Nº 95
Enero - Abril 2022

INSTITUTO DE DERECHO Y ÉTICA INDUSTRIAL

COMUNICACIONES

EN PROPIEDAD INDUSTRIAL Y DERECHO DE LA COMPETENCIA

IDEI

DOCTRINA • LEGISLACIÓN • JURISPRUDENCIA

FUNDACIÓN CEFI
Centro de Estudios para el Fomento de la Investigación

SECCIONES

ACTUALIDAD · PROPIEDAD INDUSTRIAL
PROPIEDAD INTELECTUAL
PUBLICIDAD · COMPETENCIA · ÉTICA
LEGISLACIÓN Y NOTICIAS

INSTITUTO DE DERECHO Y ÉTICA INDUSTRIAL
Comunicaciones en Propiedad Industrial y Derecho de la Competencia

Comunicaciones en Propiedad Industrial y Derecho de la Competencia es una publicación especializada en Propiedad Industrial, Derecho de la Competencia y Competencia Desleal, aborda también cuestiones como la Publicidad y la Propiedad Intelectual en sus aspectos legislativo, doctrinal y jurisprudencial, así como en sus ámbitos nacional y comunitario europeo e internacional. Se dirige a un público especializado en estas materias (abogados, profesionales de los sectores implicados, docentes universitarios).

Nº 95 Enero-Abril 2022

Directora
Nuria García García
Directora General Fundación CEFI

Consejo de Redacción
· Rais Amils Arnal
Abogada-Socia Pérez Llorca
· Helmut Brokelmann
Abogado-Socio MLAB Abogados.
· Francisco Javier Carrión
Abogado-Socio Eversheds Sutherland.
· Luis Fernández-Novoa
Abogado-Socio Hoyng Rokh Monegier Spain LLP.
· Blas González Navarro
Abogado-Socio Blas A. González Abogados Magistrado en excedencia.
· Antonio Martínez Sánchez
Abogado-Socio Allen & Overy.
· Miquel Montañá Mora
Abogado-Socio Clifford Chance.
· Jesús Muñoz Delgado
Abogado-Socio Gómez Acebo & Pombo.
· Teresa Paz-Ares Rodríguez
Abogada-Socia Uría Menéndez.
· *Carlos Romeo Casabona*
Catedrático de Derecho Penal Universidad País Vasco/EHU y Director del Grupo de Investigación de la Cátedra de Derecho y Genoma Humano.
· Jesús Rubí Navarrete
Vocal Coordinador Unidad Apoyo y Relaciones Institucionales Agencia Española de Protección de Datos.
· *Patricia Zabala Arroyo*
Directora del Departamento de Asesoría Jurídica de Autocontrol.

Patronato CEFI
· María Alonso Burgaz
· Irene Andrés Justi
· Laura Badenes Torrens
· Ana Bayó Busta
· Victoria Fernández López
· Alfonso Gallego Montoya
· Daniel Girona Campillo
· Mª José López Folgueira
· Ana Martín Quero
· Silvia Martínez Prieto
· Fernando Moreno Pedraz
· Bárbara Muñoz Figueras
· Jorge Muñoz Fuentes
· Katia Piñol Torres
· Moisés Ramírez Justo
· Elisabet Rojano-Vendrell
· Pablo Sierra Gracia
· Javier de Urquía Martí

III. PROPIEDAD INTELECTUAL

LA INTELIGENCIA ARTIFICIAL Y SU FUTURO MARCO REGULATORIO

Fecha de recepción: 30 marzo 2022.
Fecha de aceptación y versión final: 6 abril 2022.

Laia Reyes Rico
Asociada Principal Uría Menéndez.

Resumen

En este artículo se analizará la futura regulación transversal de la IA en Europa, haciendo un breve repaso del estado de la cuestión a nivel global con el fin de contextualizar el marco regulatorio europeo. En particular, se desgranarán las principales obligaciones establecidas en el borrador de propuesta de Reglamento europeo sobre IA. Por último, y dada la intrínseca conexión existente entre la IA y la necesidad de compartir y tratar datos (personales o no), se revisará la normativa aplicable a los datos personales desde la perspectiva de la privacidad (como derecho fundamental) y desde el prisma de la gobernanza de los datos (como activos de gran valor).

Palabras Clave

Inteligencia artificial; Reglamento de IA; RGPD 2016/679; datos personales; gobernanza de los datos.

Abstract

This article will analyze the transversal future regulation of AI in Europe, making a brief review of the state of the issue at a global level in order to contextualize the European regulatory framework. In particular, the main obligations established in the proposal for a European Regulation on AI will be detailed. Finally, and given the intrinsic connection between AI and the need to share and process data (personal or not), the regulations applicable to personal data will be reviewed from the perspective of privacy (as a fundamental right) and from the perspective of data governance (as high-value assets).

Keywords

Artificial intelligence; AI Regulation; GDPR 2016/679; personal data and data governance.

1. INTRODUCCIÓN

Gracias al vertiginoso avance de la tecnología y, en particular, de la inteligencia artificial (IA), el mundo está experimentando una gran revolución disruptiva. Ya en el año 1950 el matemático Alan Turing planteó por primera vez que las máquinas podrían *"pensar"*. Años más tarde, en 1997, el sistema de IBM Deep Blue derrotó al campeón de ajedrez Kasparov. Desde entonces, el avance de esta tecnología ha sido exponencial y actualmente los ciudadanos interactúan con sistemas de IA de forma cotidiana.

Para entender los retos de la IA desde un punto de vista jurídico, hay que conocer el proceso técnico subyacente. En este sentido, como punto de partida, cabe aclarar que la IA se compone de "*sistemas que muestran un comportamiento inteligente al analizar su entorno y al realizar acciones, con cierto grado de autonomía, para lograr un objetivo específico*"[1]. Por su parte, el *machine learning* es una técnica de IA "*basada en mecanismos automatizados a través de los cuales los ordenadores pueden adquirir y aprender nuevos conocimientos y, por ello, pueden interactuar sin ser expresamente programados*"[2]. Es decir, los algoritmos[3] de *machine learning* o aprendizaje automático (sin intervención humana) aprenden a *"pensar"*, es decir, a conocer qué pasos han de seguir para resolver una determinada tarea, a partir del análisis previo de inmensas cantidades de datos (personales o no) y de su propia experiencia. Ello implica que, cuando se utiliza *machine learning,* las máquinas no son programadas para seguir unas instrucciones concretas. Por el contrario, son las máquinas las que –de forma autónoma– deciden qué movimientos o procesos han de realizar para ejecutar una tarea.

1. Grupo de Expertos de la Comisión Europea de IA: *A definition of AI: main capabilities and scientific disciplines, the European Commission's High-Level Expert Group on Artificial Intelligence*, 18 de diciembre de 2018 (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december.pdf [Traducción al español de la versión original].

2. Autoridad francesa de protección de datos (CNIL): *The ethical matters raised by algorithms and artificial intelligence*, diciembre de 2017.

3. Autoridad francesa de protección de datos (CNIL): *The ethical matters raised by algorithms and artificial intelligence*, diciembre de 2017 (https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf). En esta guía se definen los algoritmos como "*La descripción de una secuencia finita e inequívoca de pasos o instrucciones para producir un resultado (output) a partir de datos de entrada (input)*" [Traducción al español de la versión original].

En virtud de lo anterior, los algoritmos de aprendizaje automático necesitan *"alimentarse"* de cantidades ingentes de datos (i. e., datos de entrenamiento) para poder extraer sus propias variables y conclusiones y, así, resolver el problema al que se enfrenta la máquina. Cuantos más datos analizan las máquinas, más capacidad tienen para tomar sus propias decisiones. Por ello, la selección de la información de la que se nutren los sistemas de IA es crucial para que el aprendizaje y la toma de decisiones de las máquinas no reproduzcan o agraven los sesgos (raciales o de género) que actualmente imperan en la sociedad. Por otro lado, dado que –tal y como se ha expuesto– son las propias máquinas las que deciden qué procesos y qué decisiones son las más eficientes, el uso de sistemas de IA puede conllevar resultados imprevisibles –y no siempre favorables– para los humanos. A su vez, los criterios que siguen las máquinas pueden resultar excesivamente complejos –incluso para los ingenieros que inicialmente las han programado– y opacos (poco transparentes) para los usuarios que se ven afectados por dichas decisiones. Por ello, la necesidad de regular o controlar la evolución de la IA es de vital importancia con el fin de que esta no pueda afectar de forma negativa a la seguridad (física y psicológica) ni a los derechos fundamentales (en particular, a la dignidad, la privacidad y la no discriminación) de los individuos.

En la actualidad, existen proyectos de IA muy vanguardistas y beneficiosos para la humanidad desarrollados por entidades públicas y privadas en áreas como la investigación biotecnológica, la salud, el transporte, la educación y el cambio climático. Por otro lado, ya se está comercializando tecnología capaz de identificar los sentimientos de las personas, manipular la conciencia de los seres humanos, transportar a pasajeros de forma autónoma y realizar perfiles de usuarios capaces de predecir –con una increíble exactitud– las decisiones que tomarán dichos usuarios en un futuro cercano. Las implicaciones del uso de los sistemas de IA suponen un reto a nivel jurídico, ético y social que han de ser abordados por los legisladores de manera integral sin afectar al progreso de esta gran herramienta.

En este artículo se analizará la regulación –o futura regulación– transversal de la IA en Europa, haciendo un breve repaso del estado de la cuestión a nivel global con el fin de contextualizar el marco regulatorio europeo. En particular, se desgranarán las principales obligaciones establecidas en el borrador de propuesta de Reglamento europeo sobre IA. Por último, y dada la intrínseca conexión existente entre la IA y la necesidad de compartir y tratar datos (personales o no), se revisará la normativa aplicable a los datos personales desde la perspectiva de la privacidad (como derecho fundamental) y desde el prisma de la gobernanza de los datos (como activos de gran valor).

2. EL ENFOQUE JURÍDICO DE LA IA EN EL MUNDO

Actualmente la IA no está regulada –de manera horizontal– en ninguna región del mundo. Los límites del desarrollo y uso de la IA se recogen únicamente en normas sectoriales, directrices éticas y/o códigos de autorregulación generados –en la mayoría de las ocasiones– por las mismas entidades que programan y comercializan esta tecnología. Actualmente, ya son muchos los países que han publicado un listado de principios éticos para marcar los límites de esta super-inteligencia. A nivel global, en noviembre de 2021, la UNESCO[4] publicó unas directrices sobre los principios éticos que debían regir el desarrollo de la IA. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) también emitió una guía[5] con pautas rectoras para guiar el avance de esta tecnología. No obstante, regular cuestiones éticas y jurídicas de la IA de manera transfronteriza es una tarea muy compleja, ya que los principios éticos, morales y jurídicos cambian –de forma radical– de una parte del mundo a otra (dependiendo de las religiones, culturas, nivel de democratización, etc.). Países como China o los EE.UU., que son las naciones a la cabeza de la carrera de la IA –compitiendo por conquistar esta poderosa tecnología–, han optado[6] (por el momento) por no regular el desarrollo de esta tecnología a nivel normativo y se han limitado a publicar ciertas iniciativas, directrices o guías éticas. Sin perjuicio de ello, recientemente China (la Administración de Ciberseguridad de China), en línea con su férreo control sobre las plataformas digitales extranjeras, ha publicado una norma[7] dirigida a fomentar la transparencia de los algoritmos de Internet (incluyendo los algoritmos de recomendación) desarrollados por entidades privadas y a proteger a los menores de una exposición (nociva) a Internet.

En Europa –caracterizada por ser la región líder en el ámbito normativo– ya se está trabajando en una propuesta[8] de Reglamento europeo (el "**Reglamento de IA**") –Ley de Inteligencia Artificial–. El citado borrador de Reglamento de IA fue publicado en abril del año 2021, pero todavía no ha sido aprobado. El proceso de revisión del Reglamento de IA está siendo complejo y todavía no existe una fecha aproximada para su aprobación, pero se esperan modificaciones al actual

4. Unesco: *Recomendación sobre la ética de la inteligencia artificial*, 21 de noviembre de 2021 (Recomendación sobre la Ética de la Inteligencia Artificial - UNESCO Biblioteca Digital).
5. OCDE: *Artificial Intelligence Principles*, 25 de mayo de 2019 (The OECD Artificial Intelligence (AI) Principles - OECD.AI).
6. OCDE: *Artificial Intelligence repository on AI strategies and policies* (OECD AI's live repository of over 260 AI strategies & policies - OECD.AI).
7. Administración de Ciberseguridad chino, 1 de marzo de 2022, disposiciones sobre la recomendación y administración de algoritmos de servicios de información de internet - oficina de la comisión de seguridad cibernética e informatización del comité central del pcch (cac.gov.cn).
8. Comisión Europea: Propuesta de Reglamento de IA (resource.html (europa.eu)).

borrador. Con anterioridad a la publicación de la citada propuesta, la Comisión Europea ya había analizado los riesgos de esta tecnología y, como consecuencia, ya existían varias recomendaciones europeas –que preceden al Reglamento de IA– para lograr que esta tecnología se desarrollase y utilizase en beneficio de los humanos, siendo segura, transparente y ética. En este sentido, en junio de 2018, la Comisión Europea creó el grupo de expertos sobre IA que publicó, en el año 2019, unas Directrices éticas[9] sobre una IA fiable. Además, en el mes de febrero de 2020, la Comisión Europea publicó el Libro Blanco sobre inteligencia artificial[10]. Tanto las Directrices éticas como el Libro Blanco sobre IA son *"los pilares"* sobre los que se ha trabajado para redactar el actual Reglamento de IA.

A nivel nacional, en España, aunque no existe tampoco una regulación específica sobre la IA, el Gobierno ha aprobado una Carta[11] sobre derechos digitales que, aun sin tener carácter normativo, incluye disposiciones innovadoras sobre –entre otras cuestiones– los límites del uso de la IA y los neuroderechos (i. e., los derechos que pretenden proteger a los ciudadanos de tecnologías que puedan afectar a la conciencia o toma de decisiones de los humanos).

Por todo ello, el único proyecto de texto normativo que existe en la actualidad cuyo objeto sea la regulación de la IA de forma transversal es el Reglamento de IA. A continuación se analizarán las principales cuestiones reguladas en dicho Reglamento de IA, como norma pionera en abordar esta tecnología.

3. PROPUESTA DE REGLAMENTO DE IA EN EUROPA

El Reglamento de IA recoge, principalmente y entre otras cuestiones, las obligaciones de proveedores[12] y de usuarios[13] profesionales para poder utilizar o comercializar sistemas de IA categorizados como de *"alto riesgo para la población"* por el propio Reglamento.

9. Grupo de expertos de IA: Directrices éticas para una IA fiable - Publications Office of the EU (europa.eu).
10. Grupo de expertos de IA: LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza - Publications Office of the EU (europa.eu).
11. Gobierno de España: *Carta de Derechos Digitales* (140721-Carta_Derechos_Digitales_RedEs.pdf (lamoncloa.gob.es)).
12. El Reglamento de IA, art. 3.2) incluye una definición de *"proveedor":* "*toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita".*
13. El Reglamento de IA, art. 3.3) incluye una definición de *"usuario":* "*toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional*".

3.1. Ámbito de aplicación material

El punto de partida para analizar el Reglamento de IA es revisar qué se entiende por *"sistema de inteligencia artificial"*. La definición incluida en el Reglamento de IA pretende ser lo más tecnológicamente neutra posible y resistir al paso del tiempo, habida cuenta de la rapidez con la que avanza la tecnología. En este sentido, el Reglamento define el sistema de inteligencia artificial como "*el software que se desarrolla empleando una o varias de las técnicas y estrategias* [que figuran en el anexo I [del Reglamento]] *y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa"*. Es decir, los sistemas de IA objeto de regulación en el Reglamento de IA son aquellos programas de ordenador que emplean técnicas recogidas en el anexo primero del citado Reglamento con el fin de generar resultados (como decisiones o predicciones).

El enfoque adoptado por el Reglamento de IA refleja un notorio esfuerzo por no imponer excesivas cortapisas a la IA y, por ello, el legislador ha optado por un modelo de norma basado en los riesgos. Es decir, dependiendo de los riesgos para la seguridad y los derechos de los ciudadanos derivados del uso de la IA, se imponen más o menos requisitos por parte del Reglamento. En particular, el Reglamento de IA distingue tres categorías de riesgos respecto del uso de la IA: i) inaceptable, ii) alto, o iii) de riesgo bajo o mínimo.

En aras de contextualizar el mercado de la inteligencia artificial predominante en la actualidad, cabe recordar que –en realidad– la gran mayoría de los sistemas de IA presentan un riesgo bajo o mínimo. Ello es debido a que existe un gran número de sistema de IA que no tienen un potencial impacto perjudicial para la sociedad, como por ejemplo la tecnología que ayuda a optimizar la alimentación del ganado o el regadío de los cultivos. Estos sistemas, en principio, no incidirían en la seguridad física de los ciudadanos ni supondrían una potencial afectación a la privacidad, la dignidad o el derecho a la no discriminación de los ciudadanos. De acuerdo con lo anterior, el Reglamento de IA se centra en i) imponer obligaciones a los proveedores y usuarios de sistemas de IA de alto riesgo, ii) prohibir aquellos sistemas de riesgo inaceptable, y iii) recoger ciertas recomendaciones y buenas prácticas sobre el uso de aquellos sistemas de riesgo bajo o mínimo.

Los temas de responsabilidad por el uso de sistemas de IA no son objeto de regulación en el Reglamento de IA. Sin perjuicio de ello, el legislador europeo ha publicado una propuesta[14] de Reglamento (UE) sobre máquinas y está revisando

14. Borrador de Reglamento sobre máquinas: EUR-Lex - 52021PC0202 - EN - EUR-Lex (europa.eu).

la Directiva[15] sobre responsabilidad de producto que complementarán, en cierta medida, al Reglamento de IA abordando cuestiones relacionadas con la responsabilidad civil asociada al uso de sistemas de IA. En relación con la responsabilidad relativa al uso de IA, recientemente, el Comité Europeo de Protección de Datos ha enviado una carta[16] a la Comisión Europea para que la responsabilidad que asumirán los proveedores y los usuarios de IA sea específicamente abarcada y aclarada mediante un instrumento normativo. Por otro lado, en relación con los temas de derecho de la competencia y de protección de datos, el Reglamento de IA hace referencia expresa a que dichas materias están cubiertas por las normas específicas aplicables a dichas materias.

3.2. Ámbito de aplicación territorial

En relación con el ámbito de aplicación territorial del Reglamento de IA, cabe señalar que este será de aplicación de forma extraterritorial, protegiendo, ante todo, a los ciudadanos europeos de sistemas de IA ubicados en la UE con independencia de si los proveedores de dichos sistemas están ubicados en la UE o fuera de ella (en un tercer país, como por ejemplo China o los EE.UU.).

Además, debido al carácter digital y global de la IA, algunos sistemas de IA entrarán también en el ámbito de aplicación del Reglamento de IA si la información de salida (el *output*) afecta a ciudadanos europeos, aunque dichos sistemas no se introduzcan en el mercado ni se utilicen en la UE. Por ejemplo, en los casos en los que una entidad ubicada en España contrate determinados servicios de otra entidad establecida en los EE.UU., en relación con una actividad que lleve a cabo un sistema de IA (ubicado en EE.UU.) que pudiera tener repercusiones para las personas físicas ubicadas en España. En consecuencia, el Reglamento de IA también se aplicará a los proveedores y usuarios profesionales de sistemas de IA establecidos en un tercer país, en la medida en que la información de salida (p. ej., los resultados o decisiones) generada por dichos sistemas de IA se utilice en la UE.

3.3. Sistemas de IA de riesgo alto

Los sistemas de IA categorizados como de *"alto riesgo"* son aquellos sistemas objeto de regulación –por antonomasia– en el Reglamento de IA. Dicho Reglamento de IA los define como aquellos sistemas que acarrean un alto riesgo

15. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31985L0374&from=EN.
16. Comité Europeo de Protección de Datos: *Letter on AI liability*, 22 de febrero de 2022 (edpb_letter_ai_liability_out2022-0009_1.pdf (europa.eu)).

para la salud y la seguridad o los derechos fundamentales de los ciudadanos. En consonancia con un enfoque basado en los riesgos, el Reglamento de IA permitirá los sistemas de alto riesgo en el mercado europeo, siempre que cumplan determinados requisitos obligatorios (impuestos para proveedores y usuarios). Además, los sistemas de alto riesgo deberán ser sometidos a una evaluación de conformidad *ex ante* (antes de ser lanzados al mercado), así como posteriormente y durante toda la vida del sistema de IA. Un sistema de IA se clasifica como de alto riesgo en función de su finalidad prevista –conforme a la legislación vigente relativa a la seguridad de los productos–. La clasificación de un sistema de IA como de alto riesgo no depende únicamente de la función que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se use dicho sistema. En línea con lo antedicho, el Reglamento de IA establece las normas de clasificación y se definen las dos categorías principales de sistemas de IA de alto riesgo:

a) Los sistemas de IA diseñados para utilizarse como componentes de seguridad de productos sujetos a una evaluación de la conformidad *ex ante* realizada por terceros. Los sistemas de IA destinados a ser utilizados como componentes de seguridad de productos regulados por la legislación del nuevo marco legislativo (p. ej., máquinas, productos sanitarios o juguetes) estarán sujetos a los mismos mecanismos de cumplimiento y aplicación *ex ante* y *ex post* que los productos de los que forman parte.
b) Otros sistemas de IA independientes con implicaciones relacionadas principalmente con los derechos fundamentales, los cuales se indican explícitamente en el anexo III del Reglamento de IA. La lista de sistemas de IA de alto riesgo que figura en el anexo III del Reglamento de IA contiene un número limitado de sistemas de IA cuyos riesgos ya se han materializado o es probable que lo hagan próximamente.

Además, el Reglamento de IA prevé que la Comisión Europea pueda ampliar la lista de sistemas de IA de alto riesgo a fin de garantizar que el Reglamento de IA pueda adaptarse a los nuevos usos y aplicaciones de la IA que vayan surgiendo con el avance de esta tecnología.

Por otro lado, el Reglamento de IA también establece los requisitos legales que deben cumplir los sistemas de alto riesgo en lo que se refiere a las siguientes cuestiones: i) los datos y su gobernanza, ii) la documentación y el registro, iii) la transparencia y la comunicación de información a los usuarios, iv) la vigilancia humana, v) la solidez, vi) la precisión, y vii) la seguridad. El texto normativo no impone soluciones técnicas concretas para lograr el cumplimiento de tales requisitos. En consecuencia, dichas soluciones podrían proceder de normas u otras especificaciones técnicas, o bien desarrollarse a discreción del proveedor del sistema de IA de que se trate. Esta flexibilidad reviste una importancia espe-

cial, ya que permite a los proveedores de sistemas de IA decidir cómo quieren cumplir los requisitos, teniendo en cuenta el estado de la técnica y los avances tecnológicos y científicos en este campo.

3.4. Sistemas de IA de riesgo inaceptable

El Reglamento de IA prohíbe expresamente la introducción en el mercado, la puesta en servicio y/o el uso de sistemas de IA que pueda suponer una amenaza para la sociedad. Dado que la IA puede utilizarse indebidamente y proporcionar nuevas y poderosas herramientas para llevar a cabo prácticas de manipulación, explotación y control social, el Reglamento de IA considera que dichas prácticas deben estar completamente prohibidas, ya que van en contra de los valores de la UE de respeto de la dignidad humana, la libertad, la igualdad y la democracia, así como de los derechos fundamentales, como el derecho a la no discriminación, la protección de datos y la privacidad, y los derechos del niño. A continuación se detallan los sistemas de IA expresamente prohibidos en Europa.

3.4.1. *Técnicas subliminales que trascienden la conciencia y manipulación de grupos vulnerables*

Las técnicas subliminales son aquellas que despliegan componentes imperceptibles para el ser humano o son capaces de aprovecharse de las vulnerabilidades de los menores y de ciertos grupos de personas (por razones de edad o incapacidad física o mental). En virtud de lo anterior, el Reglamento de IA no permite la introducción en el mercado, la puesta en servicio o el uso de determinados sistemas de IA destinados a alterar la conducta humana –con altas probabilidades de provocar perjuicios físicos o psicológicos–.

3.4.2. *Evaluación o clasificación de ciudadanos*

Estos sistemas de IA son capaces de evaluar o clasificar la fiabilidad de las personas físicas en función de su comportamiento social en múltiples contextos, de características personales o de su personalidad. Los sistemas de IA que proporcionan calificaciones sociales de personas físicas para su uso con fines generales por parte de las autoridades públicas o en representación de estas pueden menoscabar el derecho a la dignidad y la no discriminación, y los valores de igualdad y justicia. Por ello, el Reglamento de IA prohíbe que las autoridades públicas realicen calificación social basada en IA con fines generales.

3.4.3. *Identificación biométrica de forma remota –en tiempo real– de ciudadanos*

Salvo excepciones limitadas, el uso de sistemas de identificación biométrica remota (como el reconocimiento facial) –en tiempo real– en espacios de acceso público con fines de aplicación de la ley queda prohibido por parte del Reglamento de IA. Los sistemas de identificación biométrica remota son sistemas de IA destinados a identificar a distancia a personas físicas comparando sus datos biométricos (faciales) con los que figuren en una base de datos de referencia, sin saber de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen.

Es preciso distinguir entre los sistemas de identificación biométrica remota *"en tiempo real"* y *"en diferido",* dado que tienen características distintas, se utilizan de manera diferente y entrañan riesgos distintos. En el caso de los sistemas *"en tiempo real",* la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, casi instantánea o, en cualquier caso, sin una demora significativa. Los sistemas *"en tiempo real"* implican el uso de material *"en directo"* o *"casi en directo",* como grabaciones de vídeo generadas por una cámara u otro dispositivo con funciones similares. En cambio, en los sistemas *"en diferido"* los datos ya se han recabado y la comparación e identificación se producen con una demora significativa. Para tal fin se utilizan materiales, como imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado o dispositivos privados, que se han generado antes de aplicar el sistema a las personas físicas en cuestión.

Respecto a la referencia que hace el Reglamento de IA a *"espacio de acceso público"*, el Reglamento se refiere a cualquier lugar físico al que tenga acceso el público, con independencia de si es de propiedad privada o pública. Por consiguiente, esta noción no abarca aquellos lugares de carácter privado a los que, por lo general, no pueden acceder libremente terceros, incluidas las fuerzas o cuerpos de seguridad, a menos que hayan sido invitados o autorizados específicamente (p. ej., viviendas, clubes privados, oficinas, almacenes y fábricas). Tampoco cubre los espacios *online* (virtuales), ya que no son espacios físicos. Es importante aclarar que, de acuerdo con el Reglamento, el simple hecho de que deban cumplirse determinadas condiciones para acceder a un espacio concreto (como, por ejemplo, la adquisición de entradas o las restricciones en relación con la edad) no significa que dichos lugares no sean de *"acceso público"* de acuerdo con el Reglamento. En consecuencia, además de espacios públicos, como las calles, las zonas pertinentes de edificios gubernamentales y la mayoría de las infraestructuras de transporte, normalmente también se consideran de acceso público espacios como cines, teatros, tiendas y centros comerciales. No

obstante, se debe determinar caso por caso si un espacio es de acceso público o no teniendo en cuenta las particularidades de la situación concreta.

De acuerdo con lo anterior, el Reglamento de IA parte de la premisa de que el uso de sistemas de IA para la identificación biométrica remota *"en tiempo real"* de personas físicas en espacios de acceso público con fines de aplicación de la ley invade especialmente los derechos y las libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Además, la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan *"en tiempo real"* acrecientan el riesgo para los derechos y las libertades de las personas afectadas por las actividades de aplicación de la ley.

En consecuencia, el Reglamento prohíbe el uso de dichos sistemas con fines de aplicación de la ley, salvo en tres situaciones enumeradas de manera limitativa y definidas con precisión en las que su utilización es estrictamente necesaria para lograr un interés público esencial cuya importancia es superior a los riesgos que la tecnología presenta. Sin perjuicio de ello, las autoridades de protección de datos[17] han considerado que la prohibición de esta tecnología biométrica –incluida en el Reglamento de IA– es excesivamente laxa y ha instado al legislador europeo a extender dicha prohibición.

3.5. Riesgo bajo o limitado

Como ya se ha adelantado con anterioridad, la gran mayoría de los sistemas de IA pertenecen a esta categoría, en la que las nuevas normas no serán de aplicación porque solo representan un riesgo mínimo para los derechos o la seguridad de los ciudadanos. Esta tipología de sistemas de IA estarán sometidos únicamente a ciertas obligaciones de transparencia y se regirán, en el supuesto de que el proveedor desee adherirse, a determinados códigos de conducta sectoriales. Los sistemas de IA, como los robots conversacionales, que se utilicen para detectar emociones o determinar la asociación a categorías sociales concretas a partir de datos biométricos o generen que manipulen contenido estarán sujetos a unas obligaciones mínimas de transparencia, para que los usuarios que

17. Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos: *Dictamen conjunto 5/2021 sobre la Propuesta de Reglamento de IA*, 18 de junio de 2021 (https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_es).

interactúen con dichos sistemas de IA sean conocedores de que están interactuando con una *"máquina"*.

Una vez analizadas las principales obligaciones recogidas por el Reglamento de IA, se revisarán las implicaciones del tratamiento de datos (personales o no) en el entorno de los sistemas de IA.

4. USO DE DATOS Y SISTEMAS DE IA

A través de los sistemas de IA, como se ha adelantado con anterioridad, se tratan datos tanto para entrenar la eficiencia de los algoritmos como para poder mostrar un resultado (*output*). A través de la mayoría de los sistema de IA se tratan datos categorizados como *"personales",* es decir, información asociable (directa o indirectamente) a una persona física. En dichas ocasiones, los tratamientos están sujetos a las normas de privacidad que protegen al dato como derecho fundamental. Sin perjuicio de ello, el tratamiento que llevan cabo los sistemas de IA no implica siempre un tratamiento de datos personales. En ocasiones los algoritmos tratan información agregada o no referida a personas físicas (p. ej., información financiera relativa a una persona jurídica o información completamente anonimizada) y, por lo tanto, no les será de aplicación la normativa de privacidad.

La normativa de privacidad impone límites estrictos a la cesión de los datos, y ello, aunque favorece la privacidad de los ciudadanos, impide –por otro lado– que el valor del dato (como activo) se explote y se comparta entre las entidades y en beneficio de la sociedad (que, en realidad, es a quien pertenecen y quien los genera). Actualmente, el dato personal presenta dos *"caras"* de una misma *"moneda":* la de *"derecho fundamental"* (que es el enfoque recogido por las normas de privacidad) y la de *"activo"* (que es el tratamiento dado por las entidades y, cada vez más, por los propios ciudadanos).

El legislador europeo, conocedor de estas restricciones y –a su vez– del potencial que tienen los datos como *"activo",* ha aprobado dos propuestas de normas sobre la gobernanza de los datos, que pretenden establecer estándares y mecanismos para hacer posible que los datos se puedan ceder y, así, incrementar el valor del dato como *"activo"*.

De acuerdo con todo lo anterior, seguidamente se repasarán, en primer lugar, las normas de privacidad aplicables al tratamiento de datos en el entorno de sistemas de IA y, en segundo lugar, las dos propuestas de normas de gobernanza de los datos.

4.1. Normas de privacidad

Los datos personales, como derecho fundamental, están protegidos por la normativa de protección de datos, esto es, el Reglamento General de Protección de Datos 2016/679 (el "**RGPD**") y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (la "**Ley Orgánica 3/2018**").

Los tratamientos más comunes en el contexto de los sistemas de inteligencia artificial son, por un lado, la anonimización o seudonimización de datos personales y, por otro lado, los perfilados y la toma de decisiones automatizadas. Por ello, a continuación, se analizarán sucintamente dichos tratamientos.

4.1.1. *Anonimización vs. seudonimización*

La anonimización o la seudonimización de datos personales ha de llevarse a cabo de acuerdo con la normativa de protección de datos. Con fines aclaratorios, cabe destacar que los datos anonimizados no tienen el mismo régimen que los datos seudonimizados. Los datos anonimizados son aquella información que no permite reidentificar a la persona física a la que pertenecen (p. ej., las chicas de 30 a 35 años acceden a las redes sociales desde sus *smartphones* con mayor frecuencia que desde sus ordenadores portátiles). Sin embargo, los datos seudonimizados[18] son aquellos que sí permiten –aunque sea de forma indirecta– reconocer a la persona física a la que pertenecen (p. ej., el cliente 495 suele acceder a las redes sociales desde su *smartphone*, y con dicho código se podría llegar a una identificación). Esta distinción es sumamente importante, ya que el RGPD establece que a la información agregada o anonimizada no le es de aplicación la normativa de protección de datos, mientras que a la seudonimizada, sí. No obstante, ello no quiere decir que exista un *"cheque en blanco"* para anonimizar los datos y tratarlos con los fines que una compañía desee. Al respecto, la Agencia Española de Protección de Datos (la AEPD) ha puntualizado en repetidas ocasiones que la anonimización es un tratamiento en sí mismo[19]. Ello implica que las

18. El RGPD define en su art. 4.5. la seudonimización 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*".

19. El Informe 195/2017 de la AEPD, sección VIII, señala lo siguiente respecto a los procesos de anonimización y de pseudonimización: "[...] *tanto la anonimización como la seudonimización de los datos personales llevarán aparejada la existencia de dos tratamientos sucesivos: el que supone la propia anonimización o seudonimización a partir de los datos personales de que dispone el responsable y el que se lleve a cabo posteriormente con los datos ya anonimizados o seudonimizados.* ***La diferencia entre ambos supuestos estribará en el hecho de que mientras la normativa de protección de datos no será de aplicación a este segundo tratamiento si los datos han sido anonimizados, sí resultará aplicable en caso de que se haya producido únicamente una seudonimización*****".**

compañías necesitan una base jurídica para anonimizar dichos datos e informar a los afectados sobre el tratamiento en todo caso[20].

Además, la AEPD publicó una guía[21] sobre los procesos de anonimización en la que se concluía que, dada la rápida evolución de la tecnología, hay que tener en cuenta que los procesos realizados pueden no ser definitivos e irreversibles. Por ello, la AEPD recomienda que los procesos de anonimización sean revisados periódicamente y se evalúen (incluso realizando evaluaciones de impacto) los posibles nuevos riesgos que puedan surgir como consecuencia de diferentes factores, riesgo residual de datos anonimizados, nuevas fuentes de datos a cruzar, nuevas tecnologías, etc.[22]

Por lo tanto, partiendo de la asunción de que el proceso de anonimización no puede asegurar la imposibilidad de reidentificación de las personas en términos absolutos, se deben implementar las garantías jurídicas necesarias para preservar los derechos de los interesados[23]. En este sentido, algunos de los aspectos que deben tener en cuenta las compañías, tal y como recomienda la AEPD, son los siguientes[24]: la suscripción de acuerdos de confidencialidad y un contrato entre el responsable del tratamiento originario y el destinatario de la información anonimizada.

20. El Informe195/2017 de la AEPD, sección VIII, señala lo siguiente respecto al deber de informar en los procesos de anonimización y de pseudonimización: "*En todo caso, como se ha indicado para los supuestos anteriormente indicados, será preciso informar a los interesados acerca de los tratamientos que van a tener lugar y garantizar el adecuado ejercicio por aquéllos de su derecho de oposición, al operar éste, según el artículo 21 del reglamento, en los supuestos en que el tratamiento se funde en la regla del equilibrio de derechos e intereses prevista en el artículo 6.1 f) del reglamento*".

21. AEPD: *Orientaciones y garantías en los procedimientos de anonimización de datos personales* (la *"Guía de Anonimización"*) (https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf).

22. La AEPD en su Código de Big Data, sección IV.4. (pág. 30), dice lo siguiente: "*Se deben* ***establecer medidas adicionales de seguridad en todos los elementos que intervienen en el proceso de la anonimización, como auditorías periódicas de las fuentes de información, de los canales de transmisión de la información, de las localizaciones físicas de las fuentes de información, etc****., aplicando los estándares, sellos y buenas prácticas en seguridad y privacidad de la información.* ***Este marco integral debería incluir un procedimiento de detección y notificación de posibles brechas de privacidad que pudieran surgir, como casos de re-identificación***".

23. En la Guía de Anonimización, sección 8 (pág. 24), la AEPD indica que "***No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas****, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen. Es recomendable la adopción de códigos de conducta en las organizaciones para facilitar la aplicación de la legislación vigente, así como la obtención de certificaciones, sellos o etiquetas que permitan demostrar a terceros su adecuado cumplimiento, de forma que la privacidad se pueda convertir en valor referencial de las mismas*".

24. Guía de Anonimización de la AEPD, sección 5 (págs. 21 y 22).

4.1.2. *Perfilados y decisiones automatizadas*

Los perfilados y las decisiones automatizadas son una categoría de tratamientos de datos intrínsecamente relacionada con los sistemas de IA.

El punto de partida debe ser conocer qué actividades implican la elaboración de perfiles y las decisiones automatizadas y, en consecuencia, que las compañías que utilizan sistemas de inteligencia artificial puedan identificar cuándo deben adoptar, además de todas las obligaciones impuestas por la normativa de protección datos, las garantías específicas para esta tipología de tratamientos que exige el RGPD en materia de transparencia, información y limitación de su uso.

El concepto de perfilar o de crear perfiles sobre personas físicas se define en el RGPD como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*". De acuerdo con dicha definición, el perfilado es una categoría de tratamiento de datos que tiene lugar si concurren estos dos requisitos: que el tratamiento de datos se lleve a cabo de forma automatizada y que dicho tratamiento tenga por objeto evaluar a una persona física o a un grupo de individuos.

Tratar un dato de forma automatizada implica procesar dicho dato con herramientas tecnológicas, por ejemplo a través de algoritmos de *machine learning*. Cabe aclarar que, dado que el RGPD no exige que el perfilado conlleve un tratamiento *"únicamente"* automatizado, la participación humana en el proceso de perfilado no determina la inexistencia de una elaboración de perfiles.

Por su parte, el término *evaluar* implica hacer un juicio sobre una persona o hacer predicciones o sacar conclusiones sobre una persona, aspectos personales de una persona física. En este sentido, la mera clasificación de las personas por características como, por ejemplo, la ciudad de residencia, edad o sexo no implicaría necesariamente la elaboración de un perfil. La elaboración de perfiles conlleva crear *"nuevos"* datos personales que no han sido directamente facilitados por los propios interesados, con el fin de hacer predicciones o deducciones estadísticas sobre su capacidad de realizar una tarea, sus intereses o su comportamiento futuro.

Una vez aclarado qué es perfilar, cabe señalar que –tal y como se indicaba anteriormente– existe otra actividad muy común en el ámbito de los sistemas de inteligencia artificial: la toma de *"decisiones automatizadas",* que en ocasiones se confunde con el perfilado. No obstante, la adopción de decisiones automatizadas tiene un ámbito de aplicación distinto al del perfilado. En particular, las

decisiones automatizadas son las acciones adoptadas a través de medios tecnológicos sin la participación de seres humanos. Las decisiones automatizadas pueden llevarse a cabo con o sin la elaboración de perfiles, y la elaboración de perfiles, a su vez, puede no conllevar la toma de decisiones automatizadas. Por ejemplo, una decisión automatizada sería la concesión de un determinado préstamo a un cliente o un bonus a un empleado por alcanzar determinados requisitos tasado. En el ámbito del *marketing*, la inclusión de publicidad comportamental *online* sería un ejemplo de decisión automatizada. Estas decisiones, de forma automática, no implicarían la elaboración de un perfil del usuario. Sin embargo, si durante dos años se monitorizan los productos y servicios financieros contratados por un cliente (i. e., se perfila) y dicha información se junta con otro tipo de información financiera de dicho usuario con el fin de elaborar un perfil de solvencia muy exhaustivo, la concesión del préstamo sí supondría la adopción de decisiones automatizadas basadas en el perfil del usuario. Por lo tanto, en este último caso, sí tendría lugar la generación de un perfil.

Las normas de privacidad establecen una prohibición general con el fin de que las compañías no implementen mecanismos en los que sea un algoritmo únicamente (sin intervención humana) el que tome una decisión o elabore un perfil, y que dichas decisiones o perfilados tengan efectos jurídicos en los usuarios o que "*les afecte significativamente de modo similar*". No obstante, dicha regla general acepta excepciones (como que el afectado otorgue su consentimiento expreso), siempre que se implementen garantías adicionales establecidas en el RGPD. Además, el RGPD concede el derecho a los usuarios a obtener intervención humana por parte de las entidades que tratan los datos con sistemas automatizados de IA, a expresar su punto de vista y a impugnar las decisiones tomadas por las máquinas. Además las entidades que lleven a cabo decisiones automatizas y elaboren perfiles deben, como regla general, realizar evaluaciones de impacto (*privacy impact assessment*) y facilitar a los usuarios información significativa sobre la lógica aplicada por los algoritmos, así como la importancia y las consecuencias acerca de dicho tratamiento previstas para los afectados.

En este sentido, cabe preguntarse si en determinados sectores relacionados con el uso de sistemas de IA –como por ejemplo el sector del *marketing*– se toman decisiones automatizadas o se elaboran perfiles basados únicamente en tratamientos automatizadas que "*tengan efectos jurídicos*" en los usuarios o que les "*afecten significativamente de modo similar*". Respecto del primer supuesto, resulta difícil –al menos actualmente– pensar que pueda ser de aplicación en el sector de la publicidad. No obstante, las autoridades de datos han llamado la atención sobre la posibilidad de que –aunque excepcionalmente– ciertas decisiones o elaboraciones de perfiles automatizadas (sin intervención humana) puedan tener "*efectos significativamente similares*" en las personas. Para discernir

si existe dicho riesgo, las autoridades de datos indican que se han de tener en cuenta los siguientes factores : i) el nivel de intrusismo del proceso de elaboración de perfiles, incluido el seguimiento de las personas en diferentes sitios web, dispositivos y servicios; ii) las expectativas y deseos de las personas afectadas; iii) la forma en que se presenta el anuncio; o iv) el uso de conocimientos sobre las vulnerabilidades de los interesados.

En relación con ello, las autoridades de datos advierten de que un tratamiento que pueda tener poco impacto sobre las personas en general podría tener un efecto significativo en determinados grupos de la sociedad, como grupos minoritarios, adultos vulnerables o niños. Es más, en el caso de estos últimos, las autoridades de datos hacen especial hincapié en que pueden ser especialmente susceptibles e influenciables en el entorno en línea, particularmente respecto de la publicidad comportamental. Por ello, las autoridades de datos concluyen, a este respecto, que las compañías deberán abstenerse en general de elaborar perfiles sobre los niños con fines de publicitarios.

4.2. Normas de gobernanza de los datos

Con independencia de la relevancia de las normas de privacidad, en la actualidad, el volumen de datos –tanto personales como no personales– que generan y recogen los ciudadanos, las entidades privadas y los organismos públicos es ingente y sigue creciendo de manera exponencial gracias al avance de las tecnologías emergentes. En el año 2025 se prevé, de acuerdo con datos aportado por la Comisión Europea, que el volumen de datos aumente a 115 zettabytes. El diagnóstico de la Unión Europea es, sin embargo, que el potencial de los datos –como activo– está insuficientemente explotado. Los datos podrían utilizarse para innovar, investigar y hacer más eficientes las nuevas tecnologías. Para poner fin a esta carencia e impulsar la competitividad en Europa y su transformación digital, el legislador europeo considera necesario explotar los datos de forma más eficiente, segura y homogénea dentro de la Unión. Para ello, los datos deberían estar disponibles para ser intercambiados y reutilizados con fines lícitos, como los de investigación o innovación.

No obstante, existen diversos obstáculos a la creación de un ecosistema para que los datos circulen y se intercambien con facilidad a nivel europeo. Desde una perspectiva legal, por ejemplo, existen límites a la cesión de ciertos datos, como en los casos en los que están protegidos por derechos de terceros (derechos de propiedad intelectual, de protección de datos o de confidencialidad comercial, etc.). Por otro lado, existen impedimentos técnicos y operativos que complican su compartición e interoperabilidad y, además, no hay incentivos a nivel europeo que compensen los intereses económicos particulares (de los ciudadanos o las

entidades privadas) de mantener la *"titularidad"* de la explotación sobre dichos datos. Estos y otros factores son los que han generado la actual infrautilización de los datos a nivel europeo.

La Unión Europea, hecho el diagnóstico, y con el fin de crear un mercado europeo de datos (tanto personales como no personales) homogéneo, transparente y neutral ha hecho públicas –como parte de la Estrategia Digital Europea–una propuesta de Reglamento[25] (UE) sobre la gobernanza de los datos (*Data Governance Act*) –Reglamento de Gobernanza– y una propuesta de Reglamento[26] sobre la ley del dato (*Data Act*) –Reglamento de Datos–. No es el único intento normativo en este sentido en Europa y en España, puesto que ya existen normas sobre intercambio y explotación de datos de organismos públicos, conocidas como normativa de datos abiertos u *open data* (i. e., la Directiva (UE) 2019/1024[27] y la Ley 37/2007[28]). No obstante, estas dos propuestas de Reglamentos pretenden dar un paso más y fijar los parámetros básicos para que el intercambio de datos se promueva y para que se genere un mercado único de datos.

4.2.1. *Reglamento de Gobernanza*

A efectos de sintetizar las principales novedades introducidas por la propuesta de Reglamento de Gobernanza, los conjuntos de medidas se pueden dividir en tres grandes bloques.

El primer grupo de medidas regula las pautas básicas para que los organismos públicos puedan poner a disposición del mercado datos que obran en su poder y que están protegidos por derechos de terceros. El propósito es que sean reutilizados por personas físicas o jurídicas incluso con fines comerciales. Para ello, y entre otras estrategias, se propone implementar técnicas de anonimización o seudonimización antes de compartir los datos personales con el fin de asegurar la protección que confieren otras normas a los titulares de dichos datos bajo el RGPD.

En segundo lugar, la propuesta de Reglamento de Gobernanza crea la figura de los proveedores de servicios de intercambio de datos, como intermediarios que aceleren el intercambio de datos entre entidades privadas o de personas físicas a entidades privadas. Los proveedores de este tipo de servicios estarán suje-

25. Reglamento de Gobernanza de los Datos: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0767&from=ES.

26. Reglamento de Datos: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.

27. Directiva (UE) 2019/1024: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019L1024&from=ES.

28. Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.: https://www.boe.es/buscar/doc.php?id=BOE-A-2007-19814.

tos a una serie de reglas de notificación, supervisión y sanción para garantizar la confianza de las entidades y los ciudadanos en esta figura de intermediarios y permitir así la creación y crecimiento de un mercado único de datos europeo.

En el tercer bloque de propuestas se diseña un marco para posibilitar la cesión de datos voluntaria con fines altruistas, sin ánimo de obtener gratificaciones y en beneficio del interés general (como la investigación científica o la mejora de servicios públicos). Para fomentar esta tipología de cesiones, la propuesta de Reglamento de Gobernanza regula la figura de las organizaciones de gestión de datos con fines altruistas, que es una figura de intermediación en este tipo de cesiones de datos, y para las que prevé un registro público, requisitos de transparencia y operativa y un régimen de supervisión. También se prevé la aprobación de un formulario de consentimiento para que los interesados autoricen el uso de sus datos. De nuevo, la norma pretende crear una serie de figuras e instrumentos que generen confianza a los ciudadanos y a las entidades, de forma que se fomente el intercambio de datos también con fines altruistas.

Mientras que el Reglamento de Gobernanza establece los procesos y estructuras para facilitar el intercambio de datos por parte de las empresas, los particulares y el sector público, el Reglamento de Datos aclara quiénes pueden generar valor a partir de los datos y en qué condiciones.

4.2.2. *Reglamento de Datos*

La propuesta de Reglamento de Datos incluye, principalmente, medidas que permitan a los usuarios de dispositivos conectados acceder a los datos generados por ellos, que suelen recoger exclusivamente los fabricantes, e intercambiarlos con terceros para prestar servicios de posventa u otros servicios innovadores basados en datos. Mantiene incentivos para que los fabricantes sigan invirtiendo en la generación de datos de alta calidad al cubrir sus costes relacionados con la transferencia y excluir el uso de datos intercambiados en competencia directa con sus productos.

Por otro lado, el Reglamento de Datos establece medidas para reequilibrar el poder de negociación de las pymes mediante la prevención del abuso de los desequilibrios contractuales en los contratos de intercambio de datos. Además, el Reglamento de Datos regula los medios para que los organismos del sector público obtengan y usen datos en poder del sector privado que sean necesarios en circunstancias excepcionales, especialmente en caso de emergencias públicas (como inundaciones e incendios forestales), si los datos no están disponibles de otro modo. La información sobre los datos es necesaria para responder con rapidez y seguridad, a la vez que se reduce al mínimo la carga para las empresas.

Las nuevas normas permitirán a los clientes cambiar efectivamente de proveedores de servicios de tratamiento de datos en la nube y establecer salvaguardias contra la transferencia ilícita de datos. En este sentido, los consumidores y las empresas podrán acceder a los datos de su dispositivo y utilizarlos para servicios posventa y de valor añadido, tales como el mantenimiento predictivo.

Aunque la aprobación de los instrumentos anteriormente descritos ayudará a impulsar la circulación de los datos (al menos, por parte de los organismos públicos), las propuestas de Reglamentos suscitan ciertos retos en términos prácticos. El establecimiento de requisitos formales como los de notificación, registro o régimen de supervisión (recogido en el Reglamento de Gobernanza) aportará seguridad y confianza a este mercado, pero, por otra parte, puede generar algunas trabas a su desarrollo si esos requisitos no se materializan de la forma adecuada. Lo cierto es que ya existen operadores en el mercado que intermedian en el intercambio de datos, sin una regulación específica. Lo que es claro es que, con estas dos propuestas, la Unión Europea identifica y pretende abordar un reto en el que la región entera se juega mucho: el uso eficiente de los datos como motor de la nueva sociedad y economía.

5. CONCLUSIONES

El avance incuestionable de la tecnología y, en particular, de la IA ha suscitado la necesidad de que el legislador europeo se posicione como líder (y pionero) a nivel global en regular –de forma transversal– la IA. En particular, la Comisión Europea ha publicado una propuesta –pendiente de aprobación– de Reglamento sobre IA que aborda principalmente los requisitos que proveedores y usuarios profesionales deberán acatar para poder comercializar y utilizar sistemas de IA categorizados como de *"alto riesgo"* por el propio Reglamento. Además, el Reglamento de IA prohíbe expresamente el uso de herramientas con IA con ciertas finalidades que podrían menoscabar los derechos fundamentales de los ciudadanos de la UE.

Por otro lado, el uso de sistemas de IA está intrínsecamente relacionado con el uso de datos (personales o no), tanto para entrenar a los algoritmos como para ser analizados por los sistemas de IA para producir un resultado (*output*). Sin perjuicio de que cualquier tratamiento de datos personales estará sujeto a la normativa aplicable sobre privacidad, el legislador europeo está tomando conciencia del valor del dato como activo. De ahí que, recientemente, la Comisión Europea haya publicado dos propuestas de Reglamentos sobre la gobernanza de los datos con el fin de flexibilizar la compartición de datos entre entidades y que el beneficio de su explotación pueda revertir, en última instancia, en el conjunto de la sociedad.

ISSN: 1579-3494

40 Aniversario
FUNDACIÓN CEFi
Centro de Estudios para el Fomento de la Investigación