemos que la aspiración europea es crear un mercado único de los datos, de todos, de los personales y de los no personales, cada una de las categorías con su normativa de protección, y aportar seguridad al manejo de los datos. La circulación

---

[28] Hasta el momento de elaboración del Plan de coordinación los países que han redactado un plan sobre IA son Francia, Finlandia, Reino Unido, Italia, Dinamarca, Suecia, Austria, Alemania, España, Polonia, Países Bajos y Suecia. España en respuesta a todos los documentos europeos ha elaborado ENIA, Estrategia Nacional de Inteligencia Artificial, noviembre 2020.

[29] Conclusiones del Consejo Europeo de 28 de junio de 2018, disponible en https://www.consilium.europa.eu/es/press/press-releases/2018/06/29/20180628-euco-conclusions-final/#

[30] *Anexo de la Comunicación de la Comisión al Parlamento europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Plan coordinado sobre inteligencia artificial*, disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0022.02/DOC_2&format=PDF

[31] *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos*, COM (2020) 66 final, disponible https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066

Diapositivas sobre la Estrategia de 2020 https://ec.europa.eu/commission/presscorner/detail/es/fs_20_283

[32] La perspectiva humana se bifurca de dos maneras. Por un lado, los datos deben servir para afrontar las necesidades de las personas y mejorar su vida y por otro, el ser humano debe formar parte de los procesos de inteligencia artificial pues con su intervención se asegurará el respeto a los derechos fundamentales. El valor del dato como bien social y económico adquiere su plenitud en la vida empresarial y social..., ob. cit., pág. 10 y ss.

de los datos en toda la UE y en todos los sectores ha de respetar las normas y valores sobre protección de datos, entre otra normativa aplicable. Esta legislación debe ser clara y debe garantizar el principio de seguridad jurídica. Europa, señala la Estrategia, aspira además a la soberanía digital, posición principal frente al resto de la comunidad internacional[33] y esa primacía exige incorporar no solo inversiones en infraestructuras y tecnología, sino también iniciar un proceso de alfabetización en materia de datos a través del derecho a la educación, aunque no solo.

Las acciones que recoge la Estrategia se basan en cuatro pilares: a) un marco de gobernanza intersectorial para el acceso a los datos y su utilización. En este sentido la Comisión tenía previsto iniciar en el primer semestre de 2021 un acto de ejecución sobre conjuntos de datos de gran valor en el marco de la Directiva sobre datos abiertos[34], de manera que estén disponibles de forma gratuita y en un formato legible en toda la UE y proponer una norma sobre datos para 2021; b) inversiones en datos y refuerzo de las capacidades e infraestructuras de Europa para albergar, tratar y utilizar los datos, interoperabilidad (en el periodo 2021-2027)[35]; c) competencias para empoderar a las personas, invertir en cualificaciones y en pymes. Empoderamiento a través de los derechos que reconocen las normas, en especial el derecho a la portabilidad y el resto de los derechos que forman parte del contenido esencial del derecho a la protección de datos, y para la adquisición de competencias digitales básicas y específicas, lo que requiere un enfoque de la educación con perspectiva digital, tal y como aparece regulado en el art. 83 LOPDGDD. El tejido empresarial de las pymes precisa una atención determinada y su desarrollo y consolidación dependerá, en un futuro ya cercano, del acceso a datos; d) por último, hay que habilitar espacios comunes europeos de datos en sectores estratégicos y en ámbitos de interés público[36].

---

[33] En la actualidad la superioridad de Europa en materia digital pretende afirmarse frente a Estados Unidos.

[34] *Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público* (versión refundida), DOCE L 172.

[35] La UE aspira a elaborar un código normativo de computación en la nube, como compendio de los códigos de conducta relativos a datos en la nube, con el fin de regular el mercado europeo de servicios en la nube (2022).

[36] La Comisión apoyará la creación de los nueve espacios comunes europeos de datos: el relativo a la industria (fabricación), al Pacto Verde, a la movilidad, a la salud, en materia financiera, relativo a la energía, al sector agrario, a las administraciones públicas y en materia de cualificaciones. Todo ello con un enfoque internacional abierto, pero con el respeto a los valores europeos, en especial la intimidad cuando se trate de datos personales. En lo que respecta a los datos no personales la seguridad y las reglas justas y fiables. Respecto del Paco Verde, la Estrategia Europea empleará la tecnología para hacer de Europa un espacio limpio y climáticamente neutro. Los datos representan un potencial significativo que pueden reforzar el Pacto Verde Europeo y apoyar las acciones prioritarias en relación con el cambio climático, economía circular, contaminación cero, biodiversidad, deforestación y garantía de su cumplimiento, ob. cit., pág. 27. Por lo que respecta a los datos de salud, la pretensión de la Europa digital en materia de salud es crear un espacio de datos de salud que favorezca la investigación y el diagnóstico médico.

La consolidación de la soberanía digital de Europa exige el control de las transferencias internacionales. Europa aspira no solo a crear el espacio europeo de los datos sino, desde un enfoque abierto, conectar con el entorno digital fuera de las fronteras de la Unión, lo que exige fomentar la cooperación internacional en materia de datos. Los flujos internacionales de datos constituyen un valor en sí mismo[37] y la sociedad digital no entiende ni debe someterse a fronteras. En ocasiones, los obstáculos y las restricciones digitales obedecen a normas y criterios diferentes y, sobre todo, a mecanismos de garantía desiguales para los derechos de los sujetos. Además de promover desde las instituciones europeas los flujos de datos con terceros países de confianza de forma segura, la UE trabaja para exportar sus normas y valores al resto de la comunidad internacional. El modelo europeo, que garantiza un efectivo control del sujeto sobre sus datos personales y los mecanismos para restaurar las lesiones provocadas en el derecho a la protección de datos personales, constituye una buena herramienta legislativa para homogeneizar el espacio internacional de los datos. Así, el RGPD ha constituido un referente en materia de protección de datos para las legislaciones latinoamericanas más recientes, convirtiéndose en un estándar común a imitar. En EEUU, algunos estados han regulado inspirados en nuestro RGPD. El Estado de California aprobó la Ley de Privacidad del Consumidor de California (CPA) que entrará en vigencia en 2020, inspirada en el GDPR de la Unión Europea.

El *Libro Blanco sobre la inteligencia artificial*[38] que acompaña a la Estrategia aboga por el desarrollo de un ecosistema de IA que aproxime las ventajas de la misma y cuyo objetivo redunde en beneficio de los ciudadanos, de las empresas y de los servicios de interés público[39]. Este escenario de la IA debe asentarse sobre los valores

---

[37] Con vistas a facilitar de mejor manera los flujos internacionales de datos, la Comisión creará un marco analítico europeo para la medición de los flujos de datos, fechado para el cuarto trimestre del 2021, "Este debe ser un marco duradero que proporcione instrumentos para llevar a cabo un análisis continuo de los flujos de datos y del desarrollo económico del sector europeo de tratamiento de datos, incluidos una metodología sólida, una valoración económica y mecanismos de recogida de flujos de datos. Servirá para comprender mejor las pautas de los flujos de datos y los centros de gravedad, tanto dentro de la UE como entre la UE y el resto del mundo, y puede servir de base para que, en su caso, la Comisión ofrezca las respuestas políticas. También debería contribuir a impulsar una inversión adecuada para superar las posibles carencias de infraestructuras que impidan los flujos de datos. Por consiguiente, la Comisión solicitará a su debido tiempo la cooperación con las organizaciones financieras e internacionales pertinentes en lo referente al marco de medición de los flujos de datos (por ejemplo, el BEI, el BERD, la OCDE, el FMI)", *Estrategia Europea*…, ob. cit., pág. 28.

[38] *Libro Blanco sobre la inteligencia artificial*..., ob. cit.

[39] *Libro Blanco…,* ob. cit., pág. 3. El Libro Blanco habla de sectores empresariales en los que Europa es especialmente fuerte, como "maquinaria, transporte, ciberseguridad, agricultura, economía verde y circular, atención sanitaria y sectores de gran valor añadido, como la moda y el turismo), mientras que en el ámbito de los servicios de interés público, "por ejemplo mediante una reducción de los costes de la prestación de servicios (transporte, educación, energía y gestión de los residuos), una mayor sostenibilidad de los productos, o proporcionando a los servicios y fuerzas de seguridad las herramientas adecuadas para que aseguren la protección de los ciudadanos".

europeos, llamada constante de todos los documentos mencionados, de forma que los beneficios del uso de mecanismos de IA reviertan en los ciudadanos europeos y no vayan en detrimento del ejercicio y disfrute de sus derechos. El Libro Blanco alude a la necesidad de generar confianza en los ciudadanos, el llamado "ecosistema de confianza", a través de normas europeas que velen por la protección de los derechos fundamentales y por la protección de los derechos de los consumidores. Esto es, un conjunto normativo anclado en las características del Estado de Derecho que favorezca la seguridad jurídica para que las empresas y organismos públicos adopten las aplicaciones de IA en su tarea cotidiana. Junto a la confianza que deben proporcionar las normas, ha de alcanzarse de forma simultánea una situación de excelencia en el conocimiento y en el dominio de la IA, el llamado "ecosistema de excelencia", que capacite tanto al sector público como al privado y a los ciudadanos para el empleo ágil y seguro de los servicios ofrecidos. El bienestar social presente y futuro y la economía sostenible dependen cada vez más de los datos, en la medida en que estos incorporan también un valor social y colectivo que hay que potenciar y proteger.

La consecución del ecosistema de excelencia contempla acciones dirigidas a consolidar de forma segura la IA y desde dicha idea se aboga por la colaboración entre todos los Estados miembros para fomentar el desarrollo y la utilización de la IA en Europa[40], revisando el *Plan coordinado de inteligencia artificial* y apoyando las inversiones nacionales y privadas. Igualmente se destaca la necesidad de mejorar las capacidades de la población en lo que a competencias digitales se refiere, pero también incrementar la posibilidad de atraer talento de fuera de la Unión. Por otro lado, la preocupación europea de la extensión por la IA a las pymes y la necesidad de contar para ello con acceso a la financiación desde un colaboración público privada es constante.

En lo que respecta a la consecución del ecosistema de confianza, el aspecto fundamental a tener en cuenta es la elaboración de normas que favorezcan el aprovechamiento de las ventajas de la IA por parte del ciudadano, sin que este vea comprometidos sus derechos fundamentales, esto es, potenciar el valor social de los datos a través de su reutilización sin menoscabo del valor individual que tienen como proyección de aspectos de nuestra vida y nuestra intimidad en la sociedad digital. A estos efectos la Comisión publicó una Comunicación en la que asumía los requisitos señalados por el grupo de expertos que debían hacer una IA fiable: acción y supervisión humana; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y medioambiental; rendición de cuentas[41].

---

[40] La colaboración entre la Comisión y los Estados miembros se plantea en "áreas clave como la investigación, la inversión, la introducción en el mercado, las capacidades y el talento, los datos y la cooperación internacional". El Plan estará operativo hasta 2027 y se revisará regularmente, *Libro Blanco sobre inteligencia…*, ob. cit., pág.

[41] *Libro Blanco sobre inteligencia…*, ob. cit., pág. 13.

Las directrices señaladas no son vinculantes, pero recogen principios a tener en cuenta en la futura legislación y defienden la necesidad de elaborar una normativa clara para Europa que redundaría en la confianza necesaria para la extensión de la IA. La regulación debe ser complementaria con otras medidas con el fin de promover la capacidad innovadora y competitiva de Europa en este sector. Aunque en materia de protección de datos la norma reguladora ya existe, las características peculiares de la IA (en especial la opacidad, señala la Comisión) pueden requerir una adaptación de la norma o una nueva legislación. Por otra parte, la legislación que se aborde debe dejar espacio para su ajuste futuro a los rápidos avances de la materia estudiada. La legislación común en materia de IA debe abordarse sin demora, pues la normativa desarrollada en algunos países de la UE al respecto puede provocar la fragmentación del espacio europeo y quebrar la armonía legislativa que debe existir en este ámbito.

Por otro lado, desde Europa se trabaja en foros multilaterales como la OCDE y el G20 para la elaboración de principios éticos en materia de IA[42]. Asimismo, los documentos europeos destacan la importancia de la IA en el cumplimiento de los Objetivos de Desarrollo Sostenible[43].

Tal y como hemos señalado en páginas atrás los datos no personales son una herramienta importante para la IA y deben ser objeto de regulación tanto su reutilización como el acceso a estos, así como cuestiones éticas, de responsabilidad y de solidaridad. Aunque el trabajo principal en IA se lleva a cabo con datos anonimizados y con conjuntos de datos agregados, es necesaria una regulación uniforme que afronta el Reglamento relativo a un marco para la libre circulación de datos no personales en la UE. El propio Reglamento recuerda además que, si las posibilidades tecnológicas propiciaran la identificación de los sujetos a través de la reversión de los datos anonimizados con los que trabaja la IA y por tanto se transformaran en datos personales, la norma aplicable en dichos procesos sería el RGPD.

3.1. La propuesta de Reglamento por el que se establece el programa Europa Digital

La propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el periodo 2021-2027[44] recoge los planteamientos

---

42 *Libro Blanco sobre inteligencia…*, ob. cit., pág. 11

43 *Libro Blanco sobre inteligencia…*, ob. cit., pág. 3.

44 *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el periodo 2021-2017* COM (2018) 434 final, disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52018PC0434. El Parlamento europeo ha votado a favor de la propuesta de financiación que recoge el programa Europa Digital 2021-2027, para el desarrollo de la inteligencia artificial, la informática de alto rendimiento, la ciberseguridad y las competencias digitales.

europeos en IA contenidos en los documentos anteriormente vistos. Desde el punto de vista formal y en congruencia con el peligro ya advertido de la posibilidad de fragmentación del espacio europeo de los datos con legislaciones propias de cada Estado miembro, los órganos europeos proponen la regulación de la IA a través de un acto legislativo directamente aplicable en todos los países de la Unión y cuya obligatoriedad y eficacia quedan al margen de la intervención de una norma interna. El empleo de este tipo de norma evidencia la necesidad de establecer un marco común en la materia regulada y aplicable al tiempo en todos los Estados miembros, donde se contemplan, como pilares clave que sustentan la transformación digital de la economía y de la sociedad para los próximos diez años (al menos, constata la propuesta), la computación avanzada, el tratamiento de datos, la ciberseguridad y la IA. En estos ámbitos, el Reglamento establece los objetivos y el presupuesto del programa Europa Digital 2021-2027, las formas de financiación y las normas para la concesión de la misma (art. 1 Reglamento).

El documento representa básicamente un importante instrumento de financiación para consolidar la transformación digital de la economía y de la sociedad europea[45]. Dicho programa reconoce la necesidad de invertir para impulsar la transformación digital en espacios de interés público, así como en el ámbito empresarial[46], lo que redundará en beneficio de la economía, de la sociedad europea y por supuesto de los ciudadanos. El programa tiene como el segundo de sus objetivos específicos la IA (art. 3.2 b) Reglamento). La aportación financiera en este objetivo persigue los siguientes objetivos operativos (art. 5 Reglamento):

> "a) Intensificar y reforzar las capacidades básicas de inteligencia artificial en la Unión, incluidos los recursos de datos y las bibliotecas de algoritmos de conformidad con la legislación sobre protección de datos;
>
> b) hacer accesibles dichas capacidades a todas las empresas y administraciones públicas;
>
> c) reforzar y poner en red las instalaciones de ensayo y experimentación de inteligencia artificial existentes en los Estados miembros".

Los objetivos de la propuesta de Reglamento inciden por tanto en la necesidad de incrementar las capacidades en IA, con el respeto a la legislación de la protección

---

[45] Aunque en consonancia con la intención de la UE de convertirse en el espacio líder en tecnología digital, el programa Europa Digital estará abierto para su integración a países de la Asociación Europea de Libre comercio que son miembros del Espacio Europeo y a otros candidatos (art. 10 propuesta de Reglamento).

[46] Europa reconoce que la insuficiencia de inversiones en el pasado ha obligado a los científicos e ingenieros de la UE a recurrir a los recursos informáticos de fuera de Europa, en especial de Estados Unidos, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa…, Exposición de Motivos, ob. cit. Con el fin de superar la situación de subdesarrollo del mercado de IA en relación con el de EEUU, donde las capacidades de datos facilitan la innovación en el sector a gran escala, la UE constata que los puestos de expertos altamente cualificados en ámbitos como la IA, el análisis de datos y la ciberseguridad no se cubren. La demanda europea es muy elevada.

de datos, pues la norma reconoce la necesidad de disponer de conjuntos de datos a gran escala, lo que justificamos en beneficio social pero con las debidas cautelas, y de instalaciones de ensayo y experimentación[47], favorecer la accesibilidad de las capacidades a las empresas y al sector público y reforzar e impulsar las iniciativas ya existentes en los Estado miembros. La cantidad asignada (art. 9.2 b) propuesta de Reglamento) aspira a crear el sostén económico necesario para el desarrollo y consolidación de la IA. A estos efectos, la propuesta contempla la creación de una red inicial de centros de innovación digital que podrán recibir financiación para proporcionar a las empresas, organizaciones del sector público, las pymes y las empresas de capitalización media servicios temáticos relacionados con la IA (art. 16).

4. EL ESTADO SOCIAL Y LA INTELIGENCIA ARTIFICIAL

El Estado social constituye una estructura jurídico constitucional que contempla la intervención dinámica y activa del poder público en la sociedad desde una perspectiva comprometida con una finalidad concreta, que es asegurar la igualdad y la libertad de los individuos y los grupos. El art. 9.2 CE lo recoge con claridad: "Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover todos los obstáculos que impiden o dificulten su plenitud y facilitar la participación de los ciudadanos en la vida política, económica, cultural y social".

De Estado del bienestar se habla para referirse al nivel de prestaciones que el poder público mantiene en la sociedad y al alto grado de satisfacción que con ello deben alcanzar la mayor parte de los individuos. La obligación de remover los impedimentos que dificultan el disfrute de condiciones de vida dignas se concreta en la previsión de actuaciones dirigidas a un conjunto de sectores y ámbitos materiales que demandan la intervención de los poderes públicos y que constituyen los principios rectores de la política social y económica (Capitulo III, del Título Primero de la Constitución, arts. 39 a 52). La concentración de principios materiales en dicho capítulo no significa que fuera de él no encontremos también derechos que requieren una fuerte intervención del Estado para su disfrute y ejercicio, por ejemplo, el derecho fundamental a la educación, cuya naturaleza prestacional lo convierte en un elemento pilar del Estado social como Estado interventor y proveedor y que además adquiere en el campo digital una dimensión esencial.

[47] La propuesta de Reglamento reconoce en la Exposición de Motivos (40) que "El Reglamento general de protección de datos (RGPD), aplicable desde mayo de 2018, al ofrecer un conjunto único de normas directamente aplicables en los ordenamientos jurídicos de los Estados miembros, garantizará la libre circulación de datos personales entre los Estados miembros de la UE y reforzará la confianza y la seguridad de las personas, dos elementos indispensables para un verdadero mercado único digital. Las acciones emprendidas en el marco del presente programa, cuando impliquen el tratamiento de datos personales, deben, por consiguiente, contribuir a la aplicación del Reglamento general de protección de datos, por ejemplo, en el ámbito de la inteligencia artificial y la tecnología de la cadena de bloques."

El surgimiento del Estado social en el siglo XIX, tras el fracaso del Estado liberal como Estado abstencionista, aparece conectado con la inclusión en los textos constitucionales, como consecuencia de demandas democráticas y de la mayor participación de la sociedad en los procesos de decisión política, de un conjunto de derechos sociales y laborales, de prestaciones y acciones en favor de la mejora de las condiciones de vida de los ciudadanos. En el siglo XXI y en la actual sociedad digital, la labor del Estado desde el enfoque prestacional tiene perfiles muy definidos, pues está fuertemente determinada por los avances tecnológicos y por las necesidades que la sociedad demanda ante dichos adelantos, así como por las prestaciones que hay que cubrir. Se habla del Estado del bienestar digital[48] en el contexto tecnológico y se incide, por una parte, en las ventajas que la extensión de dichos servicios pueden representar para los derechos fundamentales y en la obligación de prestarlos, y por otra parte en la dependencia del bienestar social e individual, cada vez en mayor grado, del correcto manejo de la tecnología y de la información que proporcionan los datos[49]. Desde los documentos europeos se insiste en la importancia de la IA para el desarrollo del bienestar social desde todos los frentes imaginables, por ejemplo, a través de la protección medioambiental[50].

Con independencia de la amenaza concreta que el uso de la tecnología y de la IA puede suponer para el disfrute de los derechos fundamentales, como espacio de libertad del individuo y que se abordará desde la configuración del Estado de Derecho y de la casuística, el rápido desarrollo de la IA y su despliegue en todos los sectores sociales pueden favorecer surgimiento de profundas desigualdades a todos los niveles. Son las denominadas brechas digitales[51] (que ya han aparecido con la extensión de la tecnología) y que provocan una situación que ataca de lleno un elemento esencial del Estado social como es la consecución de la igualdad real. La lucha contra dichas brechas constituye una finalidad activa y presente en la misma esencia de dicho modelo de Estado, esto es, remover los obstáculos y las barreras que dificulten la implantación de la igualdad y la libertad.

Las brechas digitales provocadas por la falta de acceso a las tecnologías, en su modalidad de IA o de cualquier otra, deben ser combatidas desde el poder público para evitar que el acceso a recursos y oportunidades fracture la sociedad. En efecto, las brechas digitales que pueden producirse afectando al disfrute de los derechos fundamentales si no se derriban, corrigen y eliminan podrían ocasionar una fisura difícil

---

[48] Lazcoz Moratinos, Guillermo y Castillo Parrilla, José Antonio, "Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI", *Revista chilena de Derecho y Tecnología*, vol. 9, 1 (2020) págs. 207-225, p. 209.

[49] *Libro Blanco sobre inteligencia*…, ob. cit., pág. 3

[50] *Libro Blanco sobre inteligencia*…, ob. cit., pág. 7.

[51] Sobre las brechas digitales ver el documento de la OCDE, Resumen. Perspectivas de la OCDE sobre las tecnologías de la información en 2002, disponible en http://www.oecd.org/digital/ieconomy/1933290.pdf

de enmendar. Pese a los esfuerzos para que el acceso a la información, la generalización del conocimiento y la difusión de las tecnologías de la información y la comunicación lleguen a todos los rincones, existe una disparidad en su uso, que puede tener su origen en diferencias de género, raza, económicas, mundo rural y mundo urbano, capacidades, mayores, etc. El peligro de excluir del beneficio del uso de los sistemas de IA a colectivos desfavorecidos y con menores oportunidades podría amplificar las desigualdades. Las desigualdades pueden reflejarse incluso entre países, en caso de que los menos avanzados tecnológicamente deban importar sistemas ajenos que no se acoplen bien a sus peculiaridades sociales y culturales, por lo que quedarán en una posición de debilidad. En sentido contrario, a mayor inclusión social mayor inclusión y desarrollo digital y aumento del desarrollo y del bienestar de la sociedad[52].

El Estado, de manera inexcusable, y también los poderes privados, deben contribuir a la difusión de los procesos de IA de manera democrática, justa e inclusiva. Como hemos tenido ocasión de analizar, el compromiso económico para la financiación de la extensión de las aplicaciones de IA es un compromiso asumido y emprendido por la UE y que compromete la acción del poder público en la dirección de llevar a cabo todas las acciones para facilitar la extensión de las tecnologías de IA. En este sentido el incremento de la inversión para disminuir y reducir la brecha digital es imprescindible.

Desde la perspectiva educativa, pilar también esencial del Estado social, se habla de alfabetización digital para referirse a la necesidad de formar en el empleo de los datos, con el fin de aumentar la población con habilidades digitales básicas y específicas, para, en este último caso, reducir la brecha existente de especialistas digitales, con atención particular a las mujeres. La LOPDGDD contempla en su art. 97 políticas de impulso de los derechos digitales, atribuyendo al Gobierno la elaboración de un Plan de Acceso a Internet, en colaboración con las comunidades autónomas para, entre otras cuestiones, "fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales".

Por otra parte, tanto *la Estrategia Europea y el Plan coordinado* (ambos de 2018) aluden al esfuerzo del sector público para favorecer la implantación de la IA en todos los sectores económicos y sociales. La Comisión habla de la creación de espacios europeos de datos comunes que agregarán datos con el fin de ponerlos a disposición del sector público y del sector privado[53]. Ya más reciente, el Libro Blanco de 2020 señala

[52] López Garrido, D. (coord.), Serrano Pérez, Mª M., Fernández Aller, C., Derechos y obligaciones de los ciudadanos/as en el entorno digital, Fundación Alternativas, Documento de trabajo 195/2017, pág. 33.

[53] *Plan coordinado*…, (COM) 2018 795, ob. cit., pág. 8.

la necesidad de que las Administraciones públicas adopten productos y servicios de IA para realizar sus funciones. En especial la administración sanitaria, transportes y otros servicios públicos[54].

4.1. La disponibilidad de los datos como obligación propia del Estado social

Insistimos en la idea según la cual el Estado social concibe el Estado como una estructura jurídica y pública cuyo fin permanente es intervenir en la sociedad desde su concepción de poder público, para trabajar en la consecución de la libertad y la igualdad real de todos los miembros de la sociedad y eso incluye la corrección y eliminación de las barreras que la imposibilitan, tal y como señala el art. 9.2 CE.

En esa función prestacional e interventora del poder público podemos enmarcar la obligación del Estado social digital de defender y procurar la disponibilidad adecuada de los datos a todos los sectores sociales para su empleo, pues su valor reside en su uso, pero también en su reutilización a través de la IA, y ambos revierten en la mejora de las condiciones de vida del ciudadano, por supuesto con las debidas garantías para la protección de los derechos, esto es, el sometimiento a la legislación de protección de datos.

Hay que recordar que, junto al valor individual del dato, las informaciones personales tienen un sentido social, una función colectiva que cumplir y que en el Estado social digital se puede lograr en un escenario en el que la reutilización de los datos se ordene y regule[55]. En este sentido hay que tener en cuenta la titularidad de los datos, su naturaleza y quién o quiénes serán sus usuarios.

En el caso de los datos de carácter personal que se encuentran en poder de las Administraciones públicas, son de aplicación los principios de protección de los datos y los derechos de que dispone el individuo para mantener el control sobre las informaciones personales que le atañen y que recoge el RGPD. Aunque el consentimiento del individuo para el tratamiento de sus datos queda muy reducido para habilitar el tratamiento de datos de carácter personal por las diferentes bases jurídicas que lo justifican al margen de aquel. No obstante, el tratamiento de datos sin necesidad de consentimiento ha de respetar los principios de la protección de datos y los derechos de los individuos.

---

[54] En concreto la Acción 6 del Libro Blanco de 2020 señala que "La Comisión iniciará conversaciones por sector abiertas y transparentes, en las que dará prioridad a la atención sanitaria, las administraciones rurales y los operadores de servicios públicos, para presentar un plan de acción que facilite el desarrollo, la experimentación y la adopción de la inteligencia artificial. Las conversaciones por sector se emplearán para preparar un «Programa de adopción de la IA» específico que respaldará la contratación pública de sistemas de inteligencia artificial, y ayudará a transformar los propios procesos de esta contratación", dentro de la actividad de promoción de la IA dentro del sector público, pág. 11.

[55] Turégano Mansilla, I., "La dimensión social de la privacidad ...", *ob. cit.*, pág. 30.

Por lo que respecta a los datos generados por el sector público que no poseen el calificativo de datos personales y que representan un beneficio para todos los ciudadanos, corresponderá a los poderes públicos propios de un Estado social favorecer su utilización y procurar su empleo en beneficio del interés y del bien público. Este tipo de datos pueden servir para mejorar las prestaciones sanitarias, para luchar contra el cambio climático y el daño ambiental, para combatir la delincuencia, etc.

El empleo adecuado que se ha de dar a los datos por parte de la Administración Pública responde a la labor que la Administración recogida en el art. 103.1 CE según el cual: "La Administración sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía y descentralización, desconcentración y coordinación con sometimiento pleno a la Ley y al Derecho", principios que se reiteran también en el art. 3 de la Ley de Régimen Jurídico del Sector Público (en adelante, LRJSP).

Los datos que favorecen el interés general deben estar al servicio de las instituciones públicas para redundar en beneficio de la sociedad, pero también hay que contemplar la posibilidad de que empresas de titularidad privada puedan servirse de estos datos (intercambio de datos entre la Administración Pública y las empresas o G2B)[56]. La apertura de la información pública controlada por la Administración constituye una política fuerte de la UE, regulada a través de la *Directiva 2019/1024 relativa a los datos abiertos y a la reutilización de la información del sector público*. El art. 1 de la Directiva señala el objeto de la norma, que es fomentar el uso de los datos abiertos y estimular la innovación de los productos y servicios, para lo cual se establecen las normas mínimas que regulan la reutilización y los dispositivos prácticos para facilitar la reutilización de: los documentos en manos de los organismos del sector público de los Estados miembros, los documentos conservados por empresas públicas, bajo las condiciones que señala el precepto y los datos de investigación de acuerdo con el art. 10.

La posibilidad de que los datos que generan las Administraciones Públicas puedan ser reutilizados por las pymes, por los investigadores y por la sociedad civil incrementa su valor y redunda en la mejora de la calidad de vida de los ciudadanos y de la sociedad, siempre con el respeto a las normas vigentes, en especial las relativas a la protección de datos. Como señala el considerando 9, "La información del sector público representa una fuente extraordinaria de datos que pueden contribuir a mejorar el mercado único y al desarrollo de nuevas aplicaciones para los consumidores y las personas jurídicas. El empleo inteligente de los datos, incluido su tratamiento a través de aplicaciones de inteligencia artificial, puede tener un efecto transformador en todos los sectores de la vida".

La Directiva define la reutilización en el contexto de la norma como "el uso por personas físicas o jurídicas de documentos que obran en poder de organismos del

[56] Estrategia de Datos… (2020), ob. cit., pág. 9.

sector público y de empresas públicas (art. 2.11)". Por otro lado, la reutilización de los datos del sector público es un elemento importante para favorecer la transparencia y la responsabilidad y mejorar la calidad de la información recopilada y tratada y el propio servicio público al ciudadano (considerando 14).

En lo que respecta a nuestro ordenamiento jurídico, el art. 155 LRJSP contempla la obligación de facilitar la transmisión de datos personales entre Administraciones Públicas de acuerdo con la normativa en vigor, (RGPD y LOPDGDD), habiendo de especificar "las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad". La norma en su apartado segundo impide el tratamiento ulterior de los datos para fines incompatibles para los que se recogieron, según el art. 5.1.b) RGPD. La utilización posterior de los datos para fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considera incompatible con los fines iniciales. Ahora bien, esta regla general admite otra excepción, siempre que las leyes especiales que contemplen los tratamientos de datos no prohíban expresamente el tratamiento ulterior para finalidades distintas de las iniciales, en el caso en que la Administración cesionaria requiera los datos para una finalidad que valore como compatible con la primera, en cuyo caso lo ha de comunicar a la Administración cedente para su valoración. La Administración Pública cedente podrá oponerse de forma motivada en el plazo de diez días. El tratamiento ulterior de datos podrá realizarse en el caso que el tratamiento de datos para fines distintos esté previsto en una norma con rango de ley, según el art. 23.1 RGPD.

Por otro lado, puede y debe facilitarse el intercambio de datos de titularidad privada por parte de los poderes públicos (intercambio de datos entre las empresas privadas y las Administraciones Públicas o B2G) (queda excluido el uso de estos datos B2G con fines policiales). Para facilitar este movimiento de datos los expertos recomiendan adoptar medidas legales, éticas y de inversión en tres áreas principales.

En primer lugar, los expertos aluden a la gobernanza del intercambio de datos B2G en la UE, lo que implica fijar estructuras de gobernanza en los Estados miembros europeos; establecer una función reconocida ("administradores de datos") en organizaciones públicas y privadas y explorar la creación de un marco regulador en toda la UE.

En segundo lugar, los expertos abogan por la transparencia, participación ciudadana y el desarrollo de pautas éticas, lo que ha de proyectarse en un intercambio de datos B2G enfocado en los ciudadanos. La centralidad de los ciudadanos obliga a los poderes públicos a invertir en capacitación y educación con el fin de favorecer la implantación y extensión de la cultura del intercambio de datos.

En tercer lugar, será necesario invertir en modelos operativos, estructuras y herramientas técnicas. Crear incentivos para que las empresas compartan datos, rea-

lizar estudios sobre los beneficios del intercambio de datos B2G[57] y brindar apoyo para desarrollar la infraestructura técnica a través de los programas Horizon Europe y Digital Europe. En lo que se refiere al intercambio de datos B2G, el Grupo de expertos ha elaborado un conjunto de buenas prácticas de intercambio de datos del sector privado al público con claros beneficios para la ciudadanía y con la finalidad de perseguir el interés general, incluyendo nuevos principios sobre responsabilidad y sobre el uso justo y ético de los datos[58].

La finalidad de crear estructuras nacionales para poner en común este tipo de datos es incentivar y potenciar una cultura de intercambio de datos y estudiar la elaboración de un marco normativo que prevea y regule la reutilización de los datos privados por parte del sector público con el objetivo de servir al interés general[59].

Así pues, los poderes públicos han de establecer un marco de interoperabilidad para evitar obstaculizar la combinación de datos de diferentes sectores o del mismo sector. El Marco de interoperabilidad revisado[60] establece la obligación de los Estados de elaborar un plan de interoperabilidad en consonancia con dicho plan diseñado desde Europa, pues el traspaso de datos debe conseguirse en la totalidad del espacio europeo. El plan debe contemplar protocolos compatibles para la recogida y tratamiento de datos entre distintos sectores. En respuesta al Marco diseñado desde Europa, los Estados miembros deben completar con acciones internas las propuestas de la Comisión, con el fin de garantizar la interoperabilidad del sector público en toda la Unión.

En España la interoperabilidad solamente se contempla en el ámbito de la actuación de la Administración Pública. Así, el art. 42 de la Ley 11/2007, de 22 de junio, de

---

57 Ejemplos de buenas prácticas conseguidas con el intercambio de datos https://ec.europa.eu/digital-single-market/en/good-practices-b2g-data-sharing

58 Algunas asociaciones exitosas de intercambio de datos B2G en la UE incluyen un sistema de datos forestales abiertos en Finlandia para ayudar a gestionar el ecosistema, mapeo de las actividades pesqueras de la UE utilizando datos de seguimiento de barcos y datos de secuenciación del genoma de pacientes con cáncer de mama para identificar nuevos tratamientos personalizados, todo ello pensando en el interés general.

59 *Estrategia Europea*… (2020), ob. cit., pág. 10.

60 El marco de interoperabilidad está definido en la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Hacia la interoperabilidad de los servicios públicos europeos* (COM) 2010 744 final, como un acuerdo para la interoperabilidad entre organizaciones que desean colaborar para la prestación de servicios públicos. Su alcance incluye un conjunto de elementos comunes tales como vocabulario, conceptos, principios, políticas directrices, recomendaciones, estándares, especificaciones y buenas prácticas", disponible en https://ec.europa.eu/transparency/regdoc/rep/1/2010/ES/1-2010-744-ES-F1-1.PDF. El Marco europeo de Interoperabilidad (EIF) revisado se contiene en la *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Marco Europeo de Interoperabilidad-Estrategia de aplicación* (COM 2017, 134 final, de 23 de marzo) de la Comisión Europea, donde se recogen 47 recomendaciones para mejorar la interoperabilidad a través de una legislación que no dificulte los esfuerzos de interoperabilidad, disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0134&from=LT

acceso electrónico de los ciudadanos a los Servicios Públicos[61], señala que el Esquema de Interoperabilidad "comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidas en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad". La misma redacción recoge el art. 156 LRJSP.

En desarrollo de la Ley 11/2007, el Real Decreto 4/2010 de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el Ámbito de la Administración Electrónica[62] crea las condiciones necesarias para garantizar la interoperabilidad en el sector público. La interoperabilidad en el sector público pretende lograr objetivos comunes en beneficio de la ciudadanía a partir del intercambio de información. El intercambio de información debe ser fiable y seguro desde el punto de vista técnico. Si bien la interoperabilidad en el sector público está regulada y asegurada, la función del Estado social de intervenir en la sociedad exige esfuerzos para garantizar la interoperabilidad entre todos los sectores, en la línea de las previsiones europeas.

La Estrategia contempla también el intercambio de datos entre empresas de titularidad privada, o datos B2B. Por lo que ahora nos interesa su desarrollo está en fase muy incipiente y precisa para su crecimiento la existencia de claridad jurídica para saber quién utilizará los datos y con qué fines (por ejemplo, internet de las cosas), tarea que compete al legislador, así como también proveer de un marco legislativo adecuado para crear un espacio común de los datos que favorezca su uso transfronterizo y ayude a consolidar una economía ágil de los datos.

5. EL ESTADO DE DERECHO Y LA INTELIGENCIA ARTIFICIAL: PRINCIPIO DE SEGURIDAD JURÍDICA E INTERDICCIÓN DE LA ARBITRARIEDAD. PRINCIPIO DE LEGALIDAD

La necesidad de encontrar el equilibrio entre el desarrollo de la sociedad basado en un uso racional de la IA y la propia IA exige una regulación que aporte seguridad al ciudadano y a las empresas. El legislador debe afrontar una regulación común y necesaria en un Estado de Derecho con base en la seguridad jurídica, en la prohibición de la arbitrariedad y en la protección de los derechos de los individuos. La ley debe ser el elemento jurídico que ha de contemplar los elementos principales de los procesos de IA, en la medida en que pueden quedar afectados los derechos de los ciudadanos. Por tanto, en un Estado de Derecho la previsión legal de la IA debe contribuit a generar confianza en la sociedad y para ello la norma que regule la tecnología a este

[61] BOE núm. 150, de 23 de junio de 2007.

[62] BOE núm. 25, de 29 de enero de 2010.

nivel debe ser predecible, responsable, verificable, respetar los derechos fundamentales y observar las reglas éticas[63].

Las normas a desarrollar para permitir el intercambio de datos a emplear en procesos de IA deben reunir unos criterios comunes adoptados por todos los Estados miembros y que han sido precisados por la UE[64]. Debe tratarse de normas que faciliten la libre circulación de los datos, circulación en lo que atañe a los datos de carácter personal que queda asegurada con el RGPD, con eficacia directa en toda la UE y en nuestro ordenamiento, y que ha sido completado en las cuestiones que el RGPD deja abiertas con la LOPDGDD. En lo que se refiere a la circulación de datos no personales la legislación busca favorecer sus movimientos en condiciones legales para generar igualmente confianza. Las normas deben ser justas, claras, prácticas, previsibles y accesibles y con un enfoque abierto y global. En este sentido el Reglamento para la libre circulación de datos no personales ya referido en este trabajo.

La alusión a una previsión legal, requisito propio de un Estado de Derecho, ha sido uno de los elementos que el TEDH ha resaltado cuando se trata de justificar la injerencia que el tratamiento de datos provoca en el derecho a la vida privada en relación con la protección de datos, porque los procesos de IA realizan intromisiones en los derechos de los individuos y pueden, por tanto, provocar una lesión. Esa injerencia debe tener habilitación legal y ser proporcionada. Con carácter general y también por tanto en relación con la portección de datos, el TEDH habla de "calidad de la ley", cualidad que exige claridad, precisión y previsibilidad para que los ciudadanos a los que se dirige la norma puedan adaptar su conducta[65].

Así pues, la previsión legal de una injerencia[66], no solo desde el punto de vista formal sino también desde la perspectiva material, no consiste solamente en un acto normativo que formalmente habilite y justifique la injerencia desde el ordenamiento nacional. El TEDH ha insistido en que, junto a la formalidad que representa la ley se debe exigir también un contenido material entendido como "calidad de ley", tal y como hemos señalado, lo que aplicado a la injerencia significa que ha de ser accesible y previsible, "de modo que los individuos puedan disponer de información suficiente sobre la norma jurídica aplicable, se les permita regular su conducta a partir de ella y prever en un grado razonable las consecuencias que una acción determinada puede acarrear"[67]. Por tanto, para que la ley sea accesible ha de ser predecible y para

---

63 *Plan coordinado*…, ob. cit. (2018), pág. 9

64 *Estrategia Europea*…, ob. cit., (2020), pág. 7.

65 STEDH sentencia de Rekvéncy c. Hungría de 20 de mayo de 1999.

66 STEDH S y Marper &100 y STEDH Graughan & 74 y ss. Sobre esta última Serrano Pérez, Mª M., "La STEDH de 13-12-2020. Los limites del tratamiento de datos biométricos de personas condenadas en relación con la protección del art. 8 CEDH", *LA LEY. Privacidad*, número 4, abril-junio 2020, Wolters Kluver, págs. 1-7.

67 Lazcoz, G., y Castillo Parrilla, J. A., "Valoracón algorítmica ante…", ob. cit., pág. 15.

ello ha de cumplir con el principio de interdicción de los poderes públicos, principio constructor del Estado de Derecho. La cuestión de la calidad de la ley en términos de garantías suficientes para evitar la arbitrariedad de los poderes públicos ha de guardar relación con la proporcionalidad de la injerencia en una sociedad democrática[68], según el art. 8.2 CEDH.

La exigencia de calidad de la ley está presente en la sentencia del Tribunal del Distrito de La Haya[69] que valora la puesta en marcha de SyRI, esto es, un mecanismo gubernamental que emplea IA. Brevemente, la sentencia reconoce de modo pionero que el uso de mecanismos de IA ha de ajustarse a reglas y limitaciones que sean respetuosas con los derechos de los sujetos y minimicen los riesgos para la protección de los mismos[70]. El mecanismo de IA analiza datos anonimizados proporcionados por las Administraciones públicas y elabora un informe de riesgo que aporta información sobre la probabilidad de que un sujeto cometa un fraude a la Seguridad Social, lo identifica y se inicia una investigación personalizada (párrafo 3.2). La herramienta realiza perfiles preventivos sobre la posible comisión de fraudes teniendo como base la información aportada. Por tanto, este procedimiento recogido en una ley (arts. 64 y 65 Ley SUWI y capítulo 5.a del Decreto SUWI) es un instrumento técnico previsto por el legislador para realizar una función de interés público que efectúa una injerencia en los derechos del sujeto, en concreto en la vida privada protegida por el art. 8 CEDH y debe contar por ello con previsión legal de calidad.

En estas cuestiones en las que se analiza la proporcionalidad de una intromisión en un derecho reconocido por la Carta, el TEDH prevé un margen de apreciación por parte de los Estados miembros que va en función de la naturaleza del derecho, de su importancia para el sujeto, de la naturaleza de la injerencia y del objetivo que persigue. Si el grado de consenso alcanzado entre las legislaciones nacionales sobre estas cuestiones es grande, el margen de apreciación de los Estados se reduce, mientras que, si no se logra un nivel de acuerdo, el margen de apreciación de los Estados aumenta. El margen de apreciación pretende asegurar un mínimo de protección a los derechos del Convenio garantizado por los Estados parte, en la medida en que se haya logrado una protección equivalente mientras que, a falta de dicha protección, o lo que es lo mismo, de una

---

[68] STEDH S y Marper & 77 y STEDH Graughan & 74 y ss. y Serrano Pérez, Mª M., "La STEDH de 13-12-2020…", ob. cit., pág. 3.

[69] Sentencia de la Corte del Distrito de La Haya, (ECLI:NL:RBDHA:2020:865).

[70] El mecanismo de IA que emplea datos de carácter personal denominado SyRI es un Sistema de Indicadores de Riesgo ideado por el Gobierno neerlandés para prevenir, descubrir y combatir el fraude a la seguridad social relacionado con la renta, las contribuciones fiscales la legislación laboral. A través del análisis de datos anonimizados la herramienta elabora informes de riesgo. El informe de riesgo aporta información sobre la probabilidad de defraudar a la seguridad social (párrafo 3.1). Con carácter previo a SyRI y a la ley que lo desarrolla ya se habían llevado a cabo técnicas para intentar descubrir el fraude a través de una estructura nacional pública de equipos de intervención.

legislación similar, la soberanía de los Estados dispone de un margen de maniobra más amplio para decidir acerca de la proporcionalidad de la injerencia.

La proporcionalidad de la medida, en el caso de una sociedad democrática y en un Estado de Derecho, añadimos nosotros, tiene que ver con la persecución del interés legítimo del Estado y en el supuesto de la sentencia sobre el mecanismo de IA la proporcionalidad de la medida es apreciada por el tribunal. Esto es, la norma que habilita la recogida masiva de datos y su tratamiento por las autoridades del Estado para prevenir el fraude es legítima, es decir, no vulnera ni el art. 8.2 CEDH ni el art. 64 Ley SUWI. También la lucha contra el fraude representa un beneficio para todos los ciudadanos y ha de ser una actividad propia del poder público, y puede, por tanto, realizarse a través de la IA. El tribunal entiende que el procesamiento de datos siguiendo el modelo de SyRI constituye una intromisión necesaria y legítima en una sociedad democrática justificada en aras del interés público perseguido, de modo similar a la decisión del caso S. y Marper. Si bien encuentra adecuada esta ponderación, la sentencia estima que las garantías contempladas en la ley no son suficientes para preservar los derechos de los sujetos en relación con la protección de datos, realizando el tribunal un contraste entre los principios del RGPD y la metodología SyRI de recogida de datos y su tratamiento.

Como generalidad podemos convenir que el equilibrio que debe buscar la ley entre los intereses públicos perseguidos y los intereses privados representados en el derecho fundamental que el Estado de Derecho ha de proteger debe rodearse de otros elementos, como el respeto a los valores y principios de la UE, sobre los que ya hemos hablado y que inciden los documentos europeos estudiados, y los valores constitucionales, así como la rendición de cuentas, esto es, el sometimiento de la actuación del poder público a la ley y la confianza necesaria creada por el cuerpo legislativo para garantizar la seguridad jurídica[71], tal y como refleja el *Libro Blanco sobre la inteligencia artificial*.

[71] Como reconoce la STC 135/2018, de 13 de diciembre, (ECLI:ES:TC:2018:135) (por todas) (FJ5) "…el término "seguridad" denota certeza, certidumbre, pero también confianza o previsibilidad. Si tales cualidades se proyectan sobre el ámbito de lo jurídico, podremos definir la seguridad jurídica como la certeza de la norma que hace previsibles los resultados de su aplicación. Sendos aspectos -certeza y previsibilidad- se encuentran íntimamente vinculados. Muestran las dos vertientes objetiva-subjetiva, definitorias de la seguridad jurídica, que aparecen reflejadas en la doctrina del Tribunal Constitucional, cuando afirma que la seguridad jurídica debe ser entendida desde un plano objetivo como la certeza sobre el ordenamiento jurídico aplicable y los intereses jurídicamente tutelados (STC 15/1986, de 31 de enero, FJ 1); pero además, desde una perspectiva subjetiva como la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en la aplicación del Derecho (STC 36/1991, de 14 de febrero, FJ 5). El primero de los aspectos se concreta en que el legislador debe perseguir la claridad y no la confusión normativa, debe procurar que acerca de la materia sobre la que se legisle sepan los operadores jurídicos y los ciudadanos a qué atenerse, y debe huir de provocar situaciones objetivamente confusas (STC 46/1990, de 15 de marzo, FJ 4). La previsibilidad del resultado aplicativo de la norma depende por tanto de la labor del legislador."

6. INTERRELACIÓN ENTRE INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES

Dentro de todos los posibles temas que están pendientes de reflexión en el Derecho constitucional, por los impactos que traerá consigo la IA, destaca el de los conflictos que se producen entre la IA y los derechos fundamentales. A este asunto dirigiremos los esfuerzos los constitucionalistas en los próximos tiempos por la inmediatez con la que se producirán las colisiones.

El uso de la IA puede mejorar la vida de los ciudadanos y de las sociedades, pero, como ya hemos apuntado, su implantación va acompañada de probables riesgos para el disfrute y ejercicio de los derechos fundamentales, en especial del derecho a la protección de los datos personales (art. 18.4 CE) y de la privacidad, del derecho a la intimidad (art. 18.1 CE), del derecho a la igualdad (art. 14 CE) por la relación existente entre la IA y el tratamiento de datos de carácter personal y la no discriminación por razón de sexo, raza, religión, opinión, discapacidad, edad, orientación sexual, etc. Aunque como veremos a lo largo del capítulo, la afectación puede alcanzar a cualquier derecho fundamental de los reconocidos en la Constitución.

Un mal uso de los procedimientos en los que se aplica la IA puede comprometer la libertad del ser humano y su vida privada en la terminología del CEDH. En todos los casos imaginables en los que la aplicación de técnicas de IA tenga como objeto principal intervenir en procesos sociales, o bien guarde relación con el individuo, puede quedar comprometido el disfrute de los derechos fundamentales, encontrándonos con resultados y decisiones que, sin la intervención del ser humano, son susceptibles de provocar desigualdades por cualquier circunstancia personal o social, vulneraciones del derecho a la protección de datos o lesiones en la intimidad del sujeto, por citar solamente algunos ejemplos más evidentes. Incluso tratándose de conjuntos de datos no personales, las conexiones que puedan establecerse entre los datos pueden tener consecuencias similares y provocar igualmente una lesión en los derechos de los ciudadanos, si dichas conexiones ofrecen un resultado que proporcione una información que, a la postre, pueda implicar algún tipo de discriminación.

El uso de la IA puede afectar a los valores sobre los que se fundamentan nuestras sociedades democráticas y de Derecho y a la propia esencia de la UE (art. 3 TUE), ya que, además de los derechos mencionados, el mal uso de la IA puede erosionar los pilares y valores de la Unión, que constituyen la base de la defensa del orden constitucional. El riesgo se extiende hacia otros derechos fundamentales, puesto que el empleo de procedimientos de IA puede provocar la vulneración de la libertad de expresión, la libertad de reunión, la dignidad humana, el derecho al trabajo, el derecho a la educación, el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores[72].

[72] Para ver el elenco de derechos fundamentales que pueden verse afectados por la inteligencia artificial ver el documento *Algorithms and Human Rights. Study on the human rights dimensions of*

Las eventuales amenazas para el ejercicio de estos derechos fundamentales pueden venir tanto por cuestiones formales y técnicas, esto es, el riesgo estaría en el diseño en origen de los sistemas de IA cuya supervisión ha de recaer siempre en el ser humano, o bien por cuestiones materiales o de fondo, esto es, como consecuencia del uso de datos, en caso de ignorar los principios de la protección de datos y tolerar su tratamiento de manera sesgada, sin una corrección humana, por ejemplo, si utilizamos datos de población urbana solamente frente a datos de población rural, en cuyo caso el resultado obtenido discriminará de forma automática a una parte de la población.

La IA como un fenómeno natural en nuestras sociedades sustituirá algunas de las funciones que hasta su llegada realizaba el ser humano. Por tanto, seremos objeto, cada vez con mayor frecuencia, de acciones realizadas gracias a la intervención de una máquina inteligente. Como decimos, esa nueva forma de actuación puede provocar decisiones cuyo control quedaría alejado del ser humano al que afectan. El riesgo potencial de agresión a los derechos de sujeto implica tanto a las autoridades públicas como a los poderes privados. El análisis de grandes volúmenes de datos y las conexiones y soluciones que ofrecerían pueden constituir un arma para que, incumpliendo las normas de protección de datos, se pueda ejercer una mayor vigilancia sobre el individuo tanto por parte del Estado como por parte de las empresas.

Por otro lado, la IA incorpora otra característica que incrementa sus posibles efectos adversos y es la capacidad de afectación a un elevado número de individuos, con nulo control por su parte. Por ello, las medidas desde el diseño para intentar evitar dicho riesgo o minimizarlo resultan esenciales. Reducir la opacidad, la complejidad, la imprevisibilidad y la autonomía que incorporan los procesos de IA a través de los cuales se adoptan determinadas decisiones que afectan a los derechos fundamentales ha de ser un objetivo a alcanzar por las normas, y aunque puede resultar difícil su comprobación, no por ello deja de ser la finalidad a conseguir.

Hay que tener en cuenta igualmente que las personas jurídicas y su actividad pueden verse dañadas por actuaciones propias de procesos de IA. Aunque la titularidad de los derechos fundamentales corresponde a la persona física (con alguna excepción), la protección constitucional contra los riesgos que puede suponer la IA debe alcanzar también a las personas jurídicas.

Hay otros temas apasionantes y pendientes de análisis con perspectiva constitucional, como el de la personalidad jurídica de las IIAA, planteándonos si pueden llegar a denominarse *right holders*. Además, está la cuestión de si la IA podrá tener derechos morales de autor. Sin duda el aspecto de la responsabilidad civil de los actos

---

automated data processing techniques and possible regulatory implications, del Consejo de Europa, DGI (2017) 12, disponible en https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

de los robots es muy relevante también. A estos temas se dedicarán otros capítulos de este texto.

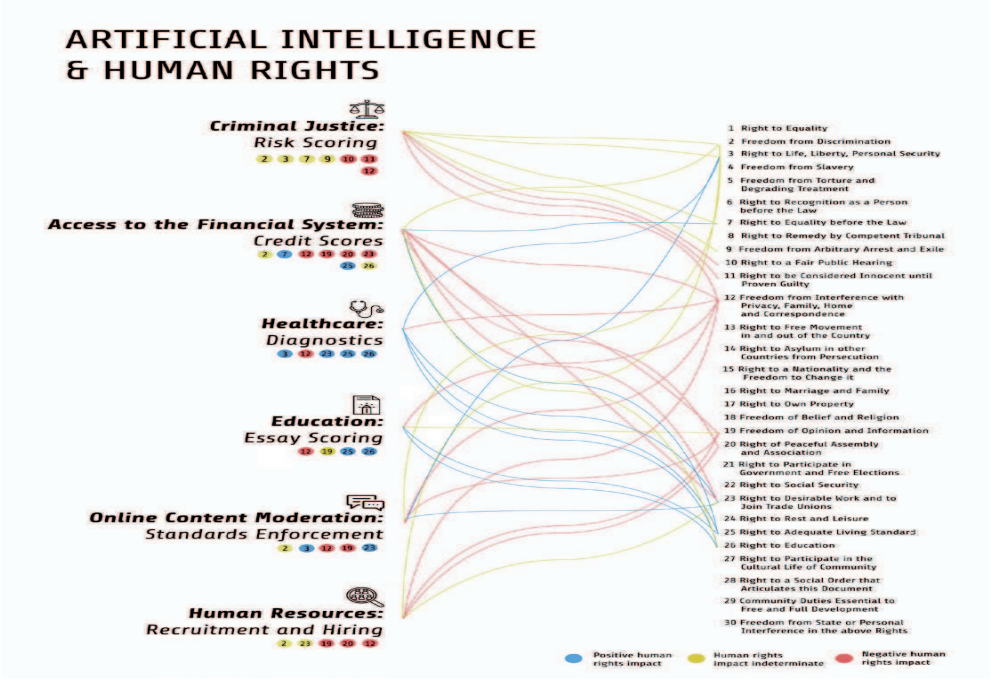
Los impactos de los sistemas que utilizan IA pueden estar relacionados con:

La calidad de los datos de entrenamiento: En la medida en que los datos utilizados para "entrenar" un sistema de IA están sesgados, el sistema resultante reflejará, o tal vez incluso exacerbará esos sesgos. Esto puede tener importantes impactos en varios derechos humanos.

Diseño del sistema: Las decisiones tomadas por los diseñadores humanos de un sistema de IA pueden tener importantes consecuencias para los derechos fundamentales. Los diseñadores humanos pueden, por ejemplo, dar prioridad a las variables que les gustaría que el sistema de IA optimizara y decidir qué variables debería tener en cuenta la IA en su funcionamiento. Esas decisiones de diseño pueden tener repercusiones tanto positivas como negativas en los derechos de las personas, que serán informadas por el individuo, las experiencias de vida y los prejuicios de los diseñadores.

Interacciones complejas: Una vez que se introduce un sistema de IA, interactuará con el medio ambiente de manera que se produzcan resultados que pueden no haberse previsto. Estas complejas interacciones pueden tener importantes repercusiones en los derechos humanos. Este no es un tema que sea único para la IA: las sociedades pre-digitales son asombrosamente complejas, y los impactos en los derechos fundamentales de las acciones de los individuos y las instituciones no son siempre conocidas en el momento en que se producen, sino durante algún tiempo después.

Un buen resumen de los impactos que el uso de la IA puede producir en los derechos humanos se muestra en el gráfico más abajo. Existen diferentes áreas en las que se utilizan sistemas de decisión de IA: en la Educación, por ejemplo, para evaluar al alumnado que pretende ingresar en una Universidad, se utilizan sistemas de decisión de IA. Si estos sistemas incluyen sesgos, porque utilizan datos que lo están, las decisiones pueden tener impacto en el derecho a la igualdad, o a educación, entre otros. Igualmente, un sistema de diagnóstico médico basado en IA puede tomar decisiones con impacto en el derecho a la salud o en la privacidad. Parecidas conclusiones pueden extraerse del uso de sistemas de IA en el ámbito financiero, o de los recursos humanos.



Raso, Hilligoss, Krishnamurthy, Bavitz, Kim (2018) Research Publication No. 2018-6. September 25, 2018. Artificial Intelligence & Human Rights: Opportunities & Risks. The Berkman Klein Center for Internet & Society Research Publication Series

Un asunto particularmente importante cuando analizamos los conflictos de la IA con los derechos de las personas es el enfoque basado en derechos humanos. Muchos autores[73] han aceptado su interés a la hora de evaluar y analizar los riesgos que se pueden producir ante una utilización masiva de sistemas de IA en nuestra vida diaria. Este enfoque se basa en los principios de derechos humanos, que sirven para orientar las decisiones que, en caso de colisión con los derechos, puedan producirse.

Estos principios son los siguientes:

- Universalidad e interdependencia de los derechos humanos
- Participación en la toma de decisiones

[73] Latonero, Mark (2018) 'Governing Artificial Intelligence: Upholding Human Rights & Dignity' *Data&Society*; Mark Hodge and Dunstan Allison-Hope, (2018) 'Artificial Intelligence: A Rights-Based Blueprint for Business,' Working Paper No 2, BSR; Filippo Raso et al, (2018) 'Artificial Intelligence & Human Rights: Opportunities & Risks' (Berkman Klein Center Research Publication No 2018-6); Petra Molnar and Lex Gill,(2018) Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System (University of Toronto).

- Transparencia y Rendición de cuentas
- No discriminación

Cualquier decisión que se tome con base en un sistema de IA debe garantizar estos principios, de forma que se garantice la transparencia y los afectados puedan conocer exactamente la manera y los criterios que se han seguido para llegar a determinada decisión. Además, esta debe garantizar que no discrimina o deja de lado a un grupo de personas.

Otro asunto que debemos tener claro es que las decisiones algorítmicas son a menudo implícitas e invisibles[74]. De esta forma, pueden tener impactos en los derechos que pasan completamente desapercibidos[75].

A continuación, examinamos muchos de los derechos humanos que sufren impactos de la IA.

Los impactos se producen de forma más intensa en las poblaciones vulnerables y marginadas. Un buen ejemplo de ello puede estudiarse en el libro de Virginia Eubanks[76]. Los más marginados de nuestra sociedad se enfrentan a niveles más altos de recopilación de datos cuando acceden a beneficios públicos, caminan por vecindarios fuertemente vigilados, entran en el sistema de salud o cruzan fronteras nacionales. Esos datos refuerzan su marginalidad cuando se usan para someterlos a un escrutinio extra. Es un ciclo de retroalimentación de la injusticia. Esto puede incluir a mujeres y niños, así como a ciertos grupos étnicos, raciales o religiosos, a los pobres, a los discapacitados y a los miembros de la comunidad LGBTQ. La marginación estos grupos se refleja en los datos y se reproduce en los resultados que afianzan los patrones históricos.

6.1. Derecho a la vida, a la libertad, seguridad, derecho a la tutela judicial efectiva

Concordancias normativas:

- Artículos 9, 15 y 24 de la Constitución Española CE.
- Art. 2, 6 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE).
- Art. 2 y 5 del Convenio Europeo de Derechos Humanos (CEDH).

---

[74] Buhmann, A., Paßmann, J, Fieseler, C. (2020) "Managing Algorithmic Accountability: Balancing Reputational Concerns, Engagement Strategies, and the Potential of Rational Discourse" *Journal of Business Ethics* 163:265–280 https://doi.org/10.1007/s10551-019-04226-4

[75] ACM Association for Computing Machinery US Public Policy Council (2017). *Statement on algorithmic transparency and accountability*. Retrieved December 1, 2017, https ://www.acm.org/binaries/conte nt/asset s/publi c-polic y/2017_usacm statement_algor ithms .pdf.

[76] Eubanks (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the poor*. Ed. St. Martins.

- Art. 3, 6, 7, 8, y 10 de la Declaración Universal de los Derechos Humanos (DUDH).
- Art. 9 y 14 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP).

El creciente uso de la IA en el sistema de justicia penal corre el riesgo de interferir con estos derechos. Dos ejemplos recientes se han resuelto de forma distinta en Holanda y EEUU.

El Tribunal de Distrito de La Haya en 2020 consideró que la legislación neerlandesa que amparaba el programa SyRI (*system risk indicator)* vulneraba el derecho a la vida privada y familiar consagrada por el artículo 8 del Convenio Europeo de Derechos Humanos porque no aseguraba una aplicación transparente y verificable del programa. En este caso fue especialmente relevante la intervención como amicus curiae del relator especial de las Naciones Unidas sobre la extrema pobreza, Philip Alston, que puso de manifiesto el uso predominante de SyRI en los barrios pobres de las grandes poblaciones holandesas, a pesar de que la abrumadora mayoría de los beneficiarios de ayudas sociales en Holanda no cometen fraude y, sin embargo, su derecho a la vida privada se ve afectado en una país que ha sido calificado por el Parlamento Europeo de paraíso fiscal.

En EEUU, el Tribunal Supremo estatal se pronunció en 2016 en el sentido de que los jueces podían apoyarse para su actividad sentenciadora, aunque con ciertas prevenciones, en los resultados de COMPAS *(Correctional Offender Management Profiling for Alternative Sanctions*). En este país se utiliza un software de calificación del riesgo de reincidencia para fundamentar las decisiones de detención en casi todas las etapas, desde la asignación de la fianza hasta la condena penal. El software ha ayudado a decidir que más acusados negros hayan sido falsamente etiquetados como de alto riesgo y con condiciones de fianza más altas, sean mantenidos en prisión preventiva y sean sentenciados a penas de prisión más largas. Además, como los sistemas de puntuación de riesgo no están prescritos por la ley y utilizan datos que pueden ser arbitrarios, las decisiones de detención informadas por estos sistemas pueden ser ilegales o arbitrarias[77].

Los programas informáticos de evaluación de riesgos penales se consideran una herramienta para ayudar simplemente a los jueces en sus decisiones de sentencia. Sin embargo, al calificar a un acusado de alto o bajo riesgo de reincidencia, le atribuyen un nivel de culpabilidad futura que puede interferir con la presunción de inocencia que se requiere en un juicio justo[78].

Los programas informáticos de predicción policial también corren el riesgo de imputar erróneamente la culpabilidad, incorporando los prejuicios policiales existen-

[77] Ordóñez Solís, David (2020). "Los jueces y las nuevas tecnologías bajo un prisma ético". *Diario LA LEY*, nº 9616, de 20 de abril de 2020, Nº 9616, 20 de abr. de 2020, Editorial Wolters Kluwer.

[78] Ulenaers, Jasper (2020) "The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?" *Asian Journal of Law and Economics*. Vol.11, issue 2. https://doi.org/10.1515/ajle-2020-0008.

tes mediante el uso de datos pasados. Los informes sugieren que los jueces saben muy poco sobre el funcionamiento de esos sistemas de calificación de riesgos, pero muchos dependen en gran medida de los resultados porque el software se considera imparcial.

La incapacidad de la IA para lidiar con los matices probablemente causará más problemas en el futuro. Las leyes no son absolutas; hay ciertos casos en los que se justifica el incumplimiento de la ley. Por ejemplo, probablemente sea aceptable saltarse un semáforo en rojo para evitar una colisión por detrás con un coche que va a la cola. Si bien un oficial de policía humano puede hacer esa distinción y optar por no multar al conductor, las cámaras de luz roja no son capaces de ese juicio. En un futuro de ciudades inteligentes existe el riesgo de que esta pérdida de matices provoque un aumento drástico de personas detenidas o multadas injustamente, con recursos limitados. Con el tiempo, estas circunstancias podrían empujarnos a un mundo en el que la gente prefiere seguir estrictamente cualquier ley o norma a pesar de las circunstancias atenuantes, perdiendo la capacidad de hacer los juicios necesarios.

Otro ámbito de la IA con importantes impactos en el derecho a la vida es el de las armas autónomas. Actualmente se están desarrollando en muchos países. El creciente uso de aviones teledirigidos y armamento similar significa que es probable que las armas autónomas sean accesibles para los agentes no estatales que no están obligados por las leyes tradicionales de los conflictos armados. Es probable que en un futuro próximo las armas autónomas sufran la incapacidad de la IA para hacer frente a los matices o a los imprevistos. En una situación de conflicto, esto podría dar lugar a la muerte o lesiones de civiles inocentes que un operador humano podría haber podido evitar.

En este sentido, es interesante que algunas organizaciones de derechos digitales hayan propuesto un listado de usos no permitidos de la IA[79]:

- la vigilancia biométrica indiscriminada y la captura y el procesamiento biométricos en espacios públicos
- el uso de la IA para determinar únicamente el acceso o la prestación de servicios públicos esenciales (como la seguridad social, la policía o el control de la inmigración)
- usos de la IA que pretenden identificar, analizar y evaluar las emociones, el estado de ánimo, el comportamiento y los rasgos de identidad sensibles (como la raza o la discapacidad) en la prestación de servicios esenciales
- la vigilancia policial predictiva
- armas letales autónomas y otros usos que identifican objetivos para la fuerza letal (como la aplicación de la ley y la inmigración)

[79] EDRi (European Digital Rights) (2020) Recommendations for a Fundamental Rights-based Artificial Intelligence Regulation. *Addressing collective harms, democratic oversight and impermissable use,* p.9. https://edri.org/our-work/can-the-eu-make-ai-trustworthy-no-but-they-can-make-it-just/

6.2. Derecho a la protección de datos de carácter personal

Concordancias normativas:

- Art. 18.4 CE
- Art. 8.1 y 8.2 CEDH
- Art 8 de la CDFUE
- Art. 16 TFUE
- Art. 12 de DUDH
- Art. 17 de PIDCP

El derecho a la protección de datos está reconocido en el art. 18.4 CE, derecho fundamental cuyo contenido esencial y objeto han sido precisados por el Tribunal Constitucional de acuerdo con los textos normativos internacionales sobre la materia[80]. La CDFUE recoge en su art. 8 el derecho a la protección de datos personales con un mayor acierto en su redacción, al incluir expresamente en el propio texto del precepto elementos principales del contenido esencial del derecho fundamental, como algunos de los principios del tratamiento de datos y de los derechos de que dispone el individuo para ejercitar el control sobre sus datos personales, verdadero objeto del derecho fundamental. En el apartado tercero el precepto hace referencia a la existencia de una autoridad de control independiente encargada de supervisar el cumplimento de las normas. El art. 16 TFUE reconoce en su apartado primero también el derecho fundamental a la protección de datos mientras que en el segundo atribuye la regulación de dicha materia al ámbito comunitario[81]. En el momento actual, el RGPD y la LOPDGDD constituyen la regulación vigente sobre la materia.

La IA constituye una herramienta que inserta y utiliza (al menos en una o más fases) un tratamiento de datos y realiza procesos de aprendizaje automático que concluyen con la toma de decisiones respecto a los sujetos cuyos datos se han manejado y que en ocasiones se trasladan a un tercero. Para llegar a la adopción de las decisiones, la IA ha de tratar un elevado volumen de datos, tanto personales como no personales.

---

[80] Sobre el derecho a la protección de datos de carácter personal existe una abundante bibliografía. Por citar aquí las más generales que abordan el tema de manera exhaustiva: Rebollo Delgado, L., Serrano Pérez, Mª M., *Manual de protección de datos*, 3ª ed., Dykinson, S. L., Madrid 2019; Arenas Ramiro, M., Ortega Giménez, A. (direct.), *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales* (en relación con el RGPD, Sepín 2019; VVAA, *Comentario a la Nueva Ley de Protección de Datos*, Dilex, 2020. *Comentario al Reglamento General de Proteccion de Datos y a la Ley Orgánica de Protección de Datos y garantia de los derechos digitales*, (dir.) Troncoso Reigada, A., Thomson Reuters, 2021.

[81] Serrano Pérez, Mª M., "Algunos aspectos del derecho fundamental a la protección de datos personales a la luz del Reglamento General de Protección de Datos de la UE: los principios de la protección de datos y los derechos de los sujetos", *Anuario 2018 Tribunal Constitucional. República Dominicana*, pág. 238.

La utilización de datos no personales (que pueden ser anonimizados) no aleja absolutamente el riesgo para las personas, pues a través de su empleo se pueden adoptar decisiones que provoquen sesgos[82], esto es, desviaciones inadecuadas en el mecanismo de inferencia que deriven en discriminaciones entre la población (aunque no en todos los casos, por ejemplo, si se trata de un modelo que predice fenómenos meteorológicos, o un sistema de control de calidad de productos industriales). Por otro lado, la probabilidad de volver a reidentificar a los sujetos, como hemos señalado en un momento anterior, obligaría a tener en cuenta el RGPD. Si el factor humano no corrige la conclusión arrojada por el sistema de IA, que ya constituye un sesgo, y lo acepta sin un juicio crítico por el hecho de proceder de una máquina, unimos al sesgo mecánico el error humano.

Vaya por delante que un sistema de IA que trata datos personales (por ejemplo, para elaborar perfiles sobre una persona física, o adopta decisiones sobre la misma) está sometido a los principios y criterios del RGPD, aunque el mecanismo de la IA presenta ciertas dificultades para la aplicación de algunos de los elementos normativos contenidos en la legislación europea y nacional. También es posible que en todo el proceso de IA encontremos etapas en las que no se emplean datos personales. Los principios y derechos del RGPD que se ven afectados por los procedimientos de IA son, entre otros, los principios de transparencia, de exactitud y el principio de minimización de los datos, el derecho de información, el ejercicio de los derechos, las decisiones automatizadas, las medidas desde el diseño y por defecto que deben incluir los instrumentos de IA y la evaluación de impacto.

Sobre la IA y la protección de datos la sentencia de la Corte de La Haya (párrafo 6.24) ha señalado que el derecho a la identidad personal y el derecho al desarrollo personal guardan relación con la vida privada y ambos con el derecho a la protección de datos personales, al igual que el respeto a la vida privada en conexión con el tratamiento de datos personales y puede afectar al derecho a la igualdad y al derecho a la protección contra la discriminación, los estereotipos y la estigmatización[83].

El art. 5.1 RGPD recoge los principios de licitud, lealtad y transparencia; principios de finalidad determinada, explicita y legítima; principios de adecuación, pertinencia y limitación de los datos a los necesarios para cumplir las finalidades; exactos y actualizados: principio de conservación de los datos al tiempo necesario para cumplir las

---

[82] 'systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others. A system discriminates unfairly if it denies an opportunity or a good or if it assigns an undesirable outcome to an individual or group of individuals on grounds that are unreasonable or inappropriate" (Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. ACM Transactions on Information Systems (TOIS), 14(3), 330-347).

[83] Hay que decir que, a juicio de la sentencia, la legislación reguladora de SyRI es respetuosa con el RGPD, en concreto el concepto de datos de carácter personal (art. 4.1 RGPD), así como los conceptos de tratamiento (art. 4.2 RGPD), responsable del tratamiento (art. 4.7 RGPD) y encargado del tratamiento (art. 4.8 RGPD).

finalidades que motivaron su recogida; principio de seguridad. El responsable del tratamiento ha de asegurarse que se cumplen todos los principios con una actitud proactiva.

La transparencia[84] es uno de los principios esenciales en un tratamiento de datos que incluya procesos de IA y va ligado al derecho a la información. El principio de transparencia demanda la existencia de una información accesible y legible, una comunicación clara de las características del tratamiento y en un lenguaje sencillo. El responsable del tratamiento ha de aportar a los interesados la información sobre su propia identidad y los fines del tratamiento. Independientemente, en virtud de este principio se debe proporcionar activamente más información para garantizar un procesamiento justo y transparente de los datos, con el fin de que los ciudadanos sean conscientes de los riesgos, las reglas, las garantías y los derechos asociados con el procesamiento de los datos personales. Disponiendo de toda la información sobre el tratamiento el sujeto podrá decidir si consiente la entrega de sus datos de carácter personal, en caso de ser el consentimiento la base jurídica sobre la que se sustenta el tratamiento.

Los arts. 13 y 14 RGPD establecen el conjunto de aspectos y elementos del tratamiento de los datos que han de ser objeto de información, en un caso si los datos se han recabado del propio sujeto y en el otro si no se han obtenido del propio interesado. Con carácter general hay que señalar que la información que se proporcione debe ser clara, en un lenguaje sencillo, transparente e inteligible, con el fin de cumplir la finalidad de trasladar al interesado las circunstancias que le van a permitir mantener el control sobre sus datos personales.

El precepto permite proporcionar la información por capas o niveles, partiendo de la información más general y básica hasta la más pormenorizada, en los niveles superiores de información. Dentro de la primera entrega de la información se incluye la relativa a la identidad del responsable del tratamiento, la finalidad, la posibilidad de ejercitar los derechos reconocidos en los arts. 15 a 22 RGPD y la posible elaboración de perfiles, información está ultima que se amplía en un segundo nivel informativo, junto con el detalle en el ejercicio de los derechos del sujeto.

Sobre la necesidad de informar se ha pronunciado la sentencia reiteradamente aludida señalando que el procedimiento de recogida de datos a los fines de detectar el riesgo de cometer un fraude a la Seguridad Social, que es el caso resuelto, a través de la elaboración de un perfil no contempla la obligación de informar al sujeto de la recogida de datos para tal fin ni de la posibilidad de ser objeto de un perfil con consecuencias directas sobre los individuos (párrafo 6.54). En relación con la obligación de informar, y teniendo en cuenta la ley reguladora del sistema de IA empleado

[84] Sobre la transparencia vid. las Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, del Grupo de Trabajo del art. 29, adoptadas el 29 de noviembre de 2017, WP 260 rev. 01, disponible en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

por el Gobierno neerlandés, el mismo tribunal determina la falta de transparencia en relación con el procedimiento, pues no se ha hecho pública la información sobre el modelo de riesgo a seguir en SyRI (párrafo 6.49), aunque de la información publicada resulta evidente que realiza un tratamiento de datos personales.

Sí se publica, por parte de la autoridad pública competente que será el responsable del tratamiento, el inicio de un proceso de investigación según los parámetros de SyRI y que los sujetos que así lo soliciten expresamente podrán tener acceso a los perfiles de riesgo (párrafo 6.54). La falta de información sobre cómo a partir de determinados datos se pueden concluir el incremento del riesgo (párrafo 6.87), o sobre el modelo algorítmico empleado por el instrumento de IA, lo que deriva en el desconocimiento del proceso seguido para la elaboración de un perfil de riesgo o de cómo se tratan los datos de las personas sobre las que el perfil de riesgo es negativo, constituyen vulneraciones del principio de transparencia y por tanto deberán ser tenidas en cuenta cuando se adopte un mecanismo de IA para respetar dicho principio. El hecho de que los datos se conserven como mínimo cuatro semanas y después esté prevista su destrucción, resulta acorde con el principio de conservación del art. 5.1 e) RGPD (párrafo 6.90), pero no salva la falta de transparencia del procedimiento. La ausencia de transparencia legal sobre las cuestiones señaladas, pese al argumento del Gobierno de la necesidad de su opacidad para poder obtener de forma masiva los datos, incurre en falta de seguridad jurídica al impedir con su ocultamiento la previsibilidad en la aplicación del Derecho y la planificación del comportamiento del ciudadano de forma que no pueda ser objeto de investigación por parte de la autoridad pública.

Resulta significativo que el Gobierno defienda la falta consciente de transparencia y de información en cuanto al modelo de riesgo y a los indicadores del mismo para evitar que los ciudadanos puedan ajustar su comportamiento, lo que lesiona precisamente el principio de seguridad jurídica y el principio de publicidad de las normas, sin que la justificación de perseguir con ello un interés general pueda, a nuestro juicio, legitimar la opacidad en el actuar de un poder público en un Estado de Derecho. Por otra parte, la falta de información y transparencia sobre la elaboración de un perfil de riesgo y la inclusión de dicho perfil en el Registro dificulta el objeto del derecho a la protección de datos de controlar las informaciones nuestras en manos de un tercero.

Este control de las informaciones personales aparece concebido de modo rebajado bajo la expresión de facilitar "un seguimiento razonable de sus datos y a ser informado del tratamiento de sus datos" (párrafo 6.59). A nuestro juicio el matiz es importante, porque del contenido claro y rotundo del derecho a la protección de datos de controlar las informaciones en manos de un tercero, el tribunal pasa a valorar un seguimiento razonable, quizá consciente de las dificultades que entrañan los procesos de IA de realizar un control y dominio de las informaciones personales que tratan, pero también dejando a salvo un contenido mínimo del derecho fundamental, que

quedaría irreconocible en sus pretensiones como tal derecho fundamental si lo redujéramos a la nada y lo vaciáramos de contenido, esto es, si justificáramos la pérdida de control sobre los datos personales debido a la complejidad de la IA. El seguimiento razonable de los datos debe incorporar un mínimo de garantías para poder continuar ejerciendo un control sobre las informaciones personales en cualquier tipo de tratamiento de datos. Precisamente en el caso analizado, la falta de garantías para preservar los derechos del sujeto junto con la falta de transparencia no resulta proporcional de acuerdo con la redacción del art. 8.2 CEDH. La falta de garantías constituye un argumento recurrente en el TEDH para considerar desproporcionada e injustificada una injerencia en la vida privada de los individuos (art. 8.2 CEDH) en relación con la protección de datos. Y en este sentido el RGPD contiene las garantías necesarias para poder proteger los derechos del sujeto.

Por lo que atañe al principio de limitación del tratamiento y el principio de minimización el principio de limitación del tratamiento hay que conectarlo con la finalidad, pues los datos han de limitarse a los necesarios para cumplir con la finalidad que ha de ser determinada, explicita y legítima y de la que se ha informado al sujeto. Respecto de la minimización de datos, esto es, la limitación a los que van a servir para cumplir la finalidad de sistema de riesgo volvemos a recuperar la sentencia de la Corte de La Haya. El procedimiento SyRI relaciona todos los archivos y grandes cantidades de datos de las autoridades (municipales, tributarias, de extranjería) de forma estructurada con el fin de identificar los posibles abusos en diferentes sectores (correspondientes con las autoridades públicas que aportan los datos) y poder identificar al sujeto (párrafo 2.3). El conjunto de datos o categorías de datos es muy amplio, como queda reflejado en la sentencia[85], aunque hemos de convenir que precisamente los procesos algorítmicos necesitan trabajar con una gran cantidad de datos para poder extraer conclusiones[86]. Aceptando la matización del principio de minimización de los datos cuando se precise un gran volumen de ellos y se persiga un objetivo de interés general contemplado en una ley, habrá que extremar todas las cautelas en lo que se refiere a las garantías para que los derechos de los sujetos cuyos datos se tratan no queden desprotegidos. Así pues, se deberá reforzar el derecho de información y la posibilidad de ejercitar los derechos por parte de los ciudadanos.

---

[85] Así pues la LUWI permite recoger datos de empleo, sobre medidas y sanciones administrativas, datos fiscales, datos sobre bienes muebles e inmuebles, datos que justifiquen la exclusión de la asistencia o prestaciones sociales, datos comerciales, datos de alojamiento, datos identificativos de las personas físicas como nombre, dirección, lugar de residencia, dirección postal, fecha de nacimiento, sexo y características administrativas y para una persona jurídica: nombre, dirección, dirección postal, forma jurídica, lugar de actividad y características administrativas, datos de integración, datos de cumplimiento de las leyes, datos educativos, datos de pensiones, datos de reintegración de obligaciones a una persona y si se están cumpliendo, datos sobre deudas de una persona, datos de prestaciones y subvenciones, permisos y exenciones, datos de seguro médico (párrafo 4.17).

[86] Lazcoz, G., y Castillo Parrilla, J. A., "Valoración algorítmica ante…", ob. cit., pág. 218.

Junto a ello y para conseguir el cumplimiento del principio de minimización se propone limitar la extensión de las categorías de datos utilizadas en cada fase del tratamiento a las que sean estrictamente necesarias, limitar el grado de detalle o precisión de la información, limitar la extensión del número de afectados y limitar la accesibilidad a las categorías de datos al personal del responsable o encargado[87]. En cada fase del tratamiento es posible que no sea necesario acceder a todos los datos disponibles, sino solo a los necesarios, por lo que es aconsejable establecer diferentes estrategias de minimización de datos.

En lo que respecta a la elaboración de perfiles[88], el art. 22 RGPD establece las directrices a seguir en relación con la elaboración de perfiles y una prohibición sobre la toma de decisiones individuales automatizadas basadas exclusivamente en la elaboración de perfiles, cuyas consecuencias para el interesado pueden generar perjuicios importantes.

Por otro lado, el art. 13.2 f) RGPD contempla la obligación del responsable de informar "la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartado 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado". La existencia de decisiones automatizadas obliga a informar al sujeto de forma significativa sobre la lógica empleada y las consecuencias de dicho tratamiento. Sobre la información significativa, solamente puede entenderse en el sentido de aportar información suficiente y clara que facilite la comprensión por parte del sujeto, indicación que nos devuelve a la transparencia, lo que excluiría un relato técnico del procedimiento y si una explicación que permita al interesado conocer el estado de sus datos y el empleo que se les da[89]. Lo primero que es necesario recordar a efectos de un tratamiento de datos que elabora perfiles es

---

87 Adecuación al RGPD de tratamientos…, ob. cit., pág. 39.

88 El art. 4.4 RGPD define la elaboración de perfiles "como cualquier forma de procesamiento automatizado de datos personales en el que ciertos aspectos personales de una persona física se evalúan sobre la base de datos personales, en particular con la intención de su desempeño profesional, situación económica, salud, preferencias personales e intereses. analizar o predecir, confiabilidad, comportamiento, ubicación o movimientos".

89 Relata la información que puede ser pertinente para que el sujeto comprenda la cuestión. El documento menciona: "El detalle de los datos empleados para la toma de decisión, más allá de la categoría, y en particular información sobre los plazos de uso de los datos (su antigüedad); La importancia relativa que cada uno de ellos tiene en la toma de decisión; La calidad de los datos de entrenamiento y el tipo de patrones utilizados; Los perfilados realizados y sus implicaciones; Valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia; La existencia o no de supervisión humana cualificada; La referencia a auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada; En el caso de que el sistema IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo", Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una interpretación, AEPD, febrero 2020, pág. 24.

la obligación de realizar una EIPD (art. 35.3 a) RGPD con el fin de verificar los riesgos que dicho tratamiento entraña para los derechos del sujeto.

El ejercicio de los derechos ejercido ante procesos de IA se somete a las reglas generales, aunque habrá que velar de forma especial cuando el ejercicio de cualquiera de ellos se ejercite como consecuencia de la elaboración de perfiles[90].

En conclusión, aunque algunos de los principios contemplados en el RGPD han de ser matizados en relación con los procesos que emplean IA y tratan datos de carácter personal, el contenido esencial del derecho a la protección de datos no puede eliminarse, esto es, el sujeto tendrá siempre que poder mantener un control sobre sus informaciones personales, a riesgo de no quedar vacío de contenido el derecho fundamental. Habrá que extremar las garantías que permiten al individuo ejercer dicho control y mantener un equlibirio entre el derecho fundamental y la necesidad de emplear los datos para la satisfacción de un bien colectivo, esto es, de forma propocionada y justificada.

6.3. Derecho a la libertad de movimiento

Concordancias normativas:

- Art. 17 CE
- Art. 6 CDFUE
- Art. 5 CEDH
- Art. 12 del PIDCP

La posibilidad de que la IA restrinja la libertad de movimiento está directamente relacionada con su uso para la vigilancia. En los sistemas que combinan datos de imágenes satelitales, cámaras alimentadas por reconocimiento facial e información de localización de teléfonos móviles, entre otras cosas, la IA puede proporcionar una imagen detallada de los movimientos de los individuos, así como predecir su futura localización. Por lo tanto, los gobiernos podrían utilizarla fácilmente para facilitar una restricción más precisa de la libertad de movimiento, tanto a nivel individual como de grupo.

Actualmente, la falta de cartografía formal en muchas comunidades pobres y desatendidas en todo el mundo ha llevado a su exclusión de las aplicaciones de cartografía del GPS. Dada la tendencia creciente del uso de IA por parte de la policía con fines predictivos, es posible que el aumento de la cartografía de esas zonas y la combinación del uso de esa información con los datos de los programas de aplicación de la ley, como los que califican los niveles de delincuencia y seguridad de los vecindarios, puedan cerrar efectivamente el turismo o inhibir el movimiento en torno a una zona

[90] Adecuación al RGPD de tratamientos…, ob. cit., págs. 25 y ss.

o dentro de ella. Incluso si esto se hace por razones legítimas de seguridad pública, se puede correr el riesgo de violar la libertad de movimiento.

La IA se puede utilizar para automatizar las decisiones sobre quién puede viajar -por ejemplo, colocando a las personas en una lista de "No volar" u otras listas de prohibiciones-. En este caso, los errores podrían dar lugar a que se restringiera injustamente la libertad de movimiento de las personas.

6.4. Derechos a la libertad de expresión, pensamiento, religión, reunión y asociación

Concordancias normativas:

- Art. 16, 20, 21, 22 CE
- Art. 10 y 11 CDFUE
- Art. 9 y 10 CEDH
- Art. 19 DUDH; art. 19 PIDCP; art. 18 PIDCP y DUDH; Art. 21 y 22 PIDCP; art. 20 DUDH

La Inteligencia artificial está modificando la forma en la que hemos comprendido el contenido de la libertad de expresión. Como explica Ballesteros[91] "en las redes sociales domina una forma antipolítica de expresión, la emoción, que va unida a la aceleración. A mayor aceleración más dominio de la emoción. La emoción es dinámica y situacional, frente a la racionalidad que es estable y lenta. Los algoritmos dan primacía a aquello que estadísticamente logra una mayor adicción. La tecnología digital es antipolítica porque multiplica todo lo irracional y devalúa la libertad de expresión convertida en multiplicación gratuita para algunos o en simple *libertad* de la emoción para otros".

Por otro lado, todos los actores acaban influyendo en la libertad de expresión a través de la vigilancia de contenidos: Las empresas de Internet utilizan la IA para detectar los mensajes que violen sus condiciones de servicio, y los gobiernos ejercen presión sobre las empresas para que aborden el problema del presunto contenido terrorista, los discursos de incitación al odio y las denominadas "noticias falsas". Esto ha dado lugar a una mayor utilización de sistemas automatizados. Muchas veces, con la consecuencia de que gran parte de los contenidos se eliminan, vulnerando la libertad de expresión.

El papel de la IA en la clasificación de contenidos y la creación y el refuerzo de los filtros burbuja supone una amenaza indirecta a la libertad de pensamiento porque

[91] González Ballesteros, Teodoro (2019). "Libertad ideológica y libertad de expresión". *Cuadernos de periodistas: revista de la Asociación de la Prensa de Madrid*, ISSN 1889-2922, Nº. 39 págs. 130-136.

determina el tipo de información a la que la gente tiene acceso. Aunque las personas suelen tener la posibilidad de acceder a otras fuentes de información o buscar opiniones diferentes, el tiempo y la atención limitados de los seres humanos hacen que la mayoría no lo haga. Y en los países que carecen de una prensa libre y sólida y cuentan con un acceso limitado a Internet, las plataformas de medios sociales como Facebook suelen ser la única fuente de información no regulada. La utilización de algoritmos puede conducir a la fragmentación de la esfera pública y a la creación de "cámaras de eco" que favorezcan sólo a determinados tipos de medios de comunicación, aumentando así los niveles de polarización de la sociedad, lo que puede poner en grave peligro la cohesión social. Un algoritmo de búsqueda también puede estar sesgado hacia determinados tipos de contenido o proveedores de contenido, con lo que se corre el riesgo de afectar a valores conexos como el pluralismo y la diversidad de los medios de comunicación. Este es el caso, en particular, en el contexto de los motores de búsqueda en línea dominantes[92]. Las predicciones algorítmicas de las preferencias de los usuarios desplegadas por las plataformas de redes sociales no sólo orientan los anuncios que pueden ver los individuos, sino que también personalizan los resultados de la búsqueda y dictan la forma en que se organizan los alimentos de los medios sociales, incluidas las noticias.

Una amenaza directa que se cierne sobre la libertad de expresión es el acoso en línea por medio de bots. Estas cuentas de bots se hacen pasar por usuarios reales y envían respuestas automatizadas a cuentas identificadas o a cualquiera que comparta una determinada opinión.

Mientras que los efectos positivos de los algoritmos de búsqueda y los motores de búsqueda para la sociedad se han resaltado mucho, no tanto todos estos impactos negativos[93]. Según el artículo 10 del Convenio Europeo de Derechos Humanos, toda medida que bloquee el acceso a los contenidos mediante el filtrado o la eliminación de los mismos debe estar prescrita por la ley, perseguir uno de los objetivos legítimos previstos en el párrafo 2 del artículo 10 y ser necesaria en una sociedad democrática. De conformidad con la jurisprudencia del Tribunal Europeo de Derechos Humanos, toda restricción de la libertad de expresión debe corresponder a una "necesidad social apremiante" y ser proporcional a los objetivos legítimos que se persiguen.

Sin embargo, la eliminación de contenidos en las plataformas de los medios de comunicación social suele realizarse mediante procesos semiautomáticos o automatizados. Los algoritmos se utilizan ampliamente para los procesos de filtrado y eli-

[92] Pasquale, Frank A. (2016). *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*. Rochester, NY: Social Science Research Network. Retrieved 7 June 2017 (https://papers.ssrn.com/abstract=2779270).

[93] Consejo de Europa (2017) Algorithms and human rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES (MSI-NET).

minación de contenidos[94] lo que repercute directamente en la libertad de expresión y plantea problemas en el Estado de derecho (cuestiones de legalidad, legitimidad y proporcionalidad).

6.5. Derechos a la igualdad y no discriminación

Concordancias normativas:

- Art. 14 de la CE.
- Art. 20, 21 CDFUE
- Art. 14 CEDH
- Art. 3, 26, 27 PIDCP

La discriminación es el trato desigual que se le da a una persona o colectividad por motivos raciales, religiosos, políticos, de sexo, de edad, debcondición física o mental, etc. El derecho a la no discriminación está profundamente establecido en el marco normativo en el que se basa la Unión Europea. Se localiza, como hemos visto, en el Artículo 21 de la Carta de los Derechos Fundamentales de la Unión Europea, en el Artículo 14 del Convenio Europeo de Derechos Humanos, y en los Artículos 18-25 del Tratado de Funcionamiento de la Unión Europea.

La literatura que ha estudiado las predicciones algorítmicas ha destacado el riesgo de discriminación[95]. Del mismo modo que a unos sujetos se les ofrece una publicidad distinta de la que reciben otros, podríamos llegar a un tratamiento distinto de unos ciudadanos frente a otros en función de los resultados de un algoritmo.

Por tanto, uno de los mayores inconvenientes del uso de algoritmos es la existencia de sesgos. Un sesgo es un prejuicio a favor o en contra de algo o alguien, que puede dar lugar a decisiones injustas. Se sabe que los humanos son parciales en su toma de decisiones. Dado que los sistemas de IA son diseñados por humanos, es posible que los humanos inyecten su sesgo en ellos, incluso de forma no intencionada. Muchos de los sistemas actuales de IA se basan en técnicas de aprendizaje automático basadas en datos. Por lo tanto, una forma predominante de inyectar sesgo puede ser en la recolección y selección de datos de entrenamiento. Si los datos de capacitación no son lo suficientemente inclusivos y equilibrados, el sistema podría aprender a tomar decisiones injustas. Pero al mismo tiempo, la IA puede ayudar a los humanos a identificar sus sesgos, y ayudarlos a tomar decisiones menos sesgadas.

---

[94] Urban, J., Karaganis, J., & Schofield, B. (2016, July 15). Notice and Takedown in Everyday Practice. https://doi.org/10.31235/osf.io/59m86.

[95] O`Neil (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*.

Los modelos de IA están diseñados para clasificar y filtrar, ya sea clasificando los resultados de la búsqueda o categorizando a las personas. Esta discriminación puede interferir con los derechos fundamentales cuando trata a diferentes grupos de personas de manera diferente. A veces esa discriminación tiene objetivos sociales positivos, por ejemplo, cuando se utiliza en programas para promover la diversidad. En la justicia penal, esta discriminación suele ser el resultado de formas de prejuicio.

En 2015, los investigadores de Carnegie Mellon encontraron que Google mostraba muchos menos anuncios de trabajos ejecutivos altamente remunerados a mujeres[96]. Los algoritmos de anuncios personalizados de Google son impulsados por la IA, y se les enseña a aprender del comportamiento del usuario. Cuanta más gente haga clic, busque y use Internet de manera racista o sexista, el algoritmo lo traducirá en anuncios. Esto se agrava por las preferencias discriminatorias de los anunciantes, y se convierte en parte de un ciclo. «La forma en que la gente percibe las cosas afecta a los resultados de la búsqueda, que afectan a la forma en que la gente percibe las cosas.»

Hay tres preocupaciones fundamentales en lo que respecta a la no discriminación. En primer lugar, tiende a haber una falta de escrutinio previo, de supervisión democrática y de debate público sobre estas cuestiones. Así pues, hubo muy poco debate parlamentario sobre la introducción de SyRI en los Países Bajos en 2006, a pesar de las advertencias de la autoridad de protección de datos y otros partidos. Además, las solicitudes de libertad de información suelen verse frustradas debido a las amplias excepciones o a la propia falta de comprensión de las autoridades de la tecnología utilizada. Por consiguiente, el impacto desigual de esos sistemas en los pobres y marginados suele pasar desapercibido. En segundo lugar, la inteligencia artificial tiende a percibirse como necesariamente más justa y precisa que la humana. Sin embargo, si bien esto puede ser cierto en el caso de tareas muy específicas, es mucho menos seguro cuando hay que tener en cuenta un contexto más amplio. Cuando la tecnología permite una ampliación masiva de los procesos pero al mismo tiempo conduce a errores a gran escala, los que menos pueden desafiar al sistema (por ejemplo, los pobres o los ancianos, los migrantes, las personas con discapacidad) se verán nuevamente afectados de manera desproporcionada. Esto es especialmente grave cuando la IA se utiliza en el contexto del Estado de bienestar. Por último, las tecnologías digitales suelen estar deliberadamente dirigidas a las personas pobres y marginadas, lo que amplía las posibilidades de una vigilancia estatal constante de esas personas.

Existen pocos asuntos en los tribunales sobre este tema. Reiteramos el citado más arriba del tribunal de distrito de La Haya *(Rechtbank Den Haag*), que ha dictado una sentencia, de fecha 5 de febrero de 2020, por la que establece que un sistema algorítmico utilizado por el Gobierno de los Países Bajos para evaluar el riesgo de fraude a la seguridad social o a hacienda, no cumple las exigencias de proporcionalidad y

[96] Kusner, M & Loftus, J. (2020). "The long road to fairer algorithms". *Nature*. Vol. 578, p. 35.

transparencia necesarias y vulnera las previsiones sobre respeto a la vida privada que reconoce el artículo 8 del Convenio Europeo de Derechos Humanos, por lo que es contrario a la ley.

6.6. Derechos a la participación política y a la autodeterminación

Concordancias normativas:

- Art. 23 CE
- Art. 39 y 40 CDFUE
- Art. 16 CEDH
- Art. 21 DUDH; art. 25 PIDCP

El papel de la IA en la creación y difusión de la desinformación pone en tela de juicio la noción de elecciones justas y crea una amenaza al derecho a la participación política y a la autodeterminación. Las elecciones presidenciales de EE.UU. de 2016 mostraron cómo una potencia extranjera puede aprovechar los bots y los algoritmos de los medios sociales para aumentar el alcance de la información falsa e influir potencialmente en los votantes. Aunque las plataformas están trabajando para prevenir este tipo de actividad, el futuro de los robots y las falsificaciones profundas potenciadas por la IA probablemente hará que estos contenidos sean más convincentes para los votantes y más difíciles de detectar para las empresas. Esto puede enfriar la participación política, en particular si los votantes pierden la confianza en la legitimidad de las elecciones.

La vigilancia impulsada por la IA podría utilizarse para restringir e inhibir la participación política, entre otras cosas, identificando y disuadiendo a determinados grupos de personas de votar. El uso del reconocimiento facial en los colegios electorales o en las cabinas de votación podría comprometer el secreto de la votación. Los gobiernos que deseen disuadir a los votantes de emitir votos para la oposición no necesitan ni siquiera vigilar directamente el acto de la votación; la mera significación de la vigilancia podría ser suficiente para convencer a los votantes de que sus votos no son secretos y podría influir en sus decisiones de voto en consecuencia.

6.7. Derechos al trabajo y a unos medios de vida adecuados

Concordancias normativas:

- Legislación española: art. 35 CE
- Art. 15, 27-34 CDFUE
- Art. 4 CEDH
- Art. 23 y 25 DUDH; Art. 6, 7, 11 ICESCR

El papel de la IA en la automatización de los trabajos podría suponer una verdadera amenaza para el derecho al trabajo; en primer lugar, porque deja fuera del mercado laboral a una gran parte de la población sin conocimientos digitales. La automatización ha dado lugar a la pérdida de empleos en ciertos sectores, y se prevé que la IA acelere esta tendencia. Aunque existe un desacuerdo importante en cuanto a la medida en que se logrará la automatización de los puestos de trabajo, no hay duda de que la IA dará lugar a algunos cambios en el mercado laboral, tanto por la creación como por la destrucción de puestos de trabajo.

Si la automatización cambia el mercado laboral de manera significativa, y un gran número de personas no pueden encontrar trabajo, tendrán que luchar para mantenerse a sí mismos y a sus familias. Los investigadores están explorando formas de asegurar que las personas puedan mantener un nivel de vida adecuado con la volatilidad del mercado laboral. Un enfoque es un ingreso básico universal, un ingreso fijo que los gobiernos proveen.

En relación a esta función de asegurar el nivel de vida adecuado a sus habitantes, algunos gobiernos, como el de EEUU, utilizan sistemas de decisión algorítmica que están ocasionando discriminación[97], tal y como se ha mencionado más arriba.

Otro ámbito en el que la IA influye en el derecho al trabajo es el ámbito de la vigilancia de los trabajadores, que se ha reforzado con los algoritmos de supervisión. Así mismo, la IA está siendo cada vez más utilizada en los procesos de selección, lo que origina la aparición de sesgos.

6.8. Derecho a la salud

Concordancias normativas:

- Art. 43 CE
- Art. 35 CDFUE
- Art. 12 PIDESC

La IA ha acompañado al Internet de las cosas en Medicina en el contexto del diagnóstico médico, utilizando tomografías computarizadas para diagnosticar enfermedades. Tanto la IA como el Big Data han tenido impactos en logística, para localizar y distribuir los suministros médicos en el país, así como para hacer seguimiento de la producción y la demanda. La IA ha proporcionado recomendaciones de tratamiento más individualizadas a los pacientes, o ha hecho más accesible el asesoramiento médico especializado.

[97] Eubanks, *op.cit.*

Sin embargo, también hay formas en las que la IA podría poner en peligro el derecho a la salud. Una de ellas es la posibilidad de que los sistemas alimentados por la IA den lugar a la discriminación o se programen de manera que los resultados (como la reducción de costos) prevalezcan sobre el bienestar del paciente.

Por ejemplo, un sistema de IA podría diseñarse para recomendar diferentes tratamientos en función de la situación del seguro del paciente o de cuánto pueda pagar, lo que podría negar la atención vital a alguien debido a su situación socioeconómica, perjudicando a los grupos marginados que ya padecen un acceso insuficiente a la atención sanitaria de calidad. Otro posible problema son los bucles de retroalimentación negativa que podrían resultar de una excesiva dependencia de la orientación de un sistema de IA. Por ejemplo, si los médicos tienden a retirar la atención a los pacientes con determinados diagnósticos, como el nacimiento extremadamente prematuro o las lesiones cerebrales graves, un sistema basado en la medicina tradicional puede enterarse de que esos diagnósticos son casi siempre fatales y recomendar al médico que no los trate, aunque en algunos casos el tratamiento pueda ser eficaz.

Y por supuesto, está el impacto de los inevitables índices de error de cualquier sistema. Incluso si, por ejemplo, el "Watson" de IBM es más preciso que los médicos humanos a la hora de diagnosticar enfermedades, aún así se equivocará en el diagnóstico en ocasiones, o recomendará el tratamiento equivocado. Aquí surge el problema de la responsabilidad, que excede el ámbito de este trabajo. Pero sin duda es un reto de los más urgentes que debe resolver el Derecho en relación al avance de la IA.

6.9. Derecho a la educación

Concordancias normativas:

- Art. 27 CE
- Art. 14 CDFUE
- Art. 2 CEDH
- Art. 25 DUDH; art. 13 y 14 ICESCR

La IA puede vulnerar el principio de igualdad de acceso. Las universidades de los EE.UU. llevan años utilizando sistemas algorítmicos deterministas para recomendar a los solicitantes que deben admitir[98]. Estos sistemas suelen estar hechos a medida para satisfacer las preferencias de la escuela y tienen una serie de problemas que pueden dar lugar a la discriminación, entre ellos el uso de datos históricos de los estudiantes admitidos anteriormente para informar el modelo. Dado que muchas universidades de élite han estado históricamente llenas de hombres blancos adinerados, cualquier modelo que utilice estos datos corre el riesgo de tener el mismo sesgo. Si la

[98] O´Neil, *op.cit*.

IA se utiliza para rastrear y predecir el rendimiento de los estudiantes de tal manera que limite la elegibilidad para estudiar ciertas materias o tener acceso a ciertas oportunidades educativas, se pondrá en riesgo el derecho a la educación.

Dado el aumento de las investigaciones sobre predictores de éxito en la primera infancia, es probable que ese sistema pueda utilizarse para restringir las oportunidades de los estudiantes a edades cada vez más tempranas, lo que daría lugar a una importante discriminación, ya que a los estudiantes procedentes de entornos desfavorecidos se les negarían en última instancia las oportunidades porque las personas de esos entornos tienden a tener resultados más negativos. Ese sistema ignoraría a los estudiantes que superan la adversidad para lograr el éxito académico y profesional, y afianzaría las desigualdades educativas existentes.

6.10. Derecho a tomar parte en la vida cultural y a disfrutar de los beneficios del progreso científico

Concordancias normativas:

- Art. 44 CE
- Art. 27 DUDH; art. 15 ICESCR

Si los gobiernos utilizasen IA para identificar y reprimir a ciertos grupos culturales, se podría impedir que algunas personas participasen en la vida cultural, ya sea directa o indirectamente (por ejemplo, mediante una vigilancia que inspire temor a ser identificado o a sufrir represalias por la identidad cultural, lo que llevaría a las personas a evitar por completo las expresiones culturales). Existe el riesgo de que la IA se utilice para "criminalizar" ciertas culturas. Cuando los miembros de una cultura determinada son detenidos de manera desproporcionada o son objeto de otras medidas de represión, los comportamientos y costumbres asociados a esas culturas podrían vincularse a actividades delictivas. Por ejemplo, un sistema de ML que analizara imágenes de vídeo o fotográficas podría aprender a asociar ciertos tipos de vestimenta, formas de hablar o gestos con la actividad delictiva, y podría utilizarse para justificar la selección de estos grupos como objetivo bajo el pretexto de la prevención del delito.

Muchos en el mundo en desarrollo se preocupan de que se les "deje atrás" en la carrera mundial de la IA y el correspondiente cambio económico transformador. Sus habitantes se convertirán en consumidores pasivos de los sistemas de IA desarrollados en China u Occidente para diferentes personas, culturas y situaciones. La IA desarrollada en el extranjero corre el riesgo de profundizar la desigualdad y la división social existentes en los lugares donde el acceso a Internet y la tecnología se limitan en gran medida a los ricos y a las zonas urbanas. Este riesgo de una desigualdad más

profunda se ve agravado por el riesgo de que la automatización de los puestos de trabajo provoque la pérdida de puestos de trabajo al desplazar el papel de la industria manufacturera en el desarrollo económico.

En relación con estos derechos también cabe mencionar el derecho a la propiedad intelectual, y los posibles riesgos que pueden producirse si la IA llegase a crear nuevos "productos de la inteligencia". Habría que decidir qué sistema utilizar: el del copyright, que se origina por la sola creación; el de las patentes; el secreto industrial, entre otros sistemas[99].

6.11. Derecho al matrimonio, derechos de los niños, derechos de la familia

Concordancias normativas:

- Art. 32 CE
- Art. 9 CDFUE
- Art. 5 CEDH
- Art. 16 DUDH; Art. 23 y 24 PIDCP; art. 10 ICESCR

Si se utiliza la tecnología de la IA para el examen médico y reproductivo, y se descubre que es poco probable que algunas personas tengan hijos, el examen podría impedir que se casen, o que se casen con cierta persona si se considera que la pareja no puede concebir. Del mismo modo, las pruebas de ADN y genética impulsadas por la IA podrían utilizarse en los esfuerzos por producir hijos sólo con las cualidades deseadas.

7. SURGIMIENTO DE NUEVOS DERECHOS

La IA dará lugar, así mismo, al surgimiento de nuevos derechos:

7.1. Derecho a la no discriminación algorítmica

El papel de la IA en la toma de decisiones discriminatorias está bien documentado, y es una de las cuestiones clave en el debate ético actual. Para reconocer estas cuestiones, Access Now se asoció con organizaciones de derechos humanos y empresas de AI para publicar la "Declaración de Toronto"[100] en marzo de 2018.

---

[99] González Espejo, Maria Jesús; Pavón, J. (2020). *An introductory guide to Artificial Intelligence for Legal Professionals*. Ed. Wolters Kluwer.

[100] https://www.hrw.org/node/320092/printable/print

Los ciudadanos tienen derecho a saber bajo qué criterios son evaluados, seleccionados o descartados por las instituciones o las empresas en procesos selectivos de cualquier tipo. Por ello, la incorporación de sistemas automatizados de selección o adjudicación, tanto públicos como privados, debe estar regulada de modo que se garantice la posibilidad de auditar los criterios realmente aplicados sobre cada caso concreto para asegurar que garantizan la igualdad y están dentro de los valores constitucionales.

La pregunta de si la calidad de las decisiones difiere entre las que se toman por los humanos y las que se toman sobre la base de un cálculo algorítmico sólo puede responderse si conocemos el funcionamiento de las decisiones humanas. Hay pruebas de que es especial[101] en lo que respecta al uso del conocimiento tácito y las normas tácitas. Esto permite a los humanos, por ejemplo, identificar casos excepcionales en los que la aplicación de una norma no es apropiada aunque el caso esté dentro de su ámbito. La creciente importancia de los algoritmos en la adopción de decisiones exige una mejor comprensión del diseño y las características de los procedimientos de adopción de decisiones[102].

El artículo 22 del RGPD establece que los sistemas de decisión automatizada basados en datos personales, incluyendo la elaboración de perfiles, exigen que el individuo dé su autorización a los mismos una vez que se le haya explicado suficientemente. No basta con contar con el consentimiento.

Esta norma presenta muchos retos prácticos para el diseño y desarrollo de algoritmos de machine-learning.

En este sentido, la Association of Computing Machinery (ACM) ha concluido que los modelos computacionales pueden ser distorsionados como resultado de los sesgos contenidos en sus datos de entrada y/o sus algoritmos. Las decisiones tomadas por los algoritmos de predicción pueden ser opacas debido a muchos factores, incluyendo técnica (el algoritmo puede no prestarse a una explicación fácil), económica (el costo de proporcionar transparencia puede ser excesiva, incluyendo el compromiso de los secretos comerciales), y social (revelando las aportaciones puede violar las expectativas de privacidad). Incluso los sistemas de computación bien diseñados pueden resultar en resultados o errores inexplicables, ya sea porque contienen errores o porque cambian las condiciones de su uso, invalidando las suposiciones en las que se basaron los análisis originales.

El uso de algoritmos para la toma de decisiones automatizada sobre los individuos puede traer consigo discriminación. Los encargados de la formulación de políticas deberían hacer que las instituciones que utilizan el análisis se ajusten a las

[101] Tversky, Amos and Daniel Kahneman (1974). 'Judgment under Uncertainty: Heuristics and Biases'. *Science* 185(4157):1124–31.

[102] Consejo de Europa, *op.cit*.

mismas normas que las instituciones en las que los humanos tradicionalmente han tomado decisiones.

La ACM ha establecido los principios para la transparencia algorítmica:

1. Concienciación: Los propietarios, diseñadores, constructores, usuarios y otros interesados en los sistemas analíticos deben ser conscientes de los posibles sesgos que conlleva su diseño, aplicación y uso, así como de los posibles daños que los prejuicios pueden causar a los individuos y a la sociedad.
2. Acceso y reparación: Los organismos reguladores deben fomentar la adopción de mecanismos que permitan la participación y la reparación a los individuos y grupos que se ven afectados negativamente por el algoritmo decisiones informadas.
3. Rendición de cuentas: Las instituciones deben ser responsables de las decisiones tomadas por los algoritmos utilizados, aunque no sea posible explicar en detalle cómo los algoritmos producen sus resultados.
4. Explicación: Se alienta a los sistemas e instituciones que utilizan la toma de decisiones algorítmicas a que expliquen tanto los procedimientos seguidos por el algoritmo como las decisiones que se toman. Esto es particularmente importante en los contextos de políticas públicas.
5. Procedencia de los datos: Una descripción de la forma en que se recogieron los datos de capacitación debe ser mantenida por los diseñadores de los algoritmos, acompañadas de una exploración de los posibles sesgos inducida por el proceso de recopilación de datos humanos o algorítmicos. El escrutinio público de los datos proporciona máxima oportunidad de correcciones. Sin embargo, la preocupación por la privacidad, la protección de los secretos comerciales o la revelación de análisis que podrían permitir a los actores maliciosos jugar con el sistema puede justificar la restricción del acceso a personas calificadas y autorizadas.
6. Auditabilidad[103].: Los modelos, algoritmos, datos y decisiones deben ser registrados para que puedan ser auditados en los casos en que se sospeche que hay daño.
7. Validación y pruebas: Las instituciones deben utilizar métodos rigurosos para validar sus modelos y documentar esos métodos y resultados. En particular, deberían realizar rutinariamente pruebas para evaluar y determinar si el modelo genera un daño discriminatorio. Se alienta a las instituciones a que hagan públicos los resultados de esas pruebas.

[103] Algunas ideas en torno a la auditabilidad pueden encontrarse aquí: Salgado, J., Fernández-Aller, M. Celia (2021) "A Wide Human-Rights Approach to Artificial Intelligence Regulation in Europe" *IEEE Technology & Society Magazine*, 40(1).

Además, es muy recomendable el uso de estudios de impacto ético, en línea con los estudios de impacto en la protección de datos que recoge el Reglamento Europeo.

7.2. Derecho a la explicabilidad

El mayor reto que plantea la IA desde el punto de vista de la gobernanza es la complejidad y la opacidad de la tecnología. No sólo puede ser difícil de entender desde un punto de vista técnico, sino que las primeras experiencias ya han demostrado que no siempre está claro cuándo se ha implantado un sistema de IA en un contexto determinado, y para qué tarea.

El derecho a la información, contenido en los artículos 13.2 f), 14.2 g) y 15.1 h) del RGPD, incluye, al menos, el derecho a conocer la elaboración de un perfil y a conocer información significativa sobre la lógica aplicada por el algoritmo, en términos comprensibles conforme al principio de transparencia y suficientemente exhaustiva al mismo tiempo, sin necesidad de incluir información sobre los algoritmos utilizados o la revelación de todo el algoritmo[104]. Sin embargo, estas disposiciones no incluyen el derecho a conocer en su totalidad el código fuente del algoritmo, por lo que el derecho a la explicabilidad no está suficientemente garantizado.

Por otro lado, el RGPD no ha resuelto satisfactoriamente la utilización de algoritmos y el derecho a la explicabilidad para combatir la opacidad en su uso, sobre todo cuando quien los utiliza es el poder público. "Se trata de una norma que no está diseñada para establecer las garantías que se han de reconocer a los ciudadanos frente al ejercicio de autoridad de los poderes públicos que pueda afectar a su estatuto jurídico, a sus derechos y libertades sino para regular el tráfico jurídico privado y proteger a consumidores frente a empresas que realizan tratamientos de datos cada vez más masivos"[105]. Por otro lado, el art. 22 del RGPD no resulta satisfactorio, entre otras cosas, porque no recoge el derecho a la explicabilidad de un grupo de afectados, sino de personas individuales[106]. Además, este artículo sólo se aplicaría en los casos en que la decisión se base exclusivamente en un tratamiento de datos personales.

De todo esto deducimos la necesidad de regular el derecho a la explicabilidad de los algoritmos, de forma que se superen los inconvenientes mencionados.

---

[104] GT29 (2018). «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 a efectos del Reglamento (UE) 2016/679». Disponible en https://bit.ly/31Fz79C.

[105] Boix Palop, Andrés (2020) "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", *Revista de Derecho Público: Teoría y Método*. Marcial Pons Ediciones Jurídicas y Sociales Vol. 1 | 2020 pp. 223-270 Madrid, 2020 DOI: 10.37417/RPD/vol_1_2020_33.

[106] Edwards, Lilian; Veale, Michael (2017) "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For" *Duke Law & Technology Review* 18.

Algunos autores proponen diferentes enfoques para evitar la opacidad de los algoritmos. Uno de ellos es el de evitar el uso de *machine learning* en determinados ámbitos de aplicación[107].

7.3. Neuroderechos

Los rápidos avances en la neurociencia humana y la neurotecnología abren posibilidades de acceder, recopilar, compartir y manipular la información que se encuentra en el cerebro humano. Las aplicaciones de IA con estas finalidades plantean importantes retos a los principios de los derechos fundamentales, que hay que abordar para evitar consecuencias no deseadas.

Algunos autores[108] plantean que será necesario reconocer nuevos derechos humanos[109]:

- el derecho a la libertad cognitiva, o el derecho a controlar la propia conciencia y el proceso del pensamiento electroquímico es un sustrato necesario para cualquier otro derecho de libertad;
- el derecho a la intimidad cerebral, puesto que la disponibilidad generalizada de aplicaciones neurotecnológicas proporcionará múltiples oportunidades para que las personas accedan a su actividad cerebral y la controlen, lo que puede traer consigo una serie de actividades potencialmente beneficiosas, como la autovigilancia o la mejora neuronal. Pero además, el uso de esa información por parte de terceros sin nuestro consentimiento puede ser devastador;
- el derecho a la integridad cerebral, puesto que las intrusiones en el cerebro de las personas no sólo pueden suponer una violación de su intimidad mental, sino también pueden tener un impacto directo en sus cálculos neuronales y resultar en un daño directo a la persona;
- el derecho a la continuidad psicológica**,** porque los cambios en la función cerebral causados por la estimulación cerebral también pueden causar alteraciones involuntarias de los estados mentales críticos para la personalidad, y por tanto pueden afectar a la identidad personal del individuo;

---

[107] Burrel, Jenna (2016) "How the machine 'thinks': understanding opacity in machine learning algorithms". *Big Data and Society*. DOI: 10.1177/2053951715622512.

[108] Ienca and Andorno (2017) "Towards new human rights in the age of neuroscience and neurotechnology", *Life Sciences, Society and Policy* 13:5 DOI 10.1186/s40504-017-0050-1.

[109] Existe un proyecto en la Universidad de Columbia, Neurorights Initiative, que trabaja este asunto. *https://nri.ntc.columbia.edu*

- el derecho a negarse a hacer uso de las tecnologías que supongan un acceso a la actividad cerebral y a implantarse dispositivos externos o internos relacionados con la captura de los datos;
- el derecho de acceso igualitario a esta tecnología como tratamiento curativo o paliativo, respetándose, en este último caso, las limitaciones de uso de los datos.

Las aplicaciones clínicas de las imágenes cerebrales y otras neurotecnologías están mejorando significativamente el bienestar de los pacientes que sufren trastornos neurológicos ofreciendo nuevas herramientas preventivas, diagnósticas y terapéuticas. Además, las aplicaciones comerciales están proporcionando rápidamente nuevas posibilidades en el ámbito de la mejora cognitiva, la comunicación personalizada y el entretenimiento, como el caso de las realidades inmersivas. Incluso varias aplicaciones de la neurotecnología están adquiriendo un gran interés en el ámbito jurídico.

Disponemos de muy poca información para adoptar decisiones bien fundadas sobre este tema, por lo que se requiere una gran cantidad de investigación y análisis, incluso con respecto a las características de los procesos humanos de adopción de decisiones. Dado que los procesos de adopción de decisiones de los seres humanos no son necesariamente "mejores" que los sistemas automatizados de adopción de decisiones, sino simplemente diferentes, es probable que en la adopción automatizada de decisiones se desarrollen diferentes tipos o sesgos, riesgos o errores. Por lo tanto, es necesario debatir abiertamente qué criterios deben elaborarse para medir la calidad de la toma de decisiones automatizada.

8. CONCLUSIONES

La IA modificará parcialmente nuestro modo de vida. Está ya presente en múltiples sectores que nos afectan como la educación, cultura, medicina, transportes, ciencia, etc., que se verán mejorados en el futuro; algunos de esos contextos experimentan ya los avances que proporciona la IA y que han de revertir en la ciudadanía. La IA no tiene otro fin que mejorar la calidad de vida de los individuos. La tecnología en general ha propiciado una nueva revolución, esta vez digital y que continúa imparable en su evolución, originando un nuevo modelo de sociedad: la sociedad digital.

Pero los avances han de ir acompañados de la regulación que proporcione el Derecho y de las directrices en el uso de la IA que aconseje la Ética. Porque son tantas las posibilidades que brinda la IA que no podemos dejar que, pervertida su utilización, se convierta en un medio de agresión contra los derechos fundamentales, justificado por una finalidad económica.

No queda ningún derecho fundamental que no experimente una significativa reflexión tanto en su contenido, forma de ser ejercido, o en lo que atañe a una probable forma de ser dañado; desde la libertad de circulación, la libertad de expresión, que ha conocido una nueva dimensión tras el uso de la tecnología para comunicar ideas, el derecho al trabajo o el derecho a la educación, etc., todos se encuentran afectados en algún aspecto esencial debido a los cambios tecnológicos. Evitar la amenaza y minimizar el riesgo es el objetivo que ha de perseguir el derecho, pues provocada la agresión a través de la IA, resulta un camino especialmente dificultoso iniciar el procedimiento para restablecer al particular en el disfrute de su derecho, en ocasiones por la opacidad que muestran algunos procesos de IA. Por tanto, la transparencia será una de las características a las que deberá prestar más atención el Derecho. No obstante, y como corresponde a un Estado de Derecho, los instrumentos de defensa de los derechos de que dispone el ordenamiento jurídico para poner fin a la lesión han de actuar de forma presta para no provocar un daño irreparable, dadas las potencialidades de la tecnología de superar las barreras del tiempo y del espacio.

Pero además la IA ha hecho surgir nuevos derechos a los que ha de dar forma, contenido y protección el Derecho constitucional: el derecho a la no discriminación algorítmica, derecho a la explicabilidad y los neuroderechos

Por ser la IA un fenómeno global no puede abordarse su regulación por cada ordenamiento jurídico de forma fragmentada. Por ello, la UE ha elaborado una batería de documentos y normas sobre IA consciente de la necesidad de legislar de forma homogénea. El mercado único digital es la aspiración de la UE, además de ser líder en IA, no solo en el espacio europeo, sino mundial. Para acordar principios y reglas comunes se acometen iniciativas legislativas directamente aplicables, de modo que se aporte seguridad jurídica a los ciudadanos y confianza en la aplicación de técnicas de IA. Urge que la UE apueste por una gobernanza de la IA, y que evite la orientación basada en autorregulación y legislaciones orientadas en función del riesgo.

La IA emplea datos personales y datos no personales. La normativa sobre datos personales necesita adaptarse a la IA, aunque los principios y derechos que recoge dicha legislación para el tratamiento de datos son aplicables también a la IA. La normativa de datos no personales está en desarrollo y persigue generar confianza entre los usuarios para fomentar el empleo de la IA en diversos sectores. En ambos casos, la ley que regule elementos propios de la IA debe ser predecible, responsable, verificable, respetar los derechos fundamentales y observar las reglas éticas.

Además, las normas que regulen la IA deben prever mecanismos de financiación para implantar y consolidar la transformación digital de la sociedad. La IA mejora la eficiencia del sector público y del sector privado. La persecución del interés común y del beneficio económico respectivamente deben ser objetivos que contemplen las normas de forma equilibrada, es decir, con el respeto a los derechos fundamentales.

El Derecho constitucional, esto es, el respeto a los derechos fundamentales y a los valores constitucionales, también valores y principios consagrados por la UE, constituye el derecho apropiado para crear el sustrato común sobre el que construir la IA propia de la sociedad digital.

BIBLIOGRAFÍA

Huergo Lora, Alejandro, Diaz Gonzalez, Gustavo Manuel (2020). *La regulación de los algoritmos*. Ed. Aranzadi. ISBN: 978-84-1345-096-4

Lazoz, G., y Castillo Parrilla, J. A., (2020) "Valoración algorítmica ante los derechs humanos y el Reglamento General de Protección de Datos: el caso SyRI", *Revista chilena de Derecho y Tecnología, v*ol. 9, 1

López Garrido, D.,(2017) (coord.), Serrano Pérez, Mª M., Fernández Aller, Mª C., *Derechos y obligaciones de los ciudadanos/as en el entorno digital*, Fundación Alternativas, Documento de trabajo 195/2017.

Serrano Pérez, Mª M., y Fernández Aller, Mª C., (2020). *El valor del dato en la Economía digital.* Nº: 21/2020. 02-07-2020. Ed. Fundación Alternativas.

Turégano Mansilla, I. (2020), "La dimensión social de la privacidad en un entorno virtual", Era digital, Sociedad y Derecho, Tirant lo Blanch, Valencia.