LA BÚSQUEDA DE UN MODELO REGULATORIO DE LA IA EN LA UNIÓN EUROPEA *

The Search for the European Union Regulatory Model

Susana Ruiz Tarrías **

Anales de la Cátedra Francisco Suárez
Fecha de recepción: 10/7/2022 ISSN: 0008-7750, núm. 57 (2023), 91-119
Fecha de aceptación: 01/09/2022 http://dx.doi.org/10.30827/ACFS.v57i.25245

RESUMEN La inteligencia artificial (IA) no es sólo una moda, sino un conjunto de sistemas tecnológicos que han adquirido en los últimos años un enorme desarrollo con aplicaciones a múltiples aspectos de la vida cotidiana de los ciudadanos, tanto por parte de particulares (empresas) como de los propios Estados.
La Unión Europea ha apostado siempre por compatibilizar los avances tecnológicos con el respeto de los principios y valores de la democracia, el Estado de Derecho y los derechos y libertades fundamentales. Desde tales premisas, actualmente se enfrenta a la búsqueda de un modelo regulatorio de la IA ante las carencias del Reglamento General de Protección de Datos (RGPD) en este ámbito.
A través de la Propuesta de Reglamento (UE) sobre IA, se pretende adoptar una regulación marco del uso de la IA que suponga una "tercera vía" inspirada en los principios y valores de la Unión y se contraponga a las actuales fórmulas regulatorias "abstencionistas" (EE.UU) e "hiperreguladoras" (China), proporcionando un modelo que consiga el efecto imitador o "efecto Bruselas" de una IA "confiable" para los ciudadanos y las empresas a nivel mundial.

Palabras clave: Inteligencia Artificial (AI), Marco Regulatorio, Derechos y Libertades Fundamentales, Principios y Valores de la UE, Reglamento (UE) sobre IA.

ABSTRACT Artificial intelligence (AI) is not just a fashion, but a set of technological systems that have acquired in recent years an enormous development with applications to multiple aspects of the daily life of citizens, both by individuals (companies) and by the States themselves.

---

* Para citar/citation: Ruiz Tarrías, S. (2023). La búsqueda del modelo regulatorio de la IA en la Unión Europea. *Anales de la Cátedra Francisco Suárez* 57, pp. 91-119.

a** Departamento de Derecho Constitucional, Universidad de Granada. Plaza de la Universidad, s/n. 18001 Granada (España). El presente trabajo forma parte de una investigación más amplia para la que se ha solicitado financiación a través de las convocatorias nacionales de Proyectos de Investigación I+D+i 2021-2022 que se encuentran en fase de evaluación a fecha de presentación de este estudio. Correo electrónico: *starrias@ugr.es*

The European Union has always been committed to making technological advances compatible with respect for the principles and values of democracy, the rule of law and fundamental rights and freedoms. Based on these premises, it is currently facing the search for a regulatory model for AI, given the shortcomings of the General Data Protection Regulation (GDPR) in this area.

The Proposal for a Regulation (EU) on AI aims to adopt a "third way" regulation of the use of AI inspired by EU principles and values, in contrast to current "abstentionist" (US) and "hyper-regulatory" (China) formulas, providing a model that achieves the "Brussels effect" of "trusted" AI for citizens and enterprises worldwide.

Keywords: Artificial Intelligence (AI), Regulatory Framework, Fundamental Rights and Freedoms, EU Principles and Values, Regulation (EU) on AI.

1. Introducción

La inteligencia artificial (en adelante, IA) comprende un amplio conjunto de tecnologías de rápida evolución, cuyo desarrollo ha irrumpido en los últimos años en múltiples ámbitos de las sociedades actuales, pretendiendo convertirse en la tecnología global de un futuro que cada día es más presente, fruto de lo que se viene denominando la Cuarta Revolución industrial, por referencia a la digitalización del sector productivo global (Barona, 2019, p. 22).

La IA puede aportar amplios beneficios económicos y sociales a todos los sectores productivos, logrando una mejora de la predicción, la optimización de la toma de decisiones, la asignación de recursos, y la personalización de las prestaciones. Pero, al mismo tiempo, puede generar nuevos riesgos para los derechos y libertades de personas concretas o grupos sociales.

Estamos ante un conjunto de tecnologías con un impacto multisectorial en diversas direcciones y niveles, tanto en el plano institucional como social y, dentro de este último, con incidencia en el conjunto de la sociedad, pero también del individuo. Esta amplitud de su rango de penetración convierte a las técnicas de IA en grandes instrumentos de transformación de las sociedades actuales, del funcionamiento de sus instituciones y organizaciones públicas y privadas, y de sus relaciones con los ciudadanos, cuyos derechos y libertades fundamentales deben ser protegidos con los estándares de la Unión Europea también en el contexto de la IA.

Hasta el momento, los modelos regulatorios de la IA adoptados se fundamentan en dos arquetipos básicos. De un lado, la hiperregulación de los actores tecnológicos por parte del Estado –del que constituyen una prolongación–, como es el caso de China. De otro lado, el que opera en los

Estados Unidos, caracterizado por el *laissez faire* reconocido a las empresas tecnológicas en el marco de la ausencia de una regulación normativa de carácter general.

Por su parte, como reconoce el artículo 2 del TUE, la Unión Europea ha mostrado un firme compromiso en la defensa de los valores de la democracia, el Estado de Derecho y la garantía de los derechos y libertades, pero también está decidida a encontrar un enfoque equilibrado que preserve su liderazgo tecnológico, garantizando que los ciudadanos europeos puedan beneficiarse de las posibilidades que ofrecen las tecnologías basadas en IA, al tiempo que éstas se desarrollen y funcionen con respeto a los valores y los principios de la UE.

Con esta finalidad ha sido adoptada la Propuesta de Reglamento (UE), del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de IA, y se modifican determinados actos legislativos de la Unión (COM (2021) 206 final), de 21 de abril de 2021 (denominada impropiamente desde el punto de vista del sistema de fuentes de la UE, Ley de Inteligencia Artificial o Ley de IA).

El presente estudio trata de abordar, en primer término, los problemas derivados de la delimitación científico-jurídica del concepto de IA, especialmente ante la prevalencia tradicional de las aproximaciones "éticas" frente a los enfoques normativos de carácter jurídico-positivo.

En segundo lugar, se pretenden identificar los aspectos más problemáticos en los que puede incidir la aplicación de las técnicas de IA respecto de los datos personales de los ciudadanos, y las posibles limitaciones del actual Reglamento General de Protección de Datos de la Unión Europea (Reglamento (UE) 2016/679) (en adelante, RGPD) para afrontar una tutela adecuada de los datos personales en el contexto de la IA, habida cuenta de que, como resulta ampliamente reconocido, los datos personales de los ciudadanos constituyen "el combustible" de las técnicas de IA.

Porque, en última instancia, la existencia de insuficiencias en el RGPD para afrontar el desarrollo de las tecnologías de IA protegiendo adecuadamente los datos personales de los ciudadanos europeos según los estándares de la Unión, el riesgo cierto de una fragmentación regulatoria de la IA por los Estados miembros, la voluntad de la UE de liderar a nivel global la tecnología de la IA, y la pretensión de crear un marco regulatorio de la IA que, basado en los principios y valores de la Unión, sirva de modelo al resto de países fuera y dentro de la Unión logrando el denominado "efecto Bruselas" alcanzado mediante la regulación europea de la protección de datos personales, constituyen los objetivos que fundamentan la adopción por la Comisión Europea de la Propuesta de Reglamento (UE) sobre IA, cuyos principios básicos se describen en las páginas que siguen.

2. Las dificultades científico-jurídicas para la concreción del concepto de IA

> Actualmente, el término IA puede encontrarse en el discurso de todos los ámbitos científicos. Rebasando los límites de los estudios relacionados directamente con la informática y la computación, también la Ciencia jurídica de nuestros días ha acogido en su objeto de estudio a la IA en prácticamente todas sus ramas de conocimiento. Se trata, pues, de un objeto de análisis que admite "miradas poliédricas" (Barona, 2021, p. 18).

El interés que despierta la IA no constituye una simple cuestión de 'moda'[1], sino el resultado del esfuerzo colectivo desarrollado por la comunidad científica por comprender y, posteriormente, enjuiciar las consecuencias derivadas de la irrupción de la IA en nuestra vida cotidiana y su incidencia en los derechos y libertades que, hasta ahora, formaban parte del paradigma de las democracias constitucionales occidentales[2].

De hecho, quien más o quien menos interactúa con la IA en distintas esferas de su vida profesional o privada con asiduidad, ya que la IA es, en realidad, "un término paraguas" (Voss, 2021, p. 10), que hace referencia a un conjunto de tecnologías, algunas en fase de desarrollo, pero que en su mayoría resultan ampliamente utilizadas por todos.

Por poner algunos ejemplos, cada vez que pagamos una compra con tarjeta de crédito, un algoritmo de IA aprueba la transacción (esperemos). Cuando utilizamos los dispositivos GPS en nuestro vehículo o nuestro *smartphone*, el algoritmo encuentra la mejor ruta para llegar a nuestro destino (supuestamente). Las recomendaciones de productos por empresas digitales como Amazon se elaboran mediante IA. Pero también el traductor de Google se basa en una técnica de aprendizaje estadístico que es IA. Incluso cuando hacemos búsquedas en Google, Baidu u otros motores de búsqueda, éstos utilizan la IA para ofrecernos los resultados más ajustados a nuestra solicitud. El reconocimiento facial, que puede llevarse a cabo a través de las cámaras de nuestros smartphones mostrando un recuadro en el que se inserta un rostro, es IA. Las Apps Siri o Alexa, nos entienden cuando les hablamos y responden (normalmente) de manera útil gracias a los algoritmos de IA para la comprensión del lenguaje (bots conversacionales).

---

1. Como "*buzzword*" (palabra de moda), la califica Poullet (2021).
2. Un ejemplo desde la perspectiva del Derecho privado viene a ser el análisis de la aplicación de la IA a los mecanismos de resolución de conflictos *online* (Montesinos, 2021, pp. 507-531).

Si entramos en el ámbito de la robótica, quizá resulta más fácil visualizar la IA en objetos que han entrado en nuestros hogares como el robot Roomba, que limpia el suelo de nuestra casa[3], o robots de compañía como Nao, Pepper, Aibo o Giraff, que pueden entretenernos, hablar con nosotros y ayudar a las personas mayores a mantenerse en contacto con sus familiares, amigos o servicios de atención sanitaria. Los vehículos sin conductor se basan completamente en la IA para identificar las señales de tráfico, las líneas de la calzada, otros vehículos, peatones, semáforos, etc.

Como se puede apreciar, el ámbito de utilización de la IA resulta increíblemente extenso, y a pesar de los numerosos estudios científicos que ofrecen posibles descripciones de la IA todavía no existe un acuerdo general sobre su definición (Walz y Firth-Butterfield, 2018-2019, p. 182).

De hecho, se han utilizado diferentes denominaciones para referirse a la IA a lo largo del tiempo, como la de "máquinas ultrainteligentes", en referencia a máquinas más inteligentes que el más inteligente de los hombres[4]. Sin embargo, la combinación de los términos "máquina" e "inteligencia" ha dado lugar a numerosas controversias a partir de diferentes definiciones y teorías de la inteligencia[5], por lo que, según afirman Muehlhauser y Helm (2012, p. 2), debido a sus connotaciones emocionales, el término "inteligencia" no parece ser el más apropiado para yuxtaponerlo al de "máquinas".

Más recientemente, según señala Rossi (2016, pp. 1-2), para no identificar el término IA con el concepto de una sustitución/suplantación de la inteligencia humana por algo sintético, se han acuñado expresiones como "inteligencia aumentada" o "computación cognitiva".

Del mismo modo, el Protocolo n. 108 del Consejo de Europa, tanto en su versión inicial como en su actualización en 2018 (Protocolo 108+), opta por la utilización del término "tratamiento automatizado" de datos frente al de "tratamiento autónomo", y afirma en su art. 9.1.a) que "todo individuo" tiene el derecho "a no ser objeto de una decisión que le afecte significativamente a él o ella, basada únicamente en un tratamiento automatizado de datos sin haber tomado en consideración sus opiniones".

---

3. Sus últimas versiones, al incorporar cámaras integradas, permiten recopilar información acerca de una enorme cantidad de datos personales que afectan al ámbito de nuestra privacidad, como las dimensiones de nuestra vivienda; las cosas con las que el robot tropieza permiten deducir si tenemos hijos o no, qué edades tienen los niños atendiendo a la tipología de objetos, etc. Una información que, tras ser procesada de modo agregado, permite conocer el tipo de familia que somos, nuestra capacidad económica, nuestras aficiones, gustos decorativos, etc.
4. *Vid.* Good, 1965; Bostrom, 1998 y Legg, 2008.
5. Entre otros, Davidson y Kemp, 2011; Niu y Brass, 2011.

Asimismo, el Reglamento General de Protección de Datos (RGPD) define su ámbito de aplicación material por referencia al tratamiento "total o parcialmente automatizado" de datos personales (art. 2.1), y en su art. 22 reconoce el derecho de todo interesado "a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo similar".

Tales definiciones tratan de superar la interpretación puramente técnica que subyace a la formulación original del concepto de IA enunciado por John McCarthy y otros en 1955, en referencia a una máquina que "se comporta de un modo que podría llamarse inteligente si estuvieran actuando humanos" (McCarthy *et al.,* 1955).

No obstante, esta definición no aporta ninguna información acerca de las funcionalidades técnicas de la IA, es decir, de la tecnología (software, algoritmos, conjunto de procesos, robótica, etc.) que permite funcionar adecuadamente con anticipación a su entorno, o, más concretamente, de la "tecnología que es capaz de adaptarse por sí misma a las circunstancias sobre la base de ciertas habilidades de auto-aprendizaje para producir resultados independientes del control humano" (Walz y Firth-Butterfield, 2018-2019, p. 183).

Recientemente, el concepto de "inteligencia artificial" se ha contrapuesto por la literatura científica al de "superinteligencia artificial" (Yampolskiy y Duettmann, 2020), entendiendo por el primero "la capacidad de los sistemas creados por el hombre para imitar el pensamiento humano rudimentario", mientras el segundo se define como "la capacidad de los sistemas creados por el hombre que pueden superar a éste" (How, 2019, p. 46).

La concreción desde diversas perspectivas del concepto de IA no supone, sin embargo, avances significativos en la aportación de un concepto comúnmente compartido de la misma. Así, un reciente estudio desarrollado en el marco del Parlamento Europeo, reconoce que tampoco existe una idea común sobre la IA en la Unión Europea, donde los términos IA, robótica y algoritmos constituyen expresiones ampliamente utilizadas, si bien con significaciones muy diferentes para los ciudadanos y para los expertos (Evas, 2020, p. 12).

En este contexto, una diferenciación conceptual articulada desde el Parlamento Europeo por T. Madiega, propone distinguir entre:

– "inteligencia artificial", en referencia a máquinas de aprendizaje técnico utilizadas para buscar y analizar gran cantidad de datos;
– "robótica", para definir todo lo que puede hacerse mediante máquinas programables desde su ideación, diseño, fabricación y manejo, y

– "algoritmos y otros sistemas de toma de decisiones automatizadas", como expresión de procesos autónomos de toma de decisiones prediciendo la conducta de humanos y máquinas (Madiega, 2019, p. 2).

En todo caso, al hablar de IA el debate científico y social se sitúa en términos de ponderación riesgo/beneficio que el uso de esta técnica puede proporcionar a la sociedad y los ciudadanos[6], tomando en consideración que una IA "ética" puede marcar la diferencia en comparación con una IA sin restricciones.

3. El uso beneficioso de la IA o los principios de una IA "ética"

En este sentido, en 2017 se concretaron los denominados "*Principios de Asilomar*", tomando el nombre de la ciudad de la costa californiana donde se celebró la Conferencia (*Beneficial AI*) organizada por el *Future of Life Institute* (FLI)[7] que, concretando respecto de la robótica actual las tres leyes de la robótica formuladas por Isaac Asimov en 1942, pretenden sustentar el desarrollo de un uso beneficioso de la IA[8]:

A pesar de la importancia atribuida a la IA "ética", tampoco existe un consenso acerca de la naturaleza, composición y funciones que deben desarrollar los denominados comités u organismos de ética, creados en el marco de las tecnologías de la comunicación y la investigación y, especialmente, en relación con la IA (Polonetsky, Tene y Jerome (2015).

También en la Unión Europea se pretende proteger a los ciudadanos desde la ética de la gobernanza de las nuevas tecnologías, llegándose a formular el concepto de *etificación* como instrumento de regulación de las

6. Entre los beneficios que la IA aporta a la sociedad suele mencionarse la mejora en ámbitos específicos de nuestra vida como el cambio climático, las pandemias y la hambruna, la calidad de vida a través de una medicina personalizada, la competitividad, la política exterior y la seguridad, el mercado laboral, etc.
No obstante, estudios recientes muestran que el optimismo inicial respecto de los potenciales beneficios de la IA ha caído significativamente, precisamente entre quienes desarrollan sistemas de IA, de modo que una comprensión realista sobre su funcionamiento podría estar relacionada con unas expectativas también más realistas de sus límites (Mayor, 2022).
7. Entre los fundadores del FLI se encuentran científicos y personalidades tan relevantes como Stephen Hawking, Elon Musk, Max Tegmark (MIT), Jaan Tallinn (inventor de Skype), Stuart J. Russell (ciencias de computación), George Church (biología), Saul Perlmutter y Frank Wilczek (físicas).
8. Disponible en: https://futureoflife.org/2017/08/11/ai-principles/. Último acceso: 26.2.2022.

tecnologías de la información y de la comunicación (Van Dijk, Casiraghi y Gutwirth, 2021).

Desde tales premisas, el punto de referencia europeo relacionado con la IA se sitúa en la Dirección General de Redes de Comunicaciones, Contenidos y Tecnología (DG Connect)[9] y, en particular, en la Unidad de Excelencia e Innovación en IA, que aplica las políticas y marcos estratégicos de desarrollo "de la estrategia ética" europea de la IA de acuerdo con el Grupo Europeo sobre ética y ciencia en las nuevas tecnologías (EGE, por sus siglas en inglés). Además, también se encuentran involucradas en esta tarea la Agencia Ejecutiva de Investigación europea (REA, por sus siglas en inglés) y la Dirección General de Investigación e Innovación (RTD, por sus siglas en inglés).

El Grupo EGE fue un referente para la elaboración por el Grupo de Expertos de alto nivel sobre IA (AI HLEG, por sus siglas en inglés) del documento publicado en 2019 "Directrices Éticas para una Inteligencia Artificial fiable", donde se propone el desarrollo de unos principios "éticos" de la IAa partir de los derechos y libertades reconocidos en los Tratados UE, la Carta Europea de Derechos Fundamentales y los Tratados internacionales sobre derechos humanos (como la Carta Social Europea), así como documentos adoptados en ámbitos específicos, como el Reglamento General de Protección de Datos (RGPD) (*vid.* AI HLEG, 2019, pp. 10-11).

Más concretamente, la Propuesta de Reglamento (UE) sobre la IA hace referencia al hecho de que el uso de la IA, dadas sus particulares características, como la opacidad[10], la complejidad, la dependencia de datos, el comportamiento autónomo, etc., "puede tener repercusiones negativas" respecto de múltiples derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la UE (CDFUE).

De ahí que se afirme que la Propuesta de Reglamento (UE) sobre la IA "pretende garantizar un elevado nivel de protección para dichos derechos fundamentales", así como afrontar las distintas amenazas a través de un "enfoque basado en los riesgos claramente definidos". Para ello, utiliza un conjunto de requisitos que garanticen una IA fiable, imponiendo "obligaciones proporcionadas" a todos los actores en la cadena de valor,

9. https://ec.europa.eu/info/departments/communications-networks-content-and-technology_n#responsibi lities

10. Aunque pueden identificarse diferentes aspectos de la opacidad: opacidad como secreto de Estado o corporativo, opacidad como analfabetismo tecnológico, u opacidad como medio a través del cual los algoritmos operan en la escala de aplicación, Burrell considera posible un enfoque de la opacidad "en términos de red neutra" (Burrell, 2016, pp. 3-7).

reforzando, en última instancia, la garantía de los derechos salvaguardados por la CDFUE (Comisión Europea, 2021, p. 12).

Por lo que respecta a la protección de datos, el Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés), hizo referencia a la "ética digital" como parte de la estrategia impulsada por G. Buttarelli (2015-2019) creando, en 2018, un Grupo Asesor sobre ética (EAG, por sus siglas en inglés).

No obstante, como reconocen Van Dijk, Casiraghi y Gutwirth (2021: nota 20), en el contexto de la protección de datos personales la ética no juega un papel determinante y, de hecho, desde la designación del nuevo Supervisor en 2019 el énfasis en la ética parece haber desaparecido de la agenda de la institución.

En cualquier caso, la contraposición Ética vs. Derecho viene a ser, respectivamente, la equivalencia entre difuminación y delimitación, con las consiguientes diferencias respecto de la efectividad, aplicabilidad, garantía de cumplimiento y, en su caso, aplicación del derecho sancionador, lo que explica que en el ámbito de los organismos o comités asesores se diferencie y se equilibre cuidadosamente lo que pertenece a cada uno de los ámbitos con la finalidad de reclamar "independencia y legitimación".

Porque cuando la ética "necesita ir más allá de la ley", la industria pone el foco en promover la auto-regulación, lo que puede suponer la "obstrucción de la legislación en favor de los intereses de las grandes empresas", desdibujando su diferenciación respecto del Derecho. De ahí que los principios europeos deban presentarse como "éticos", pero no como consecuencia de un razonamiento filosófico sino porque se basan en normas o procedimientos jurídicos, como los Tratados UE o la Carta de los Derechos Fundamentales de la UE, y esta premisa resulta especialmente evidente cuando la IA entra en conexión con la protección de datos personales en la Unión Europea, de manera que el eslogan acuñado por G. Buttarelli, como Supervisor Europeo de Protección de Datos, según el cual, la ética está "antes, durante y después del Derecho", puede entenderse también como la "ética del Derecho".

Ello explica que el planteamiento regulador de la UE se fundamente en la atención prestada a las consideraciones éticas, de conformidad con los valores fundamentales de los derechos humanos y los principios democráticos y, desde tales premisas, la Propuesta de Reglamento (UE) sobre la IA se propone alcanzar un "efecto Bruselas" similar a la regulación de la UE en materia de protección de datos, en un primer momento la Directiva 95/46/CE y, actualmente, el RGPD.

El objetivo resulta ser, en consecuencia, "que el poder regulador y de mercado de la UE se traduzca en una ventaja competitiva en la IA" tanto

dentro como fuera de la Unión, de manera que la adopción del primer marco regulatorio del mundo en materia de IA "podría suponer una ventaja para establecer normas internacionales de IA basadas en los valores europeos", así como para exportar exitosamente la "IA de confianza" más allá de las fronteras de la UE (Voss, 2021, pp. 23)[11].

Una Propuesta de regulación que, según se afirma, garantiza su coherencia con la Carta de los Derechos Fundamentales de la UE, sin perjuicio de lo establecido en el Reglamento General de Protección de Datos (RGPD) –aunque éste no menciona a la IA– y la Directiva sobre protección de datos en materia penal (Directiva (UE) 2016/680), a los que complementa mediante un "conjunto de normas armonizadas" aplicables al diseño, desarrollo y utilización de determinados sistemas de IA, que, además, "reducen al mínimo" el riesgo de discriminación algorítmica (Comisión Europea, 2021, pp. 3-4)[12].

4. El impacto de la IA en el marco regulatorio de los datos personales

4.1. La aplicación de técnicas de IA a los datos personales

En este campo, el objetivo consiste en encontrar un marco regulatorio para afrontar los procesos de aprendizaje automatizado de algoritmos basados en el manejo de grandes cantidades de datos personales, en la capacidad para recoger los datos y en la identificación de patrones a partir de los mismos, de ahí que se haya llegado a afirmar que los datos personales constituyen "el combustible" de la economía digital (HM Treasury, 2018).

Ello explica que en los últimos años se haya desarrollado un creciente interés por la transferencia y el almacenamiento de datos –entre otros medios, a través de la denominada computación en nube (*cloud computing*)–, por el proceso de conversión en datos (*datificación*) de gran parte de nuestra vida (Mayer-Schönberger y Cukier, 2013, p. 78) y, paralelamente, por el análisis de los megadatos (*Big Data analytics*), creando un contexto

11. Concretamente, el marco regulatorio de la IA en los EE.UU. se basa en la ausencia de una regulación horizontal en el ámbito digital por parte de los poderes públicos, centrándose en leyes sectoriales y en la innovación del sector privado. Ciertamente, la Ley de Iniciativa Americana de Inteligencia Artificial de 2019 supuso un cierto reajuste, pero, con carácter general, el planteamiento se orienta al mercado con la finalidad de evitar el "exceso normativo" (Voss, 2021, p. 22).
12. *Vid*., al respecto, Spiekermann (2015).

completamente nuevo en favor del desarrollo de la IA pero también de sus potenciales riesgos.

Entre estos últimos, cabe destacar los derivados de su afectación a la monetarización de los datos personales de los ciudadanos en tanto que usuarios de determinadas Apps, redes sociales, dispositivos inteligentes, etc., dando lugar a una sociedad tecnocrática sustentada en el mercado de los datos. Una tendencia que pone en cuestión y socava progresivamente la capacidad de autodeterminación del individuo, el concepto de vida privada, los derechos y libertades fundamentales e, incluso, como vislumbra O'Neil (2016), es capaz de comprometer aspectos esenciales de las actuales democracias constitucionales.

Con el fin de prevenir las consecuencias desfavorables para las personas y la sociedad, el Comité Consultivo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa (Protocolo 108+), adoptó el 25 de enero de 2019, unas *Líneas directrices sobre la Inteligencia Artificial y la Protección de Datos* (T-PD(2019)01) que pretenden garantizar el uso respetuoso con el derecho a la vida privada y a la protección de datos de carácter personal (artículo 8 CEDH) por parte de las técnicas basadas en la IA.

En dicho texto, se establecen como pilares del desarrollo de la IA basado en el tratamiento de datos personales, la legalidad y la equidad del tratamiento, la definición de la finalidad, la proporcionalidad del tratamiento, la privacidad por diseño y por defecto (*privacy by design*), la responsabilidad y la demostración del cumplimiento (*accountability*), la transparencia, la seguridad de los datos y la gestión del riesgo.

Entre las orientaciones que se facilitan al legislador, se incluye la de dotar a las autoridades nacionales de control de los recursos suficientes para verificar los programas de vigilancia algorítmica desarrollados por fabricantes y prestadores de servicios de IA, respetando siempre los derechos humanos y los derechos de los interesados. Del mismo modo, se insta al legislador a que garantice la autonomía de la intervención humana en la toma de decisiones al margen de los resultados de las recomendaciones basadas en el uso de la IA (1-3).

Precisamente el reciente estudio publicado por el Servicio de Investigación del Parlamento Europeo pone el foco en el riesgo para la privacidad y los datos personales que provienen de las aplicaciones de la IA a través del reconocimiento facial debido a su capacidad para identificar individuos a distancia, en tiempo real o a partir de imágenes o vídeos anteriores, de manera remota y con una implicación individual prácticamente nula (Dumbrava, 2021, p. 28). Un riesgo que se amplifica cuando las técnicas de reconocimiento facial se utilizan en espacios públicos como instrumentos

de "vigilancia masiva", creando un vínculo permanente donde los ciudadanos son tratados como potenciales sospechosos (Jones, 2020, p. 33).

Ello explica el interés de las instituciones europeas por las tecnologías de la IA[13], que se explicita en la Comunicación (COM(2019) 66 final, de 19 de febrero de 2020, *Una Estrategia Europea de Datos*, afirmando que:

> La UE tiene el potencial para tener éxito en una economía ágil en el manejo de los datos. Cuenta con la tecnología, los conocimientos técnicos y una mano de obra altamente cualificada. Pero competidores como China y los Estados Unidos ya están innovando rápidamente y proyectando sus conceptos de acceso a los datos y uso de datos en todo el mundo. En los Estados Unidos, la organización del espacio de datos se deja al sector privado, con considerables efectos de concentración. En China se da una combinación de supervisión gubernamental con un fuerte control por parte de las grandes empresas tecnológicas de cantidades masivas de datos sin suficientes garantías para los individuos. A fin de desarrollar este potencial de Europa, tenemos que encontrar nuestro modo europeo de equilibrar el flujo y el amplio uso de los datos, preservando al mismo tiempo un elevado nivel de privacidad, protección, seguridad y ética.

En consecuencia, la Unión Europea trata de encontrar su propio modelo regulatorio de la IA entre el neo-liberalismo norteamericano y el totalitarismo chino, a través de una "tercera vía" que en Europa significaría

---

13. En el ámbito del Parlamento Europeo se pueden citar la Resolución de 20 de enero de 2021, *sobre inteligencia artificial* (P9_TA(2021)0009), pero también la Resolución de 6 de octubre de 2021, *sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales* (P9_TA(2021)0405), la Resolución de 12 de febrero de 2019, *sobre una política industrial global europea en materia de inteligencia artificial y robótica* (P8_TA(2019)0081), o la Resolución de 20 de octubre de 2020, *con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* [2020/2012(INL)], o la Resolución de la misma fecha, *sobre un régimen de responsabilidad civil en materia de inteligencia artificial* (2020/2014(INL).
Otras iniciativas relevantes del Parlamento Europeo respecto de la IA se han concretado en el *Proyecto de informe sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales* [2020/2016(INI)], o el *Proyecto de informe sobre la inteligencia artificial en los sectores educativo, cultural y audiovisual* [2020/2017(INI)].
En relación con éste último, la Comisión ha aprobado el *Plan de Acción de Educación Digital 2020-2027: Adaptar la educación y la formación a la era digital* (COM(2020) 624 final).
Por lo que respecta a la Comisión Europea, cabe mencionar la Comunicación (COM(2019)168 final), de 8 de abril, *Generar confianza en la inteligencia artificial centrada en el ser humano*, de 8 de marzo de 2019.

sustentar la economía de la IA en los principios de apoyo a la "excelencia" en la investigación y de generación de "confianza" en los ciudadanos (*Trust and Excellence*) (Poullet, 2020, p. 11)[14].

Estos mismos objetivos aparecen en el *Libro blanco sobre Inteligencia Artificial - un enfoque europeo orientado a la excelencia y a la confianza* (COM(2020) 65 final), donde la Comisión Europea subraya la importancia de la legislación de protección de datos personales al tiempo que pone de manifiesto sus carencias respecto de su aplicación a la tecnología de la IA.

De hecho, el Libro blanco sobre la IA, de 19 de febrero de 2020, alerta de que la "actual falta de un marco común europeo" sobre la IA constituye un "riesgo real" de fragmentación del mercado interior que pondría en peligro los objetivos de confianza y seguridad jurídica en el mercado único de la IA. A modo de ejemplo, se subraya que el Comité alemán sobre ética en materia de datos "propone un sistema de regulación de cinco niveles basado en el riesgo, que va desde la ausencia de regulación en el caso de los sistemas de IA más inocuos hasta la prohibición absoluta en el caso de los más peligrosos". Por su parte, Dinamarca ha puesto en marcha "un prototipo de «sello de ética de los datos»", y Malta ha articulado un "sistema voluntario de certificación de la IA".

En España, la reciente Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, bajo la rúbrica "*Inteligencia Artificial y mecanismos de toma de decisión automatizadas*", dedica su artículo 23 a esbozar una primera aproximación a la regulación de la IA en el marco de las Administraciones públicas y las empresas.

Según se afirma, la premisa para las Administraciones públicas y las empresas es la de promover "el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido" (apartado 3).

En este contexto, se dispone que las Administraciones públicas "favorecerán la puesta en marcha de mecanismos" para que los algoritmos involucrados en la toma de decisiones que utilicen "tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente" (apartado 1).

En todo caso, se especifica que "priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos" (apartado 2) —disponiendo que se promoverá la adopción de un "sello de calidad de los algoritmos" (apartado 4)—.

14. Estos eran los pilares en los que se sustentaba la Comunicación de la Comisión (COM(2018) 237 final), de 25 de abril de 2018.

Entre los mecanismos a implementar por las Administraciones públicas respecto de los algoritmos aplicados a los procesos de toma de decisiones se encuentran "su diseño y datos de entrenamiento", debiendo abordar también "su potencial impacto discriminatorio" mediante la realización de "evaluaciones de impacto".

Un conjunto de situaciones que nos llevan a preguntarnos con Y. Poullet, si las disposiciones del Reglamento General de Protección de Datos (RGPD) son adecuadas respecto de los riesgos provenientes de la IA (Poullet, 2021, 10), habida cuenta de que el derecho a la protección de datos de carácter personal, reconocido en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) debe ser tutelado efectiva y adecuadamente, también en el contexto de la utilización de técnicas de IA.

4.2. Los riesgos para la individualización de los ciudadanos provenientes de la aplicación de técnicas de IA

a) La protección de datos personales como exclusión de la individualización

El artículo 4.1) del RGPD define a los datos personales como "toda información sobre una persona física identificada o identificable («el interesado»)"[15], y se considerará persona física identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o

15. El RGPD no resulta aplicable a las personas jurídicas que, sin embargo, se ven profundamente afectadas por la elaboración de perfiles económicos. Así, sobre la base de informaciones parciales y desintegradas a las que se le aplican técnicas de IA, los bancos, las aseguradoras o ciertos operadores de servicios de la información tienen la capacidad de predecir el futuro de una empresa a través de la elaboración de *rankings* que inducen a otros operadores y al mercado a actuar en un determinado sentido con relación al puesto asignado a una empresa.
En este sentido, el Reglamento (UE) 2019/1150, de 20 de junio, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (DOUE L 186/57, de 11.7.2019), reconoce a los servicios de intermediación en línea el derecho de restricción, suspensión o cancelación, respecto de una determinada empresa o profesional, de la prestación de sus servicios (art. 4.1 y 2), y al usuario profesional, en los casos anteriores, el derecho de acceso "a los datos personales o de otro tipo, o ambos, que se hayan generado por su uso de los servicios de intermediación en línea pertinentes antes de que la restricción, suspensión o terminación haya surtido efecto" (art. 4.3).

varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Además, el artículo 22.1 del RGPD reconoce el derecho de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, aun cuando el mismo precepto reconoce excepciones muy comunes, tales como la celebración o ejecución de un contrato con un responsable del tratamiento; que se encuentre autorizada por el Derecho de la Unión o de los Estados miembros y se apliquen las garantías adecuadas para la protección de los derechos del interesado[16], o que se preste el consentimiento por parte de este último [art. 22.2 RGPD][17].

Se trata, por lo tanto, de una concreción del término "dato personal", que toma como eje el concepto de "identificación" de la persona física, de ahí que cuando el tratamiento de los datos personales para fines distintos de los que fueron recogidos no esté basado en el consentimiento del interesado, el artículo 6.4.e) RGPD considere como garantía adecuada para el interesado el "cifrado" o la "seudonimización" de sus datos personales.

De hecho, el RGPD incorpora explícitamente la "seudonimización" como medida relativa a la protección de datos, en el entendimiento de que "puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos", tratando de incentivar la seudonimización en el tratamiento de datos personales por parte de los responsables del tratamiento cuando sea posible (Considerandos 28 y 29 RGPD).

---

16. En el ámbito de esta excepción cabría situar la regulación del artículo 23 de la Ley 15/2022, de 12 de julio, adoptada en España, aun cuando cabría preguntarse su compatibilidad con las exigencias previstas en el apartado 4 del artículo 22 RGPD, habida cuenta de que la regulación española no ha incorporado ninguna diferenciación respecto a "categorías especiales" de datos. En este sentido, resulta conocido que el Tribunal Constitucional anuló el artículo 58 bis.1 de la LOREG por considerar que posibilitaba la toma de decisiones basadas únicamente en el tratamiento automatizado de un dato personal "sensible" como es la opinión política de los ciudadanos sin las debidas garantías (STC 76/2019, de 22 de mayo. ECLI:ES: TC:2019:76).

17. En opinión de Tosoni (2021), la interpretación de este precepto permite considerar que no se trata de una prohibición general incorporada por el legislador europeo sino más bien de un "derecho subjetivo" otorgado a los interesados para ser ejercido discrecionalmente por éstos, pudiendo hablarse, en consecuencia, del "derecho a objetar" a las decisiones individuales automatizadas.
No obstante, dicha interpretación no toma en consideración el hecho de que la aplicación de técnicas de IA permite elaborar perfiles a partir, incluso, de datos anónimos y de metadatos que, por su propia naturaleza, impiden al interesado conocer que sus datos personales están siendo objeto de tratamiento y, en consecuencia, difícilmente podrá oponerse a la elaboración de su perfil a través del pretendido derecho de objeción.

Precisamente, el impacto de la IA proviene precisamente, de su incidencia en el concepto de "identificación" al que hace referencia el RGPD, pues los sistemas de IA utilizan profusamente los datos seudonimizados provenientes de distintas fuentes (navegación en internet, datos de geolocalización, etc.), así como metadatos (datos adicionales que proporcionan información sobre los datos, como por ejemplo, en una llamada: el número de teléfono de origen y de destino, la hora, la duración, etc.), posibilitando la localización de los datos provenientes de una única persona y la elaboración de perfiles[18].

En el mismo sentido se ha venido pronunciando el Grupo de Trabajo del Art. 29 (WP 20 por sus siglas en inglés) en su *Opinión sobre el concepto de "dato personal"* publicada en 2007. Según estima, el concepto de datos personales se extiende a la "identificación", es decir, a la posibilidad de que el responsable del tratamiento pueda vincular los datos recogidos de modo directo o indirecto a la identidad de una persona concreta, pero también a la "accesibilidad", o lo que es lo mismo, la posibilidad de reconocer a la persona afectada sin usar ningún elemento de su identidad civil (nombre, dirección, etc.) (GT 29, 2007, p. 14).

De este modo, el aspecto más relevante proviene del hecho de que la viabilidad de identificar a una persona "no implica necesariamente la capacidad de conocer su identidad, sino de individualizarla", evidenciando su singularidad sin que su identidad legal (necesariamente) tenga que ser conocida por quienes llevan a cabo el tratamiento de sus datos personales (Poullet, 2020, p. 49).

---

18. En octubre de 2020, el TJUE se pronunció respecto de dos asuntos relacionados con la conservación de metadatos, aplicando una línea interpretativa continuista respecto de la iniciada en los asuntos *Tele2 Sverige v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, de 21 de diciembre de 2016, y *Digital Rights Ireland Ltd*, de 8 de abril de 2014.
Así, en las Sentencias de 6 de octubre de 2020, *Privacy International* y *La Quadrature du Net*, el Alto Tribunal de la UE precisó que la Directiva sobre la privacidad y las comunicaciones electrónicas, interpretada de acuerdo con los arts. 7, 8,11 y el art. 52.1 de la CDFUE:
—se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional, y
—exige al juez penal nacional que descarte las informaciones y pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de un proceso penal, cuando proceden de un ámbito que escapa del conocimiento de los jueces y pueden influir de modo determinante en la apreciación de los hechos.

El riesgo del tratamiento masivo de metadatos mediante técnicas de IA proviene, pues, de su capacidad para revelar información sensible de la persona, no tanto a partir de sus datos personales sino a través de los metadatos y de los resultados del tratamiento de los datos seudonimizados, respecto de los cuales los interesados desconocen su propia existencia y los resultados del tratamiento al que son sometidos[19]. En algunos casos, los interesados pueden conocer y prestar o no su consentimiento a la recogida de datos personales. En otros supuestos, sus datos personales podrán ser recogidos a través de las garantías adecuadas previstas en el RGPD, pero en cualquiera de los casos, los interesados desconocen el tratamiento de sus metadatos y la posterior aplicación a los mismos de técnicas de IA, por lo que, en consecuencia, carecen de la oportunidad de ejercer los derechos que le asisten respecto de sus datos personales.

---

19. La Decisión del Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés), de 21 de diciembre de 2021 (asuntos acumulados 2019-0370 & 2021-0699), cuestiona la necesidad de desarrollar un proceso de clasificación de los datos pertenecientes a determinadas categorías de interesados más allá de las previsiones contenidas en el art. 18.5 y en el Anexo II.B del Reglamento de la Europol, según el cual, los datos compartidos con Europol deben limitarse exclusivamente a individuos respecto de los cuales se haya establecido claramente un vínculo con una actividad criminal (sospechosos, delincuentes potenciales, testigos, víctimas, contactos, cómplices o informantes).
En opinión de la alta autoridad europea de protección de datos, la investigación desarrollada demuestra, por el contrario, que los Estados miembros han ido enviando cada vez mayores cantidades de datos a la Europol, incluso cuando la naturaleza de los datos recogidos a nivel nacional en el contexto de investigaciones penales y de operaciones de inteligencia criminal no se limitan a datos específicos, sino que incluyen grandes conjuntos de datos, dando lugar a la generación de mayores contenidos de datos.
La conservación de datos sin categorización de los sujetos de los datos (*Data Subject Categorisation* (DSC), en sus siglas en inglés), durante un periodo indefinido y, eventualmente, durante toda la duración de una investigación penal que puede llegar a durar diez años, resulta contraria a los preceptos citados en tanto que "genera un alto riesgo" de que la Europol trate datos de personas que no pertenecen a ninguna de las categorías de interesados enumerados en el Anexo II.B durante largos periodos de tiempo. Y ello porque, afirma, la traslación de dichos datos a la Europol por las autoridades nacionales, donde serán objeto de un tratamiento posterior al ser compartidos con otras autoridades policiales, y cotejados con la información procedente de otros países, implica una ampliación considerable del impacto y de los riesgos potenciales para el interesado más allá del ámbito nacional.
De este modo, en aplicación del art. 28.1.e) del Reglamento de la Europol, según el cual los datos personales no pueden conservarse más allá del tiempo estrictamente necesario para cumplir con los fines para los que fueron tratados, el Supervisor Europeo ordena a la Europol proceder a la categorización de los datos recibidos en el plazo de seis meses desde su Decisión, debiendo proceder a la cancelación de todos los datos no categorizados transcurrido ese plazo.

De ahí que una de las primeras dudas que se plantean respecto de los datos personales y la IA sea la cuestión del ejercicio de los derechos otorgados por el RGPD a los interesados —"individualizados" aunque no "identificados"—, pues resulta importante que esta persona pueda ejercer, también en línea, sus derechos (de oposición, de cancelación, o, simplemente, de acceso) sin revelar su identidad (Poullet, 2020, p. 51).

b) La aplicación de técnicas de IA a los datos anónimos, anonimizados y pseudoanonimizados

En principio, el RGPD no es aplicable a los datos anónimos según reconoce expresamente su Considerando 26, al afirmar que

> (...) los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Sin embargo, incluso tratándose de datos anónimos, mediante el uso de técnicas como la reagrupación de datos, la IA tiene la capacidad para elaborar el perfil de un individuo o de un grupo a través de la re-identificación, de manera que deberá valorarse "la finalidad del conjunto" de las operaciones que hacen posible el perfilado de una persona o de un grupo, sin que la relevancia de un dato anónimo concreto sea la que determine la aplicación del RGPD al tratamiento de datos personales (Poullet, 2020, p. 51).

En este contexto se plantean ciertas contradicciones internas derivadas de la utilización de los términos de anonimización y de seudonimización. Ciertamente, el RGPD utiliza de modo expreso el concepto de "seudonimización" en su artículo 4.5, definida como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Una seudonimización que, según reconocía el GT 29 en su Opinión sobre las técnicas de anonimización, de 10 de abril de 2014, ha sido objeto de numerosos "equívocos", en tanto que la seudonimización, afirma, "no constituye una técnica de anonimización", sino que, desde el punto de vista

técnico, simplemente "reduce la vinculación de un conjunto de datos con la identidad original del sujeto y, por lo tanto, es una medida de seguridad útil" (GT 29, 2014, 3).

Siguiendo la opinión del GT 29 (2014), la seudonimización consiste en sustituir un atributo (normalmente único) en un registro por otro. En consecuencia, es probable que la persona física siga siendo identificada indirectamente de ahí que la seudonimización, cuando se utiliza por sí sola, no dará lugar a un conjunto de datos anónimos. Ciertamente, según concluye el GT 29, la seudonimización constituye una medida de seguridad útil, "pero no un método de anonimización" (GT 29, 2014, p. 20).

Por su parte, la anonimización constituye el proceso que imposibilita de manera irreversible la re-identificación de los datos personales[20], de modo que la opción del legislador europeo por la utilización del término "seudonimización" en el RGPD no ha hecho sino incrementar las confusiones acerca del procedimiento técnico a aplicar, cuando proceda, a los datos que son objeto de tratamiento.

En todo caso, el GT 29 (2014) hace referencia a diferentes riesgos provenientes de la utilización de técnicas de anonimización.

El primero de ellos consiste en considerar que los datos seudonimizados son equivalentes a los datos anonimizados, pues, técnicamente, los primeros siguen permitiendo que un sujeto de datos individual sea identificado y vinculable a través de diferentes conjuntos de datos. Es probable que la seudonimización permita la identificabilidad y, en consecuencia, se mantiene dentro del ámbito de aplicación del régimen legal de protección de datos (en la actualidad, el RGPD). De este modo, afirma, la seudonimización resulta especialmente relevante "en el contexto de la investigación científica, estadística o histórica" (GT 29, 2014, p. 10)[21].

Un segundo error proviene de considerar que los datos debidamente anonimizados (que quedan fuera del ámbito de aplicación del RGPD), privan a las personas de cualquier tipo de protección, cuando en realidad pueden aplicarse otros actos legislativos al uso de estos datos, como la

---

20. La anonimización también se define en normas internacionales como la ISO 29100, como el "Proceso por el cual la información personalmente identificable (IIP, por sus siglas en inglés) se altera de forma irreversible de tal manera que ya no puede ser identificado directa o indirectamente (ISO 29100:2011).

21. En el contexto de la diferenciación entre seudonimización y anonimización, cabría subrayar que el Auto del Tribunal General de la UE en el asunto T-452/17, de 28 de junio de 2018, desestimó por inadmisibilidad manifiesta el recurso planteado por TL contra el Supervisor Europeo de Protección de Datos, en el que la parte demandante solicitaba la revisión de la Decisión de este último, de 16 de mayo de 2017, por la que denegó la petición de anonimización de la sentencia y de las páginas web que contenían datos personales.

Directiva sobre la privacidad en las comunicaciones electrónicas, que impide el almacenamiento y el acceso a "información" de cualquier tipo (incluida la información no personal) en los equipos terminales sin el consentimiento del abonado/usuario, en el marco de la aplicación del principio de confidencialidad de las comunicaciones[22].

Por último, hace referencia al equívoco consistente en no tener en cuenta, en determinadas circunstancias, el impacto sobre las personas proveniente de los datos debidamente anonimizados, especialmente en el caso de la elaboración de perfiles. La esfera de la vida privada de un individuo se encuentra protegida por el artículo 8 del CEDH y el artículo 7 de la Carta de los Derechos Fundamentales de la UE, y, aun cuando la legislación sobre protección de datos ya no se aplique a los datos anonimizados, el uso que se haga de los mismos por terceros puede dar lugar a una pérdida de privacidad (GT 29, 2014, p. 11)[23].

---

22. El Reglamento (UE) 2019/1150, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (D.O.U.E. L 186, de 11.7.2019), trata de proteger a las pequeñas, medianas y micro empresas, así como a los consumidores, de la posición dominante que adquieren los servicios de intermediación en línea en el comercio electrónico, mediante la garantía de la transparencia de la economía de la plataforma en línea.

23. En el ámbito específico de la telefonía móvil, debe tomarse en consideración, a juicio de De Monjoye *et al.,* (2018), que la mayor parte de los algoritmos de anonimización "son variaciones y mejoras del algoritmo seminal de anonimización k introducido en 1998". Sin embargo, respecto de los datos de la telefonía móvil, estudios recientes han demostrado que la seudonimización y la desidentificación estándar no son suficientes para evitar la reidentificación de los usuarios.
    En opinión de los autores, resulta constatado que cuatro puntos de datos –lugares y horas aproximados en los que estuvo presente una persona–, son suficientes para volver a identificarla de forma exclusiva el 95% de las veces en un conjunto de datos de telefonía móvil de 1,5 millones de personas. Además, las estimaciones de reidentificación mediante el uso de la "unicidad" –una métrica para evaluar el riesgo de reidentificación en conjuntos de datos a gran escala– y los intentos de anonimizar los datos de telefonía móvil mediante k-anonimización, descartaron que la desidentificación fuera suficiente para anonimizar realmente los datos.
    Por ello, consideran que los problemas de privacidad se deben a los "fallos del modelo tradicional de desidentificación y a la falta de un marco moderno y consensuado para el uso de los datos de telefonía móvil por parte de terceros, especialmente en el contexto del Reglamento General de Protección de Datos (RGPD) de la UE".
    Tales técnicas se han desarrollado para el uso anónimo de otros datos sensibles como el censo, las encuestas de hogares y los datos fiscales, respecto de los cuales se ha considerado el impacto social positivo de hacer accesibles estos datos y los medios técnicos disponibles para proteger la identidad de las personas, acordando y aplicando "una solución de compromiso" que, a pesar de no ser perfecta, ha permitido que los datos se utilicen en beneficio de la sociedad. Sin embargo, afirman, hasta la fecha, no se han aplicado estas ideas ni se ha acordado un conjunto de modelos para los datos de los teléfonos móviles.

Más recientemente, en el Informe publicado en marzo de 2022 *Deploying Pseudonimisation Techniques. The case of the Health Sector*, la Agencia Europea para la Ciberseguridad (ENISA), destaca el "valor añadido" de la aplicación de técnicas de pseudonimización al tratamiento de datos relativos a la salud, precisamente, datos que pertenecen a una de las categorías sensibles de datos según el art. 9 del RGPD.

En este sentido, reconoce que la pseudonimización puede resultar una simple "opción" pero también puede formar parte de un complejo proceso, tanto a nivel técnico como organizativo. En cualquier caso, las técnicas de pseudonimización pueden incrementar el nivel de protección de los datos personales que son tratados en el ámbito de la salud (ENISA, 2022, p. 4), apreciación que sería trasladable al tratamiento del resto de categorías enunciadas en el art. 9.1 del RGPD como categorías especiales de datos personales, tales como aquellas que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar unívocamente a una persona, o datos relativos a la vida u orientación sexual de la persona.

Según el citado informe de ENISA, la ventaja más importante de la pseudonimización cuando se aplica correctamente, es ocultar la identidad de un individuo en el contexto de un conjunto de datos específico, de modo que no sea posible relacionar los datos con el individuo concreto, logrando reducir el riesgo de la vinculación de los datos personales de un individuo específico a través de diferentes dominios de procesamiento de datos (ENISA, 2022, 8).

c) El tratamiento de categorías de datos sensibles mediante la IA

Desde luego, la capacidad de poder excluir la identificación del individuo cuando sus datos personales son tratados mediante técnica de IA resulta especialmente importante cuando puedan revelar el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. Un tratamiento de los datos personales explícitamente prohibido por el art. 9.1 del RGPD en tanto que categorías especiales de datos personales.

En este último ámbito juega un papel esencial el tratamiento de datos personales mediante técnicas de IA, como puso de manifiesto el caso

Cambridge Analytica donde, a través de comunicaciones cotidianas y de la respuesta a cuestiones aparentemente carentes de connotaciones políticas por parte de los usuarios de Facebook, una vez tratadas mediante técnicas de IA pueden revelar preferencias de los usuarios individuales.

También cabe subrayar el impacto de la IA sobre los datos biométricos, habida cuenta de la posibilidad, no ya de individualizar sino de reconocer automáticamente a un individuo a partir de sus características físicas, biológicas y conductuales, en tanto que son únicos y permanentes. El concepto de biometría reagrupa un conjunto de datos resultantes del análisis morfológico (huellas digitales, iris, reconocimiento facial, etc.), del análisis biológico (sangre, saliva, ADN, etc.) y del análisis del comportamiento (firma, voz, etc.).

De hecho, resulta significativo que en el contexto de las definiciones aportadas en el art. 3 de la Propuesta de Reglamento (UE) sobre la IA, a partir de la definición de "Datos biométricos", como "aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos", el legislador europeo desglose hasta cinco técnicas diferentes de tratamiento de dichos datos mediante IA:

- "Sistema de reconocimiento de emociones", destinado a "detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos";
- "Sistema de categorización biométrica", dirigido a "asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos";
- "Sistema de identificación biométrica remota", conducente a "identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada";
- "Sistema de identificación biométrica remota en tiempo real", consistente en un sistema de identificación biométrica remota en el que "la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión", y
- "Sistema de identificación biométrica remota en diferido", entendido como todo sistema de identificación biométrica remota "que

> no sea un sistema de identificación biométrica remota «en tiempo real»".

Por ello, resulta posible considerar que la sensibilidad de los datos puede provenir no sólo de la propia naturaleza de los datos personales sino también de la finalidad y del resultado de su tratamiento, aunque los datos personales recogidos y tratados no reciban directamente la calificación de datos sensibles.

En este sentido, como han constatado Edwards y Veale, "las herramientas de IA detectan correlaciones entre diversos atributos no protegidos para llegar a los mismos resultados discriminatorios que si tuviera en cuenta los legalmente protegidos (proxies)". Un ejemplo, afirman, puede ser el uso de la dirección personal, poniendo por caso una zona en la que vive un elevado número de personas afroamericanas y la probabilidad de que se les conceda un crédito, frente la probabilidad de que, en las mismas condiciones, se conceda un crédito a personas que viven en otra zona habitada por población mayoritariamente caucásica (Edwards y Veale, 2018, p. 52).

Estas consecuencias podrían extrapolarse a la selección de candidatos para una vivienda, un empleo o cualquier otro bien o servicio, incluso de carácter esencial, elaborando perfiles de grupos y no sólo de individuos, en cuyo caso, deberían considerarse apropiadas la realización de evaluaciones de impacto según las previsiones contempladas en el art. 35 del RGPD, donde se prevé que "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (...)".

En efecto, la evaluación del impacto de la protección de datos tiene como finalidad evaluar el origen, la naturaleza, la particularidad y la gravedad del riesgo para la privacidad de los datos personales que son objeto de tratamiento. Su resultado (el informe, el plan de acción y su ejecución), debe tomarse en consideración para adoptar las medidas adecuadas que acrediten el tratamiento de los datos personales conforme al RGPD (Considerando 84)[24].

---

24. A este respecto, se ha adoptado el estándar ISO/IEC 29134:2017 (Directrices para la evaluación de impacto sobre la privacidad), como guía de las diferentes fases a través de las cuales debe desarrollarse el estudio de la evaluación de impacto y su informe resultante. Además, al análisis de riesgos resulta aplicable el estándar ISO/IEC 31000:2009 (Gestión

No obstante, la Propuesta de Reglamento (UE) sobre la IA contempla la "Evaluación de la conformidad" como proceso a través del cual se verifica si se cumplen los requisitos establecidos en el título III, capítulo 2, de la Ley de IA en relación con sistemas de IA que suponen un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas.

Concretamente, la Propuesta normativa define un sistema de IA de "alto riesgo" cuando reúna conjuntamente las dos condiciones siguientes (art. 6 de la Propuesta de Reglamento (UE) sobre la IA):

– Que el sistema de IA esté diseñado para utilizarse como elemento de seguridad de productos o en sí mismo constituya un producto de los enunciados en el Anexo II, y
– Que el sistema de IA que constituya un elemento de seguridad de un producto o un producto en sí mismo, deba someterse a una evaluación de la conformidad por un organismo independiente, con carácter previo a su introducción en el mercado o puesta en servicio.

Más concretamente, el Anexo III de la Propuesta normativa incorpora una lista de sistemas de IA considerados de "alto riesgo" atendiendo al hecho de que sus riesgos ya se han materializado o es probable que lo hagan próximamente. Una lista que podrá ser ampliada por la Comisión –a través de la atribución de la capacidad jurídica para adoptar actos delegados que contempla en el art. 7 de la Propuesta–, con el fin de posibilitar la adaptación del Reglamento (UE) al propio desarrollo de las tecnologías de la IA[25].

De este modo, como ha reconocido el Parlamento Europeo en el Proyecto de Informe defendido por el relator Sr. Voss, "no es la IA como tecnología la que se debe regular, sino que el tipo, la intensidad y el momento de la intervención reguladora deben depender exclusivamente del tipo de riesgo que entraña el uso de un sistema de IA", desde la base de que la mayoría de los sistemas son de "bajo riesgo" frente a una minoría que son de "alto riesgo", debiendo adoptarse las salvaguardias legislativas respecto de los últimos, mientras que, respecto de los primeros, son las empresas las

---

de riesgos. Principios y directrices) e ISO/IEC 31010:2009 (Gestión del riesgo. Técnicas de evaluación de riesgos).

25. Entre los contenidos que deberían ser perfilados a lo largo del procedimiento legislativo de la Propuesta de Reglamento (UE) sobre la IA, según la Opinión conjunta adoptada por el Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés) y el Supervisor Europeo de Protección de Datos (EDPS, por sus siglas en inglés), cabría mencionar la garantía de mayor independencia del "Comité Europeo de Inteligencia Artificial" (EAIB, por sus siglas en inglés), así como la previsión de instrumentos de contacto entre los ciudadanos y las empresas respecto de cada sistema de IA (EDPB-EDPS, 2021, p. 3).

que deben "autorregularse" adoptando las medidas que ofrezca los mejores resultados (Voss, 2021, p. 27).

En este sentido, para las tecnologías de IA de "alto riesgo", las "autoevaluaciones de riesgo *ex ante* obligatorias" son equiparables a la marca CE o a las evaluaciones de impacto relativo a la protección de datos, junto a la aplicación de "reglas y normas claras en el mercado" y complementadas con la "evaluación de la conformidad *ex post*", proporcionan un marco de gobernanza suficientemente sólido de la IA, garantizando, en última instancia, la incorporación de "interruptores de parada inmediata" para que la intervención humana pueda detener inmediatamente las actividades automatizadas en cualquier momento (Voss, 2021, p. 29)[26].

5. Conclusiones

El compromiso de la Unión Europea con los valores de la democracia, el Estado de Derecho y los derechos y libertades fundamentales de los ciudadanos ha venido siendo considerado, como no podía ser de otro modo, una *conditio sine qua non* para la adopción del marco normativo de la Unión sobre los sistemas de IA.

Sin embargo, la dificultad para compaginar, de un lado, el liderazgo de la UE en materia de IA, el desarrollo del mercado único de la IA y sus ventajas para los ciudadanos europeos, junto al mantenimiento de los estándares europeos de protección de los derechos y libertades fundamentales, y la consecución de un "efecto Bruselas" en la regulación de las tecnologías de la IA, similar al adquirido por la normativa sobre protección de datos a través de la Directiva 95/46/CE y, actualmente, del Reglamento General de Protección de Datos (RGPD), ha dificultado en el tiempo la adopción de una regulación armonizadora de la UE sobre la IA.

Esta situación de parálisis regulatoria de la UE no ha impedido el desarrollo vertiginoso de los sistemas de IA dando lugar, en la práctica, a la aplicación *de facto* de un modelo regulatorio abstencionista como consecuencia de la inexistencia de una regulación común de la Unión, que ha supuesto su pérdida de liderazgo, tanto en términos de protección de los derechos y libertades de los ciudadanos europeos ante las tecnologías de IA

26. La previsión de "evaluaciones de conformidad", "autoevaluaciones de riesgo *ex ante* obligatorias" y "evaluaciones de la conformidad *ex post*", también podrían entrar en contradicción con la regulación española de la IA contemplada en el artículo 23 de la Ley 15/2022, de 12 de julio, que, siguiendo las previsiones del RGPD, únicamente menciona la realización de "evaluaciones de impacto" respecto de la aplicación de técnicas de IA.

como de competitividad del mercado único europeo en relación con las tecnologías de la IA en términos económicos.

En efecto, habida cuenta de que la actual transformación digital en la que se inserta la IA "ha desencadenado una carrera tecnológica mundial" por determinar el "status de poder político y económico" de la Unión Europea, el *Proyecto de Informe sobre la Inteligencia Artificial en la Era Digital* elaborado por el Parlamento Europeo subraya la necesidad de "actuar urgentemente", en tanto que, para poder seguir siendo competitiva, "la UE debe convertirse en un líder mundial en materia de IA" (PE, 2021, p. 36).

Ciertamente este propósito debe compatibilizarse con el respeto de los principios y valores en los que se fundamenta la UE, entre los que adquiere especial relevancia la Carta de Derechos Fundamentales de la Unión Europea, de modo que esa definición del modelo regulatorio europeo de la IA se convierta, como ha venido sucediendo con la normativa sobre protección de datos personales, en un referente internacional capaz de compatibilizar el ágil funcionamiento del mercado único (y del mercado mundial) con las señas de identidad de la UE.

Desde tales premisas, la Propuesta de Reglamento (UE) sobre la IA constituye la primera regulación general de la IA a nivel mundial, aunque diseña un marco regulatorio de mínimos que tiene por objeto los riesgos derivados del uso de las tecnologías de IA y no la IA en sí misma, tratando de proporcionar una garantía suficiente de los derechos y libertades fundamentales de los ciudadanos europeos, al mismo tiempo que se dota de agilidad al funcionamiento del mercado único europeo sobre la IA.

Se parte, en consecuencia, de una opción regulatoria de carácter horizontal pero deliberadamente selectiva, atendiendo a los riesgos derivados del uso de las técnicas de la IA. En este sentido, diferencia claramente entre las exigencias legalmente establecidas respecto de sistemas de IA de "alto riesgo" a las que se requiere "evaluaciones de conformidad *ex ante*" realizadas por organismos independientes, frente a la autorregulación de los sistemas de IA de "bajo riesgo" (considerados mayoritarios).

Una diferenciación que se completa con la capacidad de la Comisión Europea para actualizar la lista de tecnologías de IA de "alto riesgo", junto a la incorporación de las "evaluaciones de conformidad *ex post*" para las tecnologías de IA de "bajo riesgo", que funcionarían a modo de interruptores de parada inmediata en el supuesto de afectar a los derechos y libertades fundamentales.

La consecución o no del ansiado "efecto Bruselas" por el Reglamento (UE) de IA que resulte finalmente adoptado tras la conclusión del procedimiento legislativo se evidenciará con el transcurso del tiempo, pero, sin duda, la propia existencia de un marco normativo de la Unión sobre la IA

aportará a los ciudadanos europeos mayores garantías de protección de sus derechos y libertades con respecto al uso de tecnologías basadas en ella y controlará el riesgo de una fragmentación regulatoria entre los Estados miembros en esta materia.

Referencias bibliográficas

Asimov, I. (2004). *Yo, robot*. Barcelona: Edhasa.

Barona Vilar, S. (2021). Prólogo. En Barona Vilar, S. (ed.). *Justicia Algorítmica y Neuroderecho. Una mirada multidisciplinar*. Valencia: Tirant lo Blanch.

Barona Vilar, S. (2019). Inteligencia Artificial o la algoritmización de la vida y de la Justicia: ¿Solución o problema? *Revista Boliviana de Derecho*, n.º 28.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, Juanuary-June, 1-12.

Bostrom, N. (1998). How Long Before Superintelligence? *International Journal of Futures Studies*, 2.

Buttarelli, G. Ethics. EDPS. https://edps.europa.eu/data-protection/our-work/ethics_en

Davidson, J.E. y Kemp, I.A. (2011). Contemporary Models of Intelligence. En Sternberg R.J. y Kaufman, S.R., *The Cambridge Handbook of Intelligence* (pp. 54-84). Cambridge Handbooks in Psychology. New York: Cambridge University.

Dumbrava, C. (2021). Artificial Intelligence at EU borders. Overview of applications and key issues. EPRS. *European Parliamentary Research Service*. PE 690.706.

EDPB-EDPS (2021). Joint Opinion 5/2021, on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Edwards, L. y Veale, M. (2017). Enslaving the algorithm? From a 'right to an explanation' to a 'right to better decisions' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, vol. 16.

EGE (2018). *Statement on Artificial Intelligence, Robotics and "Autonomous" Systems*. Luxembourg: Publication Office of the European Union.

ENISA (2022). Deploying Pseudonimisation Techniques. The case of the Health Sector.

EDPS (2021). Decisión on the retention by Europol of datasets lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699).

Evas, T. (2020). European framework on ethical aspects of artificial intelligence, robotics and related technologies. European added value assessment. Study. EPRS. European Parliament Research Service. PE 654.179.

Good, I. J. (1965). Speculations Concerning the First Ultraintelligent Machine. En Franz L.A. y Morris, R. (eds.), *Advances in Computers* (pp. 31-88). Vol. 6. New York: Academic Press. doi:10. 1016/S0065-2458(08)60418-0

Grupo de Trabajo del Art. 29 (2007). Opinion 4/2007, on the concept of personal data (WP 136/01248/07EN).

Grupo de Trabajo del Art. 20 (2014). Opinion 05/2014, on Anonymisation Techniques (WP 216/08/29/14/EN).

High Level Expert Group on AI (AI HLEG) (2019). Ethics Guidelines for Trustworthy AI. https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf.

HM Treasury (2018). The economic value of data: discussion paper.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_ Data.pdf.

How, M-L. (2019). Future-Ready Strategic Oversight of Multiple Artificial Superintelligence-Enabled Adaptive Learning Systems via Human-Centric Explainable AI-Empowered Predictive Optimizations of Educational Outcomes. Big Data and Cognitive Computing, Issue 3.

Jones, Ch. (2020). Automated Suspicion. The EU's new travel surveillance initiatives. Statewatch.

Legg, S. (2008). *Machine Super Intelligence* [Tesis Doctoral]. Universidad de Lugano. http:/ / www. vetta.org/documents/Machine_Super_Intelligence.pdf.

Madiega, T. (2019). EU Guidelines on ethics in artificial intelligence: Context and implementation. EPRS. European Parliament Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data. A Revolution That Will Transform How We Live, Work and Thin*k. London: John Murray.

Mayor, A. (2022). An AI Wake-Up Call from Ancient Greece. April 1, 2022. digi-con.org/an-ai-wake-up-call-from-ancient-greece/.

McCarthy, J., Minsky, M.L., Rochester, N., Shannon, C.E., (1955). A proposal for the Dartmouth Summer Research Projection Artificial Intelligence. www.formal.stanford.edu/jmc/history/dartmouth/dartmouth.html.

Montesinos García, A. (2021). Inteligencia Artificial y ODR. En Barona Vilar, S. (ed.). *Justicia algorítmica y Neuroderecho: Una mirada multidisciplinar*. Valencia: Tirant lo Blanch.

Muehlhauser, L. y Helm, L. (2012). Intelligence Explosion and Machine Ethics. En Eden, A., Søraker, J., Moor, J.H. y Steinhart, E. (eds.). *Singularity Hypotheses: A Scientific and Philosophical Assessment*. Berlin: Springer. [utilizada version parcialmente modificada disponible Machine Intelligence Research Institut: https://intelligence.org/files/IE-ME.pdf?ref=hackernoon.com].

Niu, W. y Brass, J. (2011). Intelligence in Worldwide Perspective. En Sternberg R.J. y Kaufman, S.R., *The Cambridge Handbook of Intelligence* (pp. 623-645)-Cambridge Handbooks in Psychology. New York: Cambridge University.

O'Neil, C. (2016). *Weapons of math destruction. How Big Data increases inequality and threatens democracy*. New York: Crown Publishers.

Polonetsky, J., Tene, O. y Jerome, J. (2015). Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Settings. 13, *Colorado Technology Law Journal*, 333-368.

Poullet, Y. (2020). Éthique et droits de l'homme à l'heure du numérique. Académie Royal de Belgique. Col. Memorial, Bruxelles.

Poullet, Y. (2021). Le RGPD fase aux défis de l'Intelligence artificielle. Larcier-Centre de Recherche Information Droit et Societé (CRIDS). Faculté de Droit de l'UNamur.

Rossi, F. (2016). Artificial Intelligence: Potential Benefits and Ethical Considerations. Policy Department C: Citizens' Rights and Constitutional Affairs. European Parliament. PE 571.380.

Spiekermann, S. (2015). *Ethical IT Innovation. A Value-Based System Design Approach*. Auerbach Publications.

Tosoni, L. (2021). The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*, vol. 11, n.º 2, 145-162.

Van Dijk, N., Casiraghi, S., y Gutwirth, S. (2021). The 'Ethificacition' of ICT Governance. Artificial Intelligence and Data Protection in the European Union. 43, *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2021.105597

Voss, A. (2021). Proyecto de Informe sobre la Inteligencia Artificial en la Era Digital (2020/2266/(INI)). Comisión Especial sobre Inteligencia Artificial en la Era Digital. Parlamento Europeo, 2.11.2021 (PE680.928v01-00).

Walz, A y Firth-Butterfield, K. (2018-2019). Implementing Ethics into Artificial Intelligence: A Contribution, from a Legal Perspective, to the Development of an AI Governance Regime. *Duke Law & Technology Review*, 17, i-231.

Yampolskiy, R.V. y Duettmann, A. (2020). Artificial Superintelligence. Coordination & Strategy. Printed Edition of the Special Issue Published in Big Data and Cognitive Computing. www.mdpi.com/journal/BDCC.