Raúl Jiménez Martínez

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS

TRABAJO DE FIN DE GRADO

Dirigido por: Prof. Dr. Juan Pablo Gonzales Bustos

Grado en Derecho

UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2021

El TFG se ha desarrollado en la modalidad de:

- ☐ Trabajo de investigación

La investigación se presenta siguiendo las normas para autores prevista en la Revista Española de Seguros.

http://seaida.com/revista-espanola-de-seguros/normas-para-la-presentacion-de-originales/

RESUMEN

La Inteligencia Artificial está cada vez más presente en nuestra vida cotidiana. El objetivo de este trabajo es examinar el impacto de esas tecnologías en los derechos y libertades de las personas, en especial al Derecho a la Protección de Datos. A través del análisis de la normativa vigente se expondrán las principales causas por las que, actualmente, no podamos afirmar que en Europa se garantiza el Derecho a la Protección de Datos.

Inteligencia Artificial	Algoritmo	Protección de datos	Intimidad	Unión Europea

RESUM

La Intel·ligència Artificial està cada vegada més present en la nostra vida quotidiana. L'objectiu d'aquest treball és examinar l'impacte d'aquestes tecnologies en els drets i llibertats de les persones, especialment al Dret a la Protecció de Dades. A través de l'anàlisi de la normativa vigent s'exposaran les principals causes per les quals, actualment, no puguem afirmar que a Europa es garanteix el Dret a la Protecció de Dades.

Intel·ligència Artificial	Algoritme	Protecció de dades	Intimitat	Unió Europea

ABSTRACT

Artificial Intelligence is increasingly present in our daily lives. The aim of this paper is to examine the impact of these technologies on people's rights and freedoms, especially the Right to Data Protection. Through the analysis of the current regulation, we will explain the main reasons why, currently, we cannot claim that the right to data protection is guaranteed in Europe.

Artificial Intelligence	Algorithm	Data protection	Privacy	European Union

Índice

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
CE	Constitución Española
Cit.	Citado
Dir.	Dirigido
DNI	Documento Nacional de Identidad
Edit.	Editado
IA	Inteligencia Artificial
IBIDEM	Cita inmediatamente anterior, mismo documento y misma página
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
Pág. / págs.	Página/Páginas
PYMES	Pequeñas y medianas empresas
RGPD	Reglamento General de Protección de Datos
STC	Sentencia del Tribunal Constitucional
UE	Unión Europea

INTRODUCCIÓN

En las últimas décadas, los avances tecnológicos han transformado nuestra sociedad de una forma transversal, se podría afirmar que vivimos en una sociedad digital. Este fenómeno es posible gracias a que la tecnología, internet y los dispositivos inteligentes, han adquirido un papel disruptivo en la sociedad, han revolucionado la comunicación, el entretenimiento, el comercio, la educación, la sanidad, el trabajo, la industria e incluso la organización y funcionamiento de las administraciones públicas. La actual crisis provocada por la pandemia de la Covid 19 ha acelerado más, si cabe, la adaptación del ser humano a los entornos digitales, obligándolos a utilizar herramientas digitales para llevar a cabo tareas que antes de la pandemia se realizaban de forma física o presencial. Ha supuesto desde la implementación del teletrabajo, a un cambio de la forma de comprar y consumir bienes y servicios, a la implementación de la educación *online,* o a la forma de relacionarnos con las administraciones públicas, por citar algunos ejemplos.

Los avances tecnológicos han permitido la creación, perfeccionamiento e implementación de la Inteligencia Artificial. Esta tecnología está presente en todos los sectores de nuestra sociedad y ofrece tanto a las personas, las empresas, como a las administraciones públicas unas posibilidades nunca vistas antes.

Dada la universalización de estos sistemas, cada vez más presentes en nuestra vida cotidiana, y ante la perspectiva de que en un futuro cercano su perfeccionamiento e implementación total va a suponer un cambio del paradigma socioeconómico de nuestra sociedad, conviene preguntarse cómo afecta su uso a los derechos y libertades de las personas, en especial al derecho de protección de datos, dado que operan en entornos digitales, qué obligaciones tienen las empresas que operan con estos sistemas, y si el marco jurídico actual es capaz de dar la cobertura necesaria para minimizar los riesgos que se derivan de su uso.

Para dar respuesta a esas cuestiones, el presente trabajo tiene por objeto identificar los beneficios y riesgos de la inteligencia artificial, explicar el papel que juega el derecho a la protección de datos en estos sistemas y analizar la normativa europea, para ver que derechos tienen las personas, que obligaciones y límites tienen las empresas que tratan los datos personales, que sucede en caso de incumplimiento de la normativa y si ésta es suficiente para salvaguardar los derechos fundamentales y mitigar los riesgos para la protección de datos que supone el uso de la inteligencia artificial.

Todo ello a través de la explicación y contextualización del concepto, tipos y usos de la inteligencia artificial, los riesgos para la ética, la moral y la intimidad de las personas, así como el alcance y el contenido del derecho a la protección de datos personales, y el análisis y la adecuación de estos sistemas a la normativa europea. Para realizar un análisis académico de todas estas cuestiones, serán utilizadas tanto bibliografía especializada, como jurisprudencia, dictámenes y resoluciones de autoridades competentes en materia de protección de datos, como normativa.

1. INTELIGENCIA ARTIFICIAL

1.1. Concepto y características

A pesar de la importancia y la vigencia de la inteligencia artificial (en adelante, IA) en nuestras vidas y el más que probable impacto transversal que tendrá en la sociedad, aún no existe una definición universal de lo que se entiende por IA. Esto no plantea solo un problema semántico y conceptual, sino que se traduce en un problema jurídico en el momento en el que se plantea implementar una legislación que regule y delimite el ámbito de actuación de estos sistemas, ya que para ello es imprescindible determinar el objeto que se va a someter a regulación.

No obstante, y a pesar de la falta de consenso de una definición universal y al amplísimo abanico de sistemas que entran dentro de la categoría de IA, sí que es posible hacer una aproximación general bastante precisa a su concepto.

La Unión Europea (en adelante, UE) ha definido la IA como aquellos sistemas que manifiestan un comportamiento inteligente, son capaces de analizar su entorno y actuar de forma autónoma con el fin de alcanzar objetivos específicos[1], eso incluye tanto programas informáticos como podría ser el asistente por voz Siri o Alexa, al igual que dispositivos de *hardware* como un robot.

De acuerdo con esta definición, la diferencia entre un programa informático normal y una IA, es que en el primero el sistema ya tiene una respuesta determinada para una acción concreta y, en el segundo, en cambio, la respuesta no está predeterminada, sino que será el programa de forma autónoma o inteligente quien elabore y de una respuesta ante una determinada acción. Como se observa, la principal característica de los sistemas de IA es que son capaces de simular la inteligencia humana y, a partir de esa inteligencia, resolver problemas o realizar tareas de forma independiente, no solo están programadas para resolver los problemas sino para aprender a resolverlos por si mismos sin intervención humana[2]. Hay distintos tipos de IA y distintos grados de autonomía de los mismos, que serán analizados en el apartado siguiente cuando veamos los diferentes tipos de IA.

Todos ellos, sin embargo, para simular la inteligencia humana y actuar como lo haría un ser humano, reúnen tres características: la dependencia de datos, la conectividad y la

[1] COMISIÓN EUROPEA, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa. COM (2018) 237 final, Bruselas, 25.4.2018, pág. 1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES

[2] ONU, Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. CNUDMI/UNICTRAL. Aspectos jurídicos de los contratos inteligentes y la inteligencia artificial. Presentado por Chequia, New York, 25/06/2018, pág. 2. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V18/037/81/PDF/V1803781.pdf?OpenElement

autonomía, a través de las cuales pueden incluso mejorar su rendimiento aprendiendo de la experiencia[3].

Respecto a la dependencia de datos, éstos son una herramienta esencial en la que se apoyan estos sistemas, pues son imprescindibles para su funcionamiento. Podemos clasificar a grandes rasgos dos tipos de datos: los estructurados y los no estructurados. En los primeros podemos incluir información menos compleja, como números, fechas o direcciones; mientras que en los segundos incluyen datos más complejos como vídeos, imágenes o textos[4]. Para que los sistemas de IA realicen correctamente la función para la que han sido creadas y no genere daños o lesiones se requiere exactitud y pertinencia en los datos[5].

La conectividad requiere a estos sistemas estar conectados a internet, a bases de datos u otros dispositivos de forma permanente. Lo cual exige una evaluación del riesgo integral y unos sistemas de seguridad reforzados, bien ante posibles interferencias externas como la piratería, o bien ante un mal uso previsible que pueda ocasionar una amenaza para los usuarios[6].

La autonomía les permite realizar acciones o predicciones por sí mismos, al igual que aprender, razonar y llegar a conclusiones e, incluso, autocorregirse a partir de una base de datos, de forma autónoma, con una mínima intervención o, incluso, sin supervisión humana. Pero estos sistemas de IA necesitan herramientas que les permitan tratar y procesar los datos. Esas herramientas son los algoritmos, que se definen como "un conjunto de instrucciones secuenciales precisas, ordenadas, definidas, finitas y aptas para obtener un concreto resultado".[7] El avance tecnológico e informático ha permitido la creación de algoritmos que, integrados en sistemas de IA, siguen patrones no lineales en cuanto a la interpretación de los datos recopilados y eso permite la obtención de resultados imprevisibles, o que no estaban previstos inicialmente, mediante un aprendizaje adaptativo a su entorno.

La aparición de estos complejos algoritmos nos proporciona otra característica esencial de la IA, que es la opacidad. En efecto, en algunas ocasiones resulta muy difícil determinar qué proceso o que pasos ha seguido un sistema para llegar a una conclusión o realizar una acción o predicción, fenómeno que se conoce como "efecto caja negra"[8]. Ante este problema, se debe garantizar que esos algoritmos reúnan un mínimo de transparencia, control,

---

[3] COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica. Bruselas 19.2.2020 COM (2020) 64 final. Pág. 2. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064

[4] PETTERI ROUHIAINEN, L. Inteligencia Artificial. 101 cosas que debes saber sobre nuestro futuro. Editorial planeta, 2018. ISBN: 978-84-17568-08-5. Pág. 26.

[5] COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las… Cit., Pág. 10

[6] COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las… Cit., Págs. 6 y 7.

[7] BOTANA AGRA, J.M., "Protección jurídica de algoritmos y programas de ordenador". En: GARCÍA VIDAL, A. (Dir.): *Big Data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*. Valencia: Tirant lo Blanch, 2020, ISBN: 13 9788413781925, pág. 156.

[8] COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las… Cit., Págs. 10 y 11.

supervisión humana y rendición de cuentas para facilitar que los usuarios comprendan por qué estos sistemas han actuado de una determinada manera y permitir que puedan exigir responsabilidad.

1.2. Tipos de Inteligencia Artificial

Existen varios tipos de tecnología, algoritmos y sistemas informáticos (en adelante, usarán la palabra algoritmo y sistema indistintamente) que integran la IA, resulta conveniente exponer brevemente algunos de ellos, pese a que en la mayoría de IA se mezclan estas tecnologías y la línea que las separa es difusa, es interesante a efectos de contextualizar y conocer mejor el alcance de estas tecnologías.

1.2.1. Machine learning

Los sistemas de IA basados en *machine learning* o también llamados de aprendizaje automático, utilizan unos algoritmos que, según la Agencia Española de Protección de Datos (en adelante, AEPD) les permite a partir de relacionar variables y estudiar datos, identificar patrones y establecer criterios de clasificación para realizar predicciones y actuar en base a ellas[9]. Existen distintos grados de aprendizaje en función de la intervención o supervisión humana, pero para que tengamos un concepto general hay que quedarse con la idea de que estos sistemas por sí mismos son capaces de actuar y aprender de la experiencia de forma autónoma, a través de la recopilación de datos y la adaptación a su entorno.

A modo ilustrativo, un ejemplo de estos sistemas sería la publicidad personalizada que nos encontramos al navegar por internet o al utilizar las redes sociales. En efecto, en el campo del *marketing* online lo podemos observar en nuestro día a día, en las páginas web que consultamos, así como en nuestras redes sociales, cuando nos aparece publicidad relacionada con búsquedas de productos que hemos hecho recientemente, si hemos estado buscando zapatos online nos aparecerá publicidad de zapatos. El algoritmo identifica nuestros patrones de búsqueda, los compara y nos ofrece publicidad de artículos en los que potencialmente estaremos interesados, realiza una predicción y actúa adaptándose al usuario. Este es un tipo de IA muy básica y dentro del *machine learning* tenemos sistemas mucho más complejos, como los coches autónomos, pero los ejemplificaremos en apartados siguientes al ver los usos y aplicaciones actuales de la IA.

1.2.2. Expert system

Los sistemas expertos cuentan con algoritmos que son capaces de solucionar un problema complejo, dentro de un ámbito de conocimiento específico, ya que están programados con

[9] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción., febrero 2020. Pág. 6. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

información elaborada por expertos de la materia, para que el sistema resuelva tal y como lo haría un humano con amplios conocimientos en esa materia concreta[10].

Existen varios tipos de sistemas expertos, pero todos ellos comparten esa función básica de simular la forma de razonar y la obtención de un resultado frente a un problema concreto y delimitado dentro de un área de conocimiento, tal y como lo haría un experto.

Estos sistemas pueden estar basados en reglas preestablecidas, basados en datos y realizar una aplicación análoga al problema planteado, o se basan en construir deducciones a partir de variables y probabilidad[11].

En cuanto a la aplicación práctica, nos podemos encontrar que los que están basados en reglas preestablecidas, como por ejemplo en contabilidad y finanzas. Cuando acudimos a un banco y queremos pedir un préstamo, el trabajador introduce en un programa nuestros datos y el programa nos dice si somos o no solventes y, por ende, si nos será concedido o no el crédito.

Otra aplicación práctica más compleja se da en el ámbito sanitario, siendo posible que, a partir de nuestro historial, pruebas médicas y síntomas, un programa compare estos resultados con una base de datos y sea capaz de realizar un diagnóstico.

1.2.3. Neural network

A este tipo de sistemas también se les conoce como redes neuronales artificiales o computación cognitiva. Están formadas por redes neuronales artificiales interconectadas, de la misma forma que las encontramos en el cerebro humano y simulan la forma de aprendizaje que tenemos[12]. Son unos sistemas altamente complejos, capaces de procesar una gran cantidad de datos y de distinta naturaleza, todo ello simultáneamente. También pueden procesar datos no estructurados como pueden ser imágenes, textos o audios, e interpretarlos y relacionarlos como lo haría un ser humano. Esto les permite aprender e ir resolviendo problemas sin supervisión humana, simplemente mediante la experiencia y reaccionar ante situaciones que no ha experimentado antes por su capacidad de auto organización[13].

Un ejemplo práctico es el asistente de voz de Apple Siri, que es capaz de procesar tanto el lenguaje como interpretar el contexto de lo que le decimos, informarnos del estado del tráfico en tiempo real y proponernos rutas, sugerirnos música en función de nuestras

[10] CABALLERO VILLARASO, J., TABARES, A.R., GAVILÁN LEÓN, F.J., BUENA GARCÍA, M. y DÍAZ VEGA, F.J., Aplicación de algoritmos genéticos y sistemas expertos en medicina asistencial. Aplicaciones clínicas de la inteligencia artificial. AETSA 2009/6, pág. 21 y 22 Disponible en: https://www.aetsa.org/download/publicaciones/antiguas/AETSA_2009-6_Algoritmos_geneticos.pdf

[11] CABALLERO VILLARASO, J., TABARES, A.R., GAVILÁN LEÓN, F.J., BUENA GARCÍA, M. y DÍAZ VEGA, F.J., Aplicación de algoritmos genéticos y sistemas… cit., págs. 21 y 22.

[12] PINO DÍEZ, R., GÓMEZ GÓMEZ, A., y DE ABAJO MARTÍNEZ, N. *Introducción a la ingeniería Artificial: Sistemas Expertos, Redes Neuronales Artificiales y Computación Evolutiva*. Servicio de publicaciones de la Universidad de Oviedo 2001 ISBN: 84-8317-249-6. Pág. 29.

[13] LÓPEZ ONETO, M., *Fundamentos para un derecho de la inteligencia artificial. ¿Queremos seguir siendo humanos?* Tirant lo Blanch, 2020. ISBN: 978-84-1336-884-9. Pág. 51.

preferencias. Aprende, se adapta al usuario y es capaz de procesar diferentes tipos de información simultáneamente. Cuando pensamos en una IA con conciencia humana, capaz de interpretar emociones e interactuar plenamente con un ser humano, por ejemplo, teniendo una conversación dinámica y profunda, es decir, con respuestas no programadas, estamos pensando en este tipo de sistemas. Por el momento eso aún forma parte de la ciencia ficción, pero quien sabe si llegará el día o, mejor dicho, cuándo llegará el día que sea una realidad.

1.2.4. Deep learning

El aprendizaje profundo es un sistema en el que se combina el aprendizaje automático y el uso de redes neuronales artificiales. Se basa en la técnica de aprendizaje que hemos visto anteriormente y se procesa la información a través de redes neuronales artificiales, lo que le confiere una potencia y capacidad de procesamiento de datos enorme. Para aprovechar esa potencia, el aprendizaje profundo requiere de una base de datos muy amplia que le permita clasificar y reconocer el mayor número de patrones posibles[14]. Esa mejora del rendimiento de clasificación y del etiquetado de datos ha supuesto un avance significativo en tecnologías como el reconocimiento de imágenes, de voz o en la traducción automática, ya que, gracias a poseer una ingente cantidad de datos clasificados, estos algoritmos aprenden a identificar y clasificar incluso nuevos objetos y datos que no habían visto antes con una precisión asombrosa, incluso superior a la de los seres humanos[15].

Esta tecnología la usamos en nuestro día a día casi sin darnos cuenta, al usar las redes sociales cuando utilizamos la función de traducción automática de un *tweet* o un estado en *Facebook* escrito en un idioma extranjero.

1.3. Usos y aplicaciones actuales

La tecnología y la IA se está desarrollando y perfeccionando rápidamente, cada vez está presente en más ámbitos de nuestra vida y tiene un impacto transversal en nuestra sociedad. A modo de ejemplo vamos a recopilar algunos usos y aplicaciones de estos sistemas en diferentes sectores para ilustrar el carácter multidisciplinar y las posibilidades que nos ofrece, como nos señala la AEPD[16]:

- Servicios online, comercio y comunicaciones: En el uso cotidiano de internet, al realizar búsquedas en *google*, comprar online o simplemente mediante el uso de redes sociales o plataformas de contenido multimedia estamos haciendo trabajar a la IA. Éstas nos ofrecen anuncios personalizados en base a nuestras búsquedas y preferencias en la red, pero no solo operan como agentes de *marketing* autónomos ofreciéndonos anuncios personalizados o recomendando contenido que se ajuste a nuestros gustos en una plataforma de contenido como *Netflix*, también se usa

[14] PETTERI ROUHIAINEN, L., *Inteligencia* Artificia…Cit., Pág. 22.
[15] COMISIÓN EUROPEA, Comunicación de la Comisión al Parlamento Europeo…Cit, pág. 22.
[16] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Adecuación al RGPD de…Cit, pág.53.

mediante *chatbots* que ofrecen servicios de atención al cliente ante incidencias en una web o aplicación que proporciona productos o servicios, e incluso brinda asesoramiento personalizado en función de las necesidades de los consumidores.

- Servicios financieros: No sólo sirve de apoyo para conocer la solvencia de solicitantes de préstamos o hipotecas, también se usa para predecir movimientos en el mercado financiero y bursátil, ofrecer servicios de inversión automática a los clientes y asesoramiento a partir simulaciones del impacto de operaciones en su patrimonio.
- Servicios de transporte: Los avances en IA y robótica han permitido que los vehículos autónomos sean una realidad, es decir, que son capaces de circular sin o con la mínima intervención humana. Asimismo, han permitido la incorporación de semáforos inteligentes y la optimización de rutas y horarios de transportes públicos.
- Servicios de salud: En el ámbito sanitario la irrupción de estos sistemas ha logrado avances relevantes. Empezando por el desarrollo de vacunas, medicamentos y el análisis genético, así como predicciones y diagnósticos a partir de pruebas analíticas, imágenes e historia clínica.
- Servicios públicos y seguridad: La administración pública utiliza sistemas de IA para gestionar bases de datos, planificar servicios de mantenimiento de infraestructuras y tienen un papel importante en materia de seguridad pública, a través de tecnologías como el reconocimiento facial, el control de las fronteras y el rastreo y análisis de comunicaciones en materia de terrorismo. Las agencias de meteorología también utilizan estos sistemas para la predicción de alteraciones climáticas importantes o terremotos.
- Servicios en el mercado laboral e industria: Ya se utiliza la IA en recursos humanos para facilitar una selección de candidatos optimizada para los puestos de trabajo. Asimismo, los avances en robótica e IA están automatizando muchos procesos productivos que antes realizaban seres humanos, tanto en cadenas de montaje como en logística.
- Servicios jurídicos: La automatización de procesos es una realidad que poco a poco va ganando terreno incluso en los sectores más insospechados y el derecho no es una excepción. Si bien es cierto que no podemos afirmar que los agentes jurídicos como abogados, jueces, fiscales y asesores jurídicos vayan a desaparecer a corto plazo, están surgiendo herramientas que, como mínimo van a suponer una transformación en su forma de trabajar. Ya existen herramientas que son capaces de: predecir el resultado de resoluciones judiciales, predecir el riesgo de sanción ante un incumplimiento normativo, elaborar una estrategia procesal, revisar y redactar documentación como contratos u otros documentos e incluso de proponer soluciones mediando en conflictos.

Como hemos visto, la IA ofrece un abanico amplio de sistemas de apoyo francamente útiles y a priori eficaces, sin embargo, por precisos y rápidos que sean estos sistemas, de momento no tienen la capacidad de usar en sus procesos la inteligencia emocional, la empatía, la

proporcionalidad, valorar cuestiones morales, conocer cuestiones culturales y emplearlas a la hora de tomar decisiones, mediar en conflictos y negociar.[17]

1.4. Beneficios y riesgos

1.4.1. Aspectos sociales y económicos

La tecnología nos hace la vida más fácil y cómoda, nos aporta soluciones de forma rápida y nos reduce considerablemente el tiempo que debemos emplear en realizar tareas cotidianas. Nos permite comunicarnos fácil e instantáneamente a distancia, acceder a la información desde cualquier lugar del mundo, formarnos académicamente, realizar compras e incluso trabajar. Los sistemas de IA han supuesto una revolución en el ámbito científico, técnico y sanitario, con las ventajas para la salud pública que eso conlleva. Permite a las empresas y la industria ser más eficientes y ofrecer servicios las veinticuatro horas del día a usuarios y consumidores. Ha mejorado los sistemas de seguridad y prevención permitiéndonos anticiparnos a situaciones como un terremoto o un ataque terrorista. Resulta evidente que todo ello constituye un beneficio para nuestra sociedad, sin embargo, todo tiene un precio y el desarrollo tecnológico también.

La automatización de procesos industriales, logísticos y de servicios conllevan el riesgo de que eventualmente, se destruyan empleos mediante la substitución de trabajadores por máquinas o robots que pasen a ocupar esos puestos de trabajo. Existe pues un riesgo real de que se destruyan millones de empleos no cualificados. Sin duda, cabe preguntarse si el beneficio de las empresas por ahorrar costes de producción y de mano de obra compensa la destrucción de empleo y de si queremos vivir en una sociedad donde las máquinas sean herramientas que ayuden a los humanos o, por el contrario, que los substituyan.

1.4.2. Riesgos éticos

La IA facilita la automatización de procesos y decisiones, de ello surgen nuevos retos éticos y jurídicos que el Derecho debe abordar para garantizar que, en el desarrollo y el uso de estos sistemas no se vulneren nuestros derechos fundamentales y/o generen un perjuicio a la sociedad.

Las decisiones automáticas a las que llegan los algoritmos no se basan en relaciones causales, sino en correlaciones encontradas dentro de una gran cantidad de datos procesados, de un volumen tal que se les presume validez o fiabilidad. Con lo cual existe el riesgo que estén inducidas por errores o por sesgos[18]. La presencia de sesgos puede derivar

[17] MATEO BORJE, I., "La robótica y la inteligencia artificial en la prestación de servicios jurídicos" En: NAVAS NAVARRO, S. (Dir): *Inteligencia Artificial. Tecnología Derecho*. Tirant lo Blanch, 2017. ISBN: 13 9788491697213. Págs. 129 a 140.

[18] SORIANO ARNANZ, A. "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos". *Revista de derecho público: Teoría y Método*. Marcial Ponts ediciones jurídicas y sociales, nº 3, 2021. ISSN: 2695-7191, Pág. 91

en discriminación, ya que en primer lugar los algoritmos están diseñados por seres humanos, y como tales tenemos prejuicios y estereotipos sobre determinados grupos sociales. En segundo lugar, aunque estos algoritmos proyecten con precisión la realidad social, ésta se cimienta sobre una situación de desigualdad, donde existe la discriminación y hay grupos sociales desfavorecidos, por consiguiente, existe el riesgo de que los algoritmos incluyan esta discriminación y ayuden a perpetuar la desigualdad al reproducirla[19].

La UE lleva tiempo trabajando para adoptar un marco legislativo común en materia de ética digital. En 2019, un grupo independiente de expertos de alto nivel sobre IA creado por la Comisión Europea sentaron las bases de las directrices éticas que debían seguir estos sistemas[20]. En ese texto, se concluye que la IA durante su ciclo de vida debe ser:

- Lícita, es decir, respetar la normativa.
- Fiable, adaptándose a los valores éticos y morales de la UE.
- Robusta, en cuanto a la seguridad y mecanismos de resarcimiento por daños causados.

En cuanto a esos valores éticos y morales, señala principalmente los siguientes[21]:

- Respeto a la autonomía humana: Tiene una doble función, por una parte, debe respetar el derecho de las personas a elegir, participar libremente, no ser coaccionadas ni manipuladas de manera injustificada y, por otra parte, establece que los sistemas de IA deben contar con supervisión y control humano.
- Prevención del daño: Los sistemas de IA no deben dañar ni perjudicar a las personas, tanto a su integridad física como mental. Se debe velar por el respeto a la dignidad humana y garantizar un marco de seguridad en el despliegue y uso de la IA, velando por que no sea utilizada para fines contrarios al bienestar de las personas.
- Equidad: Implica perseguir los fines de una distribución igualitaria de beneficios y costes para la sociedad, así como prohibir que las personas sufran discriminación y sean objeto de sesgos que generen desigualdad de trato y oportunidades.
- Explicabilidad: Exige transparencia en la información relativa a la finalidad y toma de decisiones por parte de una IA, en aras de reforzar la confianza de los usuarios y permitirles acciones para defenderse de los daños o perjuicios que puedan sufrir.

Resulta imprescindible regular y adaptar el desarrollo y aplicación de estos sistemas en aras de asegurar que no van a atentar contra la dignidad humana, no van a ser discriminatorios por motivos de etnia, cultura o sexo, ni van a coartar los derechos y libertades de las personas. Para ello, tal y como se recoge en el documento, debe operar la transparencia y la adecuación a los valores humanos.

Otro los retos jurídicos que plantean estos sistemas es el resarcimiento de daños, ya que del proceso de automatización de decisiones y la falta de supervisión humana estos podrían

[19] SORIANO ARNANZ, A. "Decisiones automatizadas…Cit., Págs. 92 y 93.
[20] COMISIÓN EUROPEA, Directrices éticas para una IA fiable. Grupo independiente de expertos de alto nivel sobre inteligencia artificial. 8 de abril de 2019. Págs. 6 y 14 Disponible en: https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1
[21] COMISIÓN EUROPEA, Directrices éticas para una IA fiable… Cit., Págs. 14, 15 y 16.

derivar perjuicios para las personas si esas decisiones fueran erróneas, se deben establecer mecanismos de prevención, control y reparación.

Por último, un aspecto fundamental y que será el eje central del presente trabajo, es el derecho a la protección de datos. Dado que estos sistemas necesitan datos para su funcionamiento y algunos de esos son datos de carácter personal, éstos merecen una protección especial y el derecho debe velar por asegurar que estos sistemas no vulneran la privacidad de las personas.

1.5. Retos del futuro

1.5.1 Retos sociales y económicos

Una vez vistos los beneficios y riesgos que plantean los sistemas de IA, los retos a los que nos enfrentamos como sociedad no es otro que el de maximizar los beneficios que aportan a la sociedad y tratar de minimizar los riesgos.

Dado que no podemos detener el desarrollo tecnológico, lo cual sería absurdo porque no podemos progresar como civilización sin la ciencia y ésta se basa fundamentalmente en la tecnología, debemos intentar garantizar que su uso suponga un beneficio y no un perjuicio para nuestra sociedad.

No cabe duda, de que la irrupción de sistemas inteligentes que operan de forma autónoma son capaces de simplificar procesos e incluso substituir al ser humano destruyendo empleo, como hemos visto anteriormente. No es menos cierto que de ello surgirán nuevas necesidades en el mercado laboral y con ello oportunidades y creación de empleo. Sin embargo, éste será probablemente empleo que requiera cualificación y no podemos obviar el hecho de que al menos en una etapa inicial, el empleo que se destruirá será el no cualificado.

Ante este previsible cambio del paradigma socioeconómico, se nos plantea el reto de minimizar el impacto de la exclusión laboral de millones de personas. Para ello, a nuestro juicio, resulta imperioso garantizar y universalizar el acceso a una educación y formación superior que garantice la igualdad de oportunidades.

1.5.2. Retos éticos

Anteriormente se citaron algunos riesgos éticos que comprometen los sistemas de IA y como la UE consultó a un grupo de expertos en la materia, acerca de las directrices éticas que debe seguir la IA. En base a ese documento y a otros anteriores, el Parlamento Europeo aprobó en octubre de 2020, la propuesta de Reglamento del Parlamento Europeo sobre los

principios éticos para el desarrollo despliegue y el uso de la inteligencia artificial, la robótica y las tecnologías conexas[22].

La propuesta establece obligaciones para los sistemas de alto riesgo, que según el propio texto son las que, mediante su desarrollo, despliegue y uso suponen un riesgo de vulnerar derechos fundamentales, causando daños graves a las personas y la sociedad[23]. Establece unos requisitos clave que deben cumplirse: Supervisión humana, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas.

Los sistemas basados en IA deben promover valores como la inclusión social, la democracia, la solidaridad, la equidad, la pluralidad y la igualdad[24]. Necesariamente tienen que integrar mecanismos de supervisión humana para que en cualquier momento se puedan intervenir dichos sistemas, pudiendo desconectar o alterar su funcionamiento.[25] Se debe velar por la seguridad y la transparencia, dotando a los sistemas de medidas de protección suficiente y otorgando la información necesaria a los consumidores para mantenerlos al corriente de los riesgos, los errores y las posibles formas de reclamación.[26] Se prohíbe expresamente el sesgo y la discriminación ya sea por motivos de raza, sexo, orientación sexual, discapacidad, características físicas o genéticas, edad, origen étnico o social, lengua, religión o creencias, opiniones políticas, nacionalidad, estado civil o económico, educación o antecedentes penales[27]. Asimismo, no deben contribuir a la desinformación, deben promover la igualdad de género y la sostenibilidad medioambiental, teniendo en cuenta la huella ecológica y fomentando la transición verde[28].

Otro elemento esencial es el respeto a la intimidad, la dignidad humana y la protección de datos[29], que analizaremos en el siguiente apartado.

Por último, otorga a los usuarios el derecho a ser resarcidos por los daños y lesiones causadas por estas tecnologías[30]. También propone que los Estados formen una autoridad

---

[22] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, 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)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.pdf

[23] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 4.e

[24] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 5 y Considerando (31)

[25] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 7 y Considerando (10)

[26] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 8 y Considerando (19)

[27] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 9 y Considerandos (22), (23), (24)

[28] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 11 y Considerando (33)

[29] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020 … Cit., Artículo 12.

[30] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 13.

de control independiente que se encargue de evaluar y controlar el cumplimiento de estas normas, así como atender a las reclamaciones de los usuarios[31].

Como hemos podido observar, la UE está tomando una posición de liderazgo mundial en cuanto a la regulación de la IA, lo cual es un hecho muy positivo, ya que apremia una regulación macro a nivel europeo, que aborde los retos tan grandes a los que nos expone el continuo y rápido progreso de la tecnología y la transformación de la sociedad que eso supone.

Los aspectos de ética, seguridad y protección de datos son las cuestiones más importantes que debemos resolver, y la acción de la UE avanza en esa línea. De hecho, el 21 de abril de este mismo año, presentó otra propuesta de reglamento llamada *"laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts"*[32], donde se prohíben expresamente algunos usos de la IA, por ejemplo, los que inciten a los usuarios a tomar decisiones que les perjudiquen, los que en base a datos personales detecten vulnerabilidades de las personas, y regulan los usos y se establecen mecanismos de control para sistemas determinados de alto riesgo.

2. INTELIGENCIA ARTIFICIAL Y USO DE DATOS PERSONALES

2.1. El amparo de la intimidad personal y la protección de datos

Uno de los principios éticos y jurídicos que es exigible a estos sistemas es el respeto a la protección de datos, como ya hemos adelantado, está vinculada a la intimidad personal y la dignidad humana. Estos tres elementos forman parte nada menos que de los derechos fundamentales, cuyo alcance delimitaremos en el siguiente apartado, junto a la definición de datos personales.

Por ahora, vamos a centrarnos en la función que desempeñan como derechos fundamentales, es decir, los bienes jurídicos protegidos por la intimidad personal y la protección de datos, vinculados a la dignidad humana. El Tribunal Constitucional, en la STC 292/2000[33] expone lo siguiente:

- La función de intimidad personal: consiste en proteger ante cualquier invasión en el ámbito de la vida personal o familiar, que cualquier persona quiera excluir del conocimiento ajeno y de cualquier intromisión de terceros en contra de su voluntad.

[31] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 20 de octubre de 2020… Cit., Artículo 18.

[32] PARLAMENTO EUROPEO, Proposal for a regulation of the European Parliament and of the council. laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Brussels, 21.4.2021. COM(2021) 206 Final. 2021/0106 (COD) Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206&qid=1620488018088

[33] STC 292/2000, de 30 de noviembre de 2000, FJ 6. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

Permite excluir datos íntimos del conocimiento ajeno para resguardar de su vida privada una publicidad no deseada.

- La función de la protección de datos: permite garantizar a una persona el poder de disposición sobre sus datos personales, su uso y destino, e impedir un tráfico ilícito y lesivo para su dignidad y sus derechos. Pero va más allá del derecho a la intimidad, ya que protege no sólo los datos íntimos de la vida personal y familiar, sino cualquier dato personal, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean fundamentales o no. Se incluyen todos los datos que identifiquen o puedan identificar a las personas, a partir de los cuales se pueda confeccionar su perfil ideológico, racial, económico o de cualquier otra índole que pueda ser una amenaza para las personas. Para la garantía efectiva de este derecho, se imponen obligaciones a terceros y se les da a las personas un poder de disposición total sobre sus datos, que consisten en, el derecho a que se requiera el consentimiento previo de la persona para la recogida y el uso de sus datos personales, el derecho a ser informado sobre el destino y los usos de sus datos, el derecho de acceso, rectificado y la cancelación de sus datos.

Si tenemos en cuenta las características de dependencia de datos, conectividad, autonomía y opacidad que definen la IA, así como el uso de algoritmos para captar, procesar y tratar los datos, podemos identificar riesgos concretos para la intimidad y la protección de datos personales. Posteriormente, en el apartado cuarto del presente trabajo, se verá qué soluciones aporta la normativa para minimizar estos riesgos.

2.2. Riesgos para la intimidad personal y la protección de datos

2.2.1. Consentimiento indebidamente informado

Los sistemas basados en *machine learning* necesitan una gran cantidad de datos que extraer para analizar correlaciones y poder aprender de la experiencia, aquí encontramos la dependencia de datos, ya que recopila y analiza la mayor cantidad de datos posibles, y también la conectividad, puesto que también va generando o captando datos de la experiencia y reutilizándolos[34]. Pensemos por ejemplo en el *Apple watch*, el reloj de la marca *Apple*. Según su propia página web[35], este reloj ofrece la posibilidad de medir el oxígeno en sangre, realizar un electrocardiograma, medir las horas y calidad del sueño y sugerir rutinas para tener una mejor descanso, lleva un registro de la actividad física y comparte esta información con otros usuarios, sugiere música en función de los gustos del usuario, conoce las rutas que sigue para ir al trabajo y si detecta tráfico sugiere rutas alternativas, entre otras funciones, como las que ofrece el asistente por voz *siri*, o realizar pagos bancarios con el propio reloj.

[34] MERCHÁN MURILLO; A., "Retos regulatorios en torno a la Inteligencia Artificial". *Pensar, revista de ciencias jurídicas*. Nº23, 2018. Pág. 6

[35] Página web de Apple, donde explican las características y funciones de su reloj. Disponible en: https://www.apple.com/es/apple-watch-series-6/

Como vemos, este dispositivo permite recopilar una gran cantidad de datos sensibles, como datos relativos a la salud y el bienestar físico de las personas, datos bancarios, la localización exacta en cada momento del usuario e, incluso, los gustos y preferencias, hábitos de consumo y de conducta. Sería posible a través de este conjunto de datos predecir el comportamiento futuro de los usuarios, de hecho, lo hacen para mejorar la experiencia del usuario, o crear perfiles a partir del análisis del comportamiento, deducir si los usuarios están tristes o alegres, así como rastrear e identificar a los usuarios pese a que sus datos estén cifrados[36], a través de la huella digital que dejan estos dispositivos.

El elemento que legitima al dispositivo la recopilación de los datos y la activación de sus funciones es el consentimiento del usuario, que debe ser libre, específico, informado e inequívoco[37].Versa precisamente sobre el consentimiento uno de los riesgos para la intimidad de las personas, ya que se exige que esa información que se proporciona al usuario debe ser clara y concisa, tanto sobre los riesgos del tratamiento y la seguridad, como la finalidad que se persigue con ese tratamiento de datos[38]. Generalmente, los usuarios parten en desventaja, ya que no conocen los puntos débiles de esas tecnologías, ni cómo puede verse afectada la seguridad del tratamiento de sus datos, ni si esa tecnología reúne las medidas de seguridad necesarias para proteger sus datos[39]. Igual de importante es conocer con exactitud la finalidad del tratamiento de los datos, en ambos casos se requiere que la información proporcionada al usuario sea lo más transparente posible, ya que, si esa información fuera errónea, parcializada o difusa, supondría un vicio del consentimiento y un acceso ilegítimo a la privacidad de los usuarios, puesto que el consentimiento no informado socavaría el poder de disposición sobre sus datos personales, de acuerdo con el derecho de protección de datos.

2.2.2. Opacidad y autonomía: Elaboración de perfiles y decisiones automatizadas

La autonomía de los sistemas de IA implica que son capaces de realizar tareas sin que los pasos a seguir para su ejecución estén determinados, y lo hacen con poca o ninguna supervisión humana, pudiendo tomar decisiones de forma automatizada. Estos complejos algoritmos producen el efecto caja negra, ya que los procesos que han llevado a la IA a tomar esa decisión son difíciles, incluso imposibles de comprender[40]. Esta opacidad que caracteriza a los algoritmos de estos sistemas, sobre todo presentes en la IA del tipo *machine learning* y *neural network* plantea principalmente dos problemas.

En primer lugar, dificulta el derecho de un usuario afectado por una de estas decisiones a reclamar una indemnización por los daños sufridos, ya que para demostrar el nexo de

[36] MERCHÁN MURILLO; A., "Retos regulatorios...Cit, Pág. 6
[37] REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE. Artículo 4.11 Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf
[38] REGLAMENTO (UE) 2016/679... Cit., Considerando (32)
[39] MERCHÁN MURILLO; A., "Retos regulatorios…Cit,Pág. 7
[40] COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las … Cit., pág. 18.

causalidad entre el daño sufrido y la imputación del daño a la actuación de la IA se necesitan unos conocimientos técnicos que las victimas difícilmente pueden tener, lo que se traduce en indefensión[41].

En segundo lugar, al margen de la dificultad de que prospere una reclamación de responsabilidad civil, mediante el tratamiento automatizado de datos, es habitual la elaboración de perfiles y la toma de decisiones individuales automatizadas. Cabe matizar que son cuestiones distintas, aunque en ocasiones se utilizan conjuntamente y comparten la característica de la opacidad.

La elaboración de perfiles consiste, en utilizar datos personales mediante el tratamiento automatizado de datos, para evaluar diferentes aspectos personales de una persona, para analizar aspectos como su situación económica, salud, preferencias personales, intereses, comportamiento, rendimiento profesional, movimientos o ubicación[42]. Esos perfiles evalúan las características de una persona física y sus patrones de conducta con el fin de asignar a un grupo demográfico concreto sobre el cual, mediante su análisis, realizar predicciones sobre su comportamiento, sus capacidades, sus aptitudes para llevar a cabo una tarea o sus intereses[43]. En cambio, las decisiones automatizadas se basan en cualquier tipo de datos, como los ofrecidos directamente por una persona mediante respuestas en un cuestionario, los datos observados de la persona mediante el uso de un dispositivo o aplicación, o los datos que se basan en un perfil ya existente. Tanto la elaboración de perfiles como las decisiones individuales automatizadas pueden operar de forma autónoma, pero eso no quiere decir que sean independientes, pues de la elaboración de perfiles es habitual que se deriven decisiones individuales automatizadas[44].

Estas técnicas se utilizan en muchos sectores, tanto públicos como privados, para mejorar la diversificación de mercados, para personalizar la publicidad y el acceso a bienes y servicios o para ayudar al proceso de toma de decisiones. Los podemos encontrar en muchos sectores, como el financiero, en sanidad, educación, transporte o seguros[45].

Aunque resulta indudable que estas técnicas aportan una mayor eficiencia y suponen un ahorro de recursos, también implican riesgos para la intimidad y la protección de datos de las personas. Empezando por el hecho de que tal vez algunas personas ni sean conscientes de que están siendo objeto de la elaboración de un perfil, esos perfiles pueden encasillar a las personas en estereotipos o sesgos y limitarles su libertad de elección, ya que puede que se les ofrezcan bienes o servicios concretos en base a un perfil inexacto, o negar el acceso a bienes, servicios o incluso contratos[46]. Por ejemplo, en el ámbito de las relaciones públicas se utilizan estas técnicas para la selección de personal y algunas personas pueden quedar excluidas del acceso a un trabajo, también se les puede denegar alguna ayuda o subvención,

[41] *Ibidem* pág. 18
[42] REGLAMENTO (UE) 2016/679... Cit., Artículo 4.4
[43] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a efectos del Reglamento 2016/679, WP251rev.01, 6 Febrero 2018, Págs. 7 y 8 Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf
[44] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., Pág. 8.
[45] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., Pág. 5.
[46] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., Pág. 6.

ya que en el ámbito de la administración pública se utilizan estos sistemas, con lo que pueden afectar a derechos e intereses de las personas.

Por otra parte, resulta preocupante la personalización de la oferta de bienes, servicios e información, porque del análisis del comportamiento y preferencias de las personas, se puede manipular a las personas y limitar su capacidad de decisión y elección, a través de la detección de vulnerabilidades o tendencias que podrían traducirse en incentivar a las personas a realizar conductas que puedan ser lesivas para ellos mismos, como la compra compulsiva de artículos de bajo precio[47] o fomentar la ludopatía motivados por publicidad de casas de apuestas. En cuanto a la información, *Google,* por ejemplo, tiene un servicio de noticias personalizado que nos permite ver con tan solo abrir nuestro navegador web en el móvil, una serie de noticias que nos ofrece basándose en nuestras búsquedas y preferencias. Puede parecer útil, sin embargo, no cuenta con sistemas de verificación que permitan reconocer noticias o fuentes de información falsas o poco fiables, con lo que, por una parte, puede fomentar la desinformación, generar odio, segmentación y polarizar a la sociedad.

2.2.3. Monetización de los datos personales

Al hilo de la elaboración de perfiles y la publicidad personalizada, concretamente al hecho de que en algunas ocasiones no somos conscientes de que nos están analizando, conviene exponer una situación que facilita este hecho. La tecnología ha puesto a nuestra disposición una serie de herramientas de entretenimiento inmensa, ofreciéndonos diferentes servicios digitales de suministro de contenidos variados, como música, videos y redes sociales[48]. Estos servicios como *Spotify, Youtube,* o redes sociales como *Twitter, Facebook, Instagram o Tik Tok,* son aparentemente gratuitos para los usuarios, si bien algunos de ellos ofrecen servicios especiales mediante el pago de una suscripción, de forma general los podemos utilizar de forma gratuita. Sin embargo, en la práctica no son gratuitos, ya que utilizan nuestros datos personales para mejorar y personalizar el servicio, como por ejemplo el algoritmo de *Youtube,* que nos recomienda videos de contenidos en base a nuestras búsquedas y preferencias, como también para venderlos a terceras empresas que crearán perfiles y ofrecerán bienes y servicios personalizados, mediante publicidad[49].

En nuestra actual economía digital, la información y los datos personales son un bien de mercado más y por lo tanto tienen un valor económico. Habitualmente los contenidos digitales no se intercambian por dinero, sino por una contraprestación en forma de acceso a los datos personales[50]. Al margen del debate sobre la posible mercantilización de los datos personales y sus implicaciones en materia de contratos, así como el que alude a la posibilidad de los usuarios de vender por una contraprestación pecuniaria contenido que

[47] SORIANO ARNANZ, A. "Decisiones automatizadas…Cit., Págs. 93 y 94.
[48] NAVAS NAVARRO, S., "Datos personales y mercado" En: NAVAS NAVARRO, S. (Dir): *Inteligencia Artificial. Tecnología Derecho*. Tirant lo Blanch, 2017. ISBN: 13 9788491697213. Págs. 259 a 266.
[49] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., Pág. 8.
[50] PARLAMENTO EUROPEO, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales. Bruselas 9.12.2015. COM(2015) 634 final. 2015/0287 (COD). Considerando (13) Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015PC0634&from=EN

forma parte de derechos fundamentales[51], preocupa que los usuarios y consumidores de contenidos digitales no tengan conciencia del tratamiento de sus datos. En concreto, del procesamiento de los mismos, de la elaboración de perfiles, del análisis y predicción de su conducta, de la finalidad del tratamiento de sus datos, así como de la seguridad y de las repercusiones para la manipulación de su conducta que puede producirse. Dado que servicios digitales gozan de amplia popularidad y son utilizados por millones de personas, de distintas edades y condición, cabe preguntarse si como usuarios estamos debidamente informados, del pacto o contrato que suscribimos cada vez que utilizamos dichos servicios ya que, de alguna forma, perdemos el rastro y el control sobre nuestros datos personales.

3. PROTECCIÓN DE DATOS

3.1. Definición datos de carácter personal

En el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), encontramos la siguiente definición de datos personales[52]:

> Toda información sobre una persona física identificada o identificable («el interesado»); 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 varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Vemos que se trata de una definición amplia, que tiene por objetivo incluir y abarcar los máximos elementos posibles que permiten que una persona sea identificada, a efectos de otorgar una mayor protección de su intimidad. Pese a que se expone un detallado abanico de ejemplos de lo que se considera un identificador, no es una lista cerrada, por el contrario, exige una interpretación amplia.

El dictamen 4/2007 sobre el concepto de datos personales del grupo de trabajo del artículo 29 (WP29)[53] hace una interpretación y análisis exhaustivo de esa definición, destacando 4 conceptos clave:

I. La expresión "toda información" referida en la definición. Por una parte, arguye que ésta debe ser interpretada de forma amplia como hemos señalado, pero que no solo la información objetiva constituye un identificador, sino que hay elementos

[51] NAVAS NAVARRO, S., "Datos personales y mercado" … Cit., Págs. 259 a 266.
[52] Reglamento (UE) 2016/679…Cit.
[53] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de datos personales (WP29). WP 136. Págs. 6 a 24. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

subjetivos que se deben incluir, como información, evaluación u opinión subjetiva. Como por ejemplo ser evaluado como buen estudiante, mal trabajador o un cliente deudor, se considera que esos aspectos subjetivos y personales aportan características e información personal que permiten definir e identificar a alguien[54]. Teniendo en cuenta las posibilidades de comunicación e interacción social que nos permite internet y las redes sociales, la información que compartimos, tales como opinión política, gustos o preferencias sexuales, ideológicas o religiosas también forman parte nuestros datos personales, incluso en actos tan banales a priori como dar un *like* estamos generando datos personales. Cuestión distinta es que al hacerlo demos consentimiento a que éstas sean públicas, pero ya abordaremos el consentimiento al analizar el RGPD.

Atendiendo al contenido de la información, encontramos 2 tipos de datos personales con un mayor grado de protección:

- Las llamadas categorías especiales de datos personales, que en virtud del considerando (51) del RGPD, poseen una protección especial en el reglamento, prohibiendo su tratamiento de forma general y estableciendo mecanismos legales de obligado cumplimiento para ello, dada la sensibilidad de éstos, en relación con derechos y libertades fundamentales, puesto que los mismos forman parte de la esfera más íntima y privada de las personas. Los encontramos regulados en el artículo 9.1 del RGPD y son:

  > Los que revelen 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.

- Los datos relativos a condenas e infracciones penales, que atendiendo al considerando (19) y en relación con los artículos 6.1 y 10 del RGPD y 10 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[55] (en adelante, LOPDGDD), su tratamiento solo se permite por autoridades competentes, bajo el amparo de una norma de la UE o nacional o cuando sea imprescindible para la investigación, prevención, detección o enjuiciamiento de sanciones penales, en aras de proteger la seguridad pública; también por profesionales en el ejercicio de sus funciones, como abogados y procuradores.

En cuanto al formato que contiene esa información, cualquier formato es válido. Las nuevas tecnologías permiten obtener y almacenar datos, procesarlos, transmitirlos de forma variada y el RGPD debe dar una cobertura lo más amplia posible. Por consiguiente y a modo de ejemplo, son válidas las fotografías, videos, la voz, una dirección de correo electrónico o cualquier soporte, analógico o digital que sea capaz

[54] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de… cit., pág. 6.
[55] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE, núm. 294, de 6 de diciembre de 2018, pp. 119788 a 119857.

de almacenar datos, incluso si éstos no se incluyen en un fichero o base de datos, siendo válido cualquier texto libre o documento electrónico.[56] En cuanto al fichero de audio, éste podría ser la grabación de una conversación con un agente de seguros o un trabajador de una entidad bancaria, que por seguridad se graban algunas conversaciones cuando contratamos un servicio o producto.

II. La expresión "sobre" en la definición datos personales alude a que la información debe referirse a una persona concreta. A priori puede parecer una cuestión sencilla determinar cuándo un dato o información se puede vincular a las características, identidad o comportamiento de alguien. Es indudable que nuestro nombre, apellidos y DNI nos identifican, que el resultado de unas pruebas médicas hace referencia a un individuo concreto. Pero también, esa información se puede referir a objetos y no solo a personas. Si esos objetos tienen un propietario o alguna persona que tenga un vínculo estrecho con ellos, cabe la posibilidad que bajo algunas circunstancias se puedan derivar derechos u obligaciones o influyan en la situación o comportamiento de una persona. Por ejemplo, el valor de vivienda por sí mismo no es relevante a efectos de datos personales, pero si lo es desde el momento en el que ese valor le genera a su propietario la obligación de tributar por el mismo[57].

III. La expresión persona física "identificada o identificable". En cuanto al concepto de identificada, se refieren a que con los datos disponibles es indudable distinguir a un individuo concreto del resto, a través de indicadores muy concretos como nombre, apellidos o número de DNI. Con identificable se refieren a, cuando con la información disponible no es suficiente para identificar fehacientemente a alguien, pero mediante una combinación de datos, como pueden ser fecha de nacimiento o su dirección, número de teléfono, cargo o profesión, o datos de cualquier naturaleza sea posible identificar a alguien[58].

No siempre es necesario conocer nombres y apellidos de alguien para identificarlo, sino que se puede hacer indirectamente. Existen otros identificadores que permiten determinar la identidad de alguien en concreto, por ejemplo, en los ficheros digitales a las personas se les asigna un número de identificación personal para distinguirlos del resto en una lista[59]. Respecto a los identificadores en línea, el considerando (30) del RGPD, puntualiza que el uso de algunos dispositivos puede dejar huellas que, combinadas con otros datos pueden llegar a crear perfiles e identificar a usuarios. En efecto, las aplicaciones, herramientas y protocolos de direcciones de internet, como las famosas "*cookies*", o las herramientas de identificación por radiofrecuencia, facilitan que una persona sea indirectamente identificable.

Para llegar a considerar a una persona identificable, se debe atender, por una parte, a la razonabilidad de los medios, es decir, si con los recursos técnicos, humanos y datos disponibles es suficiente y; por otra parte, a la proporcionalidad del esfuerzo

[56] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de… cit., pág. 8.
[57] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de… cit., pág. 10.
[58] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de… cit., pág. 13.
[59] GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de… cit., pág. 15.

que supondría para el responsable del tratamiento de los datos[60]. Si con los datos existentes no se pudiera identificar a alguien sin realizar un esfuerzo desproporcionado, no serían considerados datos personales.

Para reforzar la seguridad de los datos personales, los encargados del tratamiento de los datos utilizan diferentes técnicas que dificultan la identificabilidad de las personas. Una de ellas es la seudonimización, que consiste en sustituir un dato o atributo de una persona por otro en un registro, de forma que sea más difícil vincular un conjunto de datos a una persona concreta[61]. No obstante, pese a que resulte más difícil esa identificabilidad, ésta siendo posible y las normas del reglamento son aplicables, de acuerdo al considerando (26) del RGPD, que, no obstante, en los considerandos (28) y (29) incentiva el uso de esta técnica, con la finalidad de dotar de más seguridad al tratamiento de datos personales.

Por otra parte, tenemos la técnica de anonimización, a través de la cual se eliminan de un conjunto de datos, los elementos suficientes para que no se le puedan atribuir a una persona concreta, que no permitan que sea posible la identificabilidad de la misma, ni por el responsable del tratamiento de los datos ni por un tercero, de forma irreversible[62]. De acuerdo al considerando (26) del RGPD, a los datos anónimos o conjuntos de datos anonimizados no le son de aplicación las disposiciones del reglamento.

IV. La expresión "persona física", delimita la aplicación del RGPD y el alcance del derecho a la protección de datos personales en función del titular de esos datos.

El RGPD, tal y como señala en el artículo 1.2 se aplica para la protección de los datos personales de las personas físicas. El considerando (14) RGPD, excluye del reglamento y de la protección, a los datos de las personas jurídicas.

Por otra parte, establece reglas especiales para la protección de datos de algunas personas físicas:

- Los fallecidos: Si bien es cierto que el considerando (27) RGPD excluye a las personas fallecidas, permite a los Estados miembros la adopción de normativa para estos supuestos. En este sentido, en España lo regula el artículo 3 de la LOPDGDD, y permite a familiares o herederos solicitar la revisión o supresión de los datos personales del fallecido.

- Los menores de edad: El artículo 8 del RGPD señala que el consentimiento para el tratamiento de datos personales de los menores de edad será lícito cuando estos tengan al menos dieciséis años, por debajo de esa edad se exige el consentimiento

[60] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Guía de buenas prácticas en protección de datos para proyectos de big data. mayo 2017. Pág. 9. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

[61] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 05/2014 sobre técnicas de anonimización. WP216. 10 abril 2014. Pág. 22. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

[62] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 05/2014…Cit, Págs. 5 y 6.

de los titulares de la patria potestad. Exige, además, que los responsables del tratamiento de los datos realicen esfuerzos para comprobar el consentimiento dado por los menores u otorgado por los que ostentan su patria potestad. Sin embargo, deja en manos de los Estados miembros establecer otro límite de edad, siempre y cuando no sea inferior a trece años. En esta línea, en España el artículo 7 del LOPDGDD, rebaja el límite para la licitud del consentimiento de los menores a los catorce años.

El considerando (38) del RGPD, pone de manifiesto la necesidad de protección de los menores, ya que son más vulnerables al no tener una conciencia plena de los riesgos y consecuencias del tratamiento de sus datos personales. En la actualidad tecnológica que vivimos, con cientos de aplicaciones, redes sociales, páginas de elaboración de perfiles y *marketing online* agresivo, y la integración de los menores de edad a dispositivos conectados a internet, parece que estas medidas de protección no serán del todo completas, hasta que no se establezcan medidas y protocolos de verificación del consentimiento estrictas y procedimientos de información integrales y transparentes.

3.2. Marco jurídico de la protección de datos

La protección de datos personales de las personas físicas constituye un derecho fundamental y, por lo tanto, irrenunciable y protegido, amparado por el artículo 18.4 en relación con el 10 de la Constitución Española (en adelante, CE)[63]. El artículo 18.4 de la CE señala que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", y el artículo 10 recoge el derecho fundamental de la dignidad de la persona. En base a esos artículos, el Tribunal Constitucional, en la STC 292/2000 configura el derecho a la protección de datos, pero lo considera un derecho autónomo[64]:

> El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 C.E. otorga, sino los datos de carácter personal.

A pesar de que se basa y se fundamenta en el artículo 18.4 de la CE, éste opera de forma autónoma y tiene un alcance mayor. La propia STC 292/2000 concreta su contenido en el FJ 7[65]:

> Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de

[63] CONSTITUCIÓN ESPAÑOLA, 1978, Artículos 10.1 18.4. BOE núm. 311, de 29/12/1978.
[64] STC 292/2000… Cit, FJ 6.
[65] STC 292/2000… Cit, FJ 7.

> los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En España se desarrolló el derecho a la protección de datos por primera vez mediante la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales[66]. Ley que posteriormente fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[67], para permitir la trasposición de la Directiva 95/46/ CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[68], a nuestro Derecho interno.

El desarrollo de legislación europea en materia de protección de datos también se basa en su condición de derecho fundamental, pues así se recoge explícitamente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea[69], y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea[70]. Sin embargo, es a partir del Convenio del Consejo de Europa para la protección de las personas, con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo en 1981[71], cuando se pone de manifiesto la necesidad de un marco legal común, y es el documento normativo en el que se inspira la normativa tanto la de los Estados firmantes del Convenio como la normativa europea que le sucedió en los años siguientes.

Con el objetivo de armonizar y consolidar la legislación europea, la Directiva 95/46/ CE fue derogada por el RGPD[72], lo que provocó que en España se adaptara la legislación mediante la aprobación de la LOPDGDD[73], que derogó la Ley Orgánica 5/1992, de 29 de octubre, y complementa algunas cuestiones que el RGPD no regula, o deja en manos de los Estados miembros su regulación. Estas dos leyes son las que principalmente regulan la protección de datos de carácter personal en la actualidad.

La importancia del RGPD, radica en la imperante necesidad de un marco legal común que opere, por una parte, como límite para los encargados del tratamiento de la información, ofreciendo garantías para la salvaguarda de los derechos de los ciudadanos respecto la protección de sus datos personales y; por otra parte, para facilitar la libre circulación de los

[66]Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales. BOE, núm. 262, de 31 de octubre de 1992, págs.37037 a 37045.
[67] Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales. BOE núm. 298, de 14/12/1999.
[68]Directiva 95/46/ CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678
[69] Carta de Derechos Fundamentales de la Unión Europea, diciembre 2000. Artículo 8 Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf
[70] Tratado de Funcionamiento de la Unión Europea. Versión consolidada 30.3.2010. Disponible en: https://www.boe.es/doue/2010/083/Z00047-00199.pdf
[71] CONSEJO DE EUROPA, Convenio para la protección de las personas, con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447
[72] REGLAMENTO (UE) 2016/679 … Cit.
[73] LEY ORGÁNICA 3/2018…Cit.

datos, tanto dentro del territorio de la unión como su transferencia a terceros países, ya que las nuevas tecnologías y la creciente economía digital precisan de seguridad jurídica[74].

4. ADECUACIÓN DE LOS SISTEMAS DE IA Y ANÁLISIS DEL REGLAMENTO (UE) 2016/679

En este apartado se analizarán los aspectos más relevantes que dispone el RGPD, así como la adecuación de los sistemas de IA que afectan o tratan datos personales de esta normativa.

El objeto del Reglamento es establecer normas para la protección de los datos personales de las personas físicas, se excluyen las personas jurídicas[75]. Esas normas son de obligado cumplimiento para todas las empresas que traten datos personales, incluidas las PYMES, y tengan un establecimiento situado en la UE, independientemente de que el tratamiento de los datos se sitúe en un tercer país o de la nacionalidad de las personas, siempre que se encuentren en el territorio común[76].

No obstante, aunque el tratamiento se realice fuera del territorio común y sus responsables o encargados no tengan un establecimiento en Europa, si se ofrecen bienes o servicios o se controla el comportamiento de personas físicas residentes en la UE, también será de aplicación el RGPD[77].

4.1. Principios del tratamiento de los datos

4.1.1. Principios generales

Los sistemas basados en IA deben cumplir una serie de principios jurídicos que rigen, legitiman y garantizan el tratamiento adecuado de los datos personales. El RGPD impone obligaciones y límites para los responsables del tratamiento[78] de los datos personales.

EL tratamiento debe realizarse de forma lícita, leal y transparente[79], de tal manera que las personas sean conscientes de que se están recopilando sus datos, siendo analizados, utilizados, de qué forma y con qué finalidad. La transparencia impone la obligación a los responsables del tratamiento[80] de informar y comunicar a la persona que ha facilitado el acceso a sus datos, todo lo relativo al tratamiento de estos, con un lenguaje sencillo, claro y entendible. Esa información abarca tanto la identidad de los responsables del tratamiento,

[74] REGLAMENTO (UE) 2016/679.... Cit., Considerandos 2, 4 ,5, 6 y 7.
[75] REGLAMENTO (UE) 2016/679... Cit., artículo 1 y considerando (14)
[76] REGLAMENTO (UE) 2016/679... Cit., artículo 3.1 y considerando (14)
[77] REGLAMENTO (UE) 2016/679... Cit., artículo 3.2
[78] Tratamiento: "Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por tratamientos automatizados o no, como la recogida, registro, utilización, consulta, extracción limitación, supresión…" Artículo 4 RGPD
[79] REGLAMENTO (UE) 2016/679... Cit., artículo 5.1a
[80] Responsable del tratamiento: "Persona física o jurídica o autoridad pública, que solo o junto con otros, determine los fines y medios del tratamiento…" Artículo 4 RGPD

como la finalidad del tratamiento, los riesgos, la normativa que rige el tratamiento y las vías de reclamación existentes.[81]Asimismo, incluye la obligación de comunicar la existencia de la elaboración de perfiles y sus consecuencias, también posibilita que toda esa información se comunique vía web,[82] que es lo más habitual, ya que los sistemas de IA fundamentalmente operan *online*.

En adición a estos tres principios básicos, encontramos los siguientes:

- **Limitación de la finalidad:** La recogida de datos personales se condiciona a la realización de una finalidad específica, determinada previamente a la recogida de los datos, quedando prohibido tratar esos datos con una finalidad distinta a la inicialmente determinada, a excepción de los casos de interés público, científico, de investigación o históricos. Se exige que la finalidad sea además de concreta y lo más explícita posible, legítima, no puede ser contraria a la ley[83].
- **Minimización de datos:** Establece la obligación de limitar tanto la recogida como el procesamiento de los datos a su mínima expresión, utilizando únicamente los adecuados y pertinentes para poder realizar la finalidad preestablecida por el sistema[84]. En la práctica esto plantea dos problemas, por un lado, determinar qué información es necesaria y, por otro lado, determinar de cuantas personas se precisa esa información para cumplir la finalidad del sistema. Si pensamos en los sistemas de *machine learning* y *neural network,* estos necesitan de la mayor cantidad de datos posibles para aprender y realizar acciones y predicciones basándose en el análisis y la correlación de datos, pudiendo llegar incluso a conclusiones inesperadas, con lo que resulta difícil establecer que información mínima es pertinente. Es cierto que la minimización de datos no establece ningún volumen concreto de datos, expone que deben ser los mínimos y necesarios para cumplir la finalidad, pero dada la complejidad técnica y la profundidad que pueden alcanzar estos sistemas, esa determinación resulta francamente difícil.
- **Exactitud**: Los datos deben ser correctos, exactos, se deben supervisar para su actualización o corrección si fuera necesario, incluyendo mecanismos de rectificación o supresión[85]. Es un aspecto fundamental, ya que la inexactitud de los datos provocaría un mal funcionamiento de estos sistemas, provocando que tomaran decisiones automatizadas erróneas que podrían afectar a los usuarios, o que realizaran predicciones imprecisas causando daños.
- **Limitación del plazo de conservación:** Existe un límite temporal para el almacenamiento y procesado de datos personales que permitan identificar a una persona, que coincide con la finalidad del tratamiento de esos datos. Se prohíbe la conservación de los datos más allá de la finalización de la finalidad que legitimó su recogida, a excepción del interés público, investigación científica o histórica. Ese

[81] REGLAMENTO (UE) 2016/679... Cit., considerando (39)
[82] REGLAMENTO (UE) 2016/679... Cit., considerandos (58) y (60)
[83] REGLAMENTO (UE) 2016/679 …Cit., artículo 5.1b y considerando (39)
[84] REGLAMENTO (UE) 2016/679 ... Cit., artículo 5.1c
[85] REGLAMENTO (UE) 2016/679... Cit., artículo 5.1d

límite temporal, además, debe estar determinado por el responsable del tratamiento, estableciendo fechas para la supresión y revisión de los datos[86].

- **Integridad y confidencialidad:** La seguridad es otro elemento clave, el tratamiento de los datos exige que los responsables presten una garantía que proteja adecuadamente los datos personales, incluidos el tratamiento no autorizado o ilícito y su integridad, incluidas la pérdida y la destrucción de los datos. La garantía de la seguridad es extensible no solo al acceso a los datos, sino también a los equipos utilizados en el tratamiento, y es obligatorio que los responsables cuenten con unas medidas técnicas suficientes y delimitadas para garantizar esa seguridad.[87]

Estos principios son vinculantes y de obligado cumplimiento para los responsables del tratamiento de los datos, a los cuales se les exige, además, que demuestren el cumplimiento efectivo de estos principios, se les impone una responsabilidad proactiva[88].

4.1.2 Licitud

Cabe analizar el principio de licitud de forma independiente, ya que constituye la base que legitima el tratamiento de datos personales.

El artículo 6 del RGPD establece bajo qué condiciones concretas se considerará lícito un tratamiento de datos personales, se debe cumplir al menos una de estas condiciones:

- Que la persona preste su consentimiento específico y válido para uno o varios fines, ya determinados previamente por el responsable del tratamiento, debe respetar el principio de limitación del tratamiento[89].
- Que el tratamiento sea necesario para la ejecución de un contrato del que el usuario es parte, o resulte necesario para tomar medidas en relación con ese contrato, como la prestación de un servicio o la conclusión del contrato[90].
- Que el tratamiento sea necesario para cumplir una disposición legal que vincule a los responsables del tratamiento, es decir, una norma de la Unión Europea o de un Estado miembro, donde se detallaran los requisitos y los fines del tratamiento[91]. Aunque exista una base legal que les permita un tratamiento de datos personales, este debe adecuarse a lo que dispone la norma y no pueden arbitrariamente utilizarlos al margen de lo dispuesto en ellas.
- Que el tratamiento sea imprescindible para proteger los intereses vitales de la persona que ha cedido sus datos o de un tercero, ese interés debe considerarse esencial para la vida de esas personas y está reservado para situaciones excepcionales, como una crisis humanitaria, catástrofes naturales o epidemias[92]. Lamentablemente tenemos un claro ejemplo en la actual crisis de pandemia

[86] REGLAMENTO (UE) 2016/679... Cit., artículo 5.1e y considerando (39)
[87] REGLAMENTO (UE) 2016/679... Cit., artículo 5.1f y considerando (39)
[88] REGLAMENTO (UE) 2016/679 ... Cit., artículo 5.2
[89] REGLAMENTO (UE) 2016/679 ... Cit., artículo 6.1a y considerando (40)
[90] REGLAMENTO (UE) 2016/679 ... Cit., artículo 6.1b y considerandos (40) y (44).
[91] REGLAMENTO (UE) 2016/679... Cit., artículo 6.1c en relación con los artículos 6.2 y 6.3.
[92] REGLAMENTO (UE) 2016/679 ...Cit., artículo 6.1d y considerando (46)

provocada por la Covid 19, donde podemos observar que se recopilan datos de los infectados, sus características, síntomas, edad y sexo, con fines de investigación y prevención, sin el consentimiento expreso de las personas, este artículo legitima esas actuaciones.

- Que el tratamiento sea necesario para satisfacer una misión de interés público o ésta le sea encomendada a terceros que serán responsables del tratamiento, es decir cuando lo realiza o bien una autoridad pública o la autoridad le confiere la tarea a un tercero. En este último caso, la autoridad le dará instrucciones claras, concisas y detalladas del tratamiento a través de una norma de la Unión o de un Estado miembro. Esa norma incluirá la finalidad del tratamiento, el tipo de datos personales que se requieren, las personas que se verán afectadas y el plazo de conservación de los datos, entre otras medidas dirigidas a garantizar un tratamiento que respete todas las garantías y principios que establece el RGPD[93]. Un ejemplo de estas situaciones es cuando una autoridad pública le confiere a una empresa el control o vigilancia de sus fronteras[94].
- Que el tratamiento sea necesario para conseguir un interés legítimo perseguido por el responsable del tratamiento o por un tercero, siempre que esos intereses no vayan en perjuicio de los derechos y libertades fundamentales de las personas, en especial aquellas vulnerables como los menores[95]. Legitimar el tratamiento de datos en base al interés legítimo de los responsables o de un tercero supone un riesgo y una dificultad valorativa, porque si bien es cierto que se debe ponderar ese interés con los derechos y libertades de las personas, esa valoración no puede caer en la arbitrariedad y deben quedar definidos los requisitos y los límites, no se puede dar carta blanca a la hora de legitimar un tratamiento de datos personales por el mero hecho de satisfacer necesidades económicas o productivas de las empresas. El interés legítimo, para ser considerado como tal, debe ser al menos lícito, es decir, ajustado a la normativa de los Estados miembros o de la Unión, especifico y conciso, para facilitar esa ponderación en relación con los derechos y libertades fundamentales y reales, debe ser tangible, realista y asumible, no especulativo[96]. En los casos en los que existe una relación entre el responsable del tratamiento de los datos y una persona, si les une un contrato a partir del cual es cliente de bienes o servicios, se considerará que existe un interés legítimo si el cliente puede prever presumiblemente que puede producirse ese tratamiento de datos si resultara necesario para los fines del tratamiento[97]. Este requisito parece a todas luces insuficiente, porque a los clientes no se les debe presuponer ningún conocimiento técnico, máxime cuando hablamos de alta tecnología caracterizada por su complejidad y opacidad. Se considera también que existe interés legítimo, cuando

[93] REGLAMENTO (UE) 2016/679... Cit., artículo 6.1e en relación con el 6.2, 6.3 y el considerando (45)
[94] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Adecuación al RGPD de… Cit., pág. 21
[95] REGLAMENTO (UE) 2016/679... Cit., artículo 6.1f
[96] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, 9 de abril 2014, WP 217, Pág. 30 Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf
[97] REGLAMENTO (UE) 2016/679... Cit., considerando (47)

se realicen actividades destinadas a preservar la seguridad de los propios datos personales, luchar contra el fraude, fines de mercadotecnia directa como la publicidad personalizada, o la transmisión de datos personales de una empresa matriz a una filial[98].

4.1.3. Consentimiento

El consentimiento es otra base fundamental que legitima el tratamiento de datos personales, en este caso una persona cede al responsable del tratamiento sus datos personales de forma libre, voluntaria e inequívoca para un fin determinado. Para considerarse válido el consentimiento, que se entiende como un acto afirmativo claro, debe estar debidamente informado de los riesgos, la seguridad y la finalidad que supone el acceso a sus datos. Se exige un lenguaje claro y sencillo que permitan entender con facilidad esa información facilitada por el responsable del tratamiento. En el supuesto de que se faciliten datos personales con más de una finalidad distinta, el consentimiento debe ser individualizado y específico para cada uno de los fines, de lo contrario se entenderá como no prestado. Hay que tener en cuenta que del mismo modo que prestar consentimiento es una declaración de la voluntad libre, se puede retirar ese consentimiento de forma libre en cualquier momento, sin perjuicio que la actividad realizada mientras sí existía el consentimiento será legítima, se exige que las personas tengan la misma facilidad para dar el consentimiento como para retirarlo[99].

4.2. Derechos del interesado

Los interesados, es decir las personas que facilitan sus datos personales, tienen unos derechos que garantiza el RGPD:

- **Derecho de acceso:** Supone el derecho a que a los interesados se les comunique que se están tratando sus datos personales, tengan acceso a sus propios datos y se les provea una serie de información relativa a ese tratamiento. En esa información se incluye la finalidad del tratamiento, un plazo de conservación determinado o los criterios para determinarlo, la enumeración de los derechos que posee como individuo respecto a sus datos personales, incluido el derecho a presentar una reclamación y ante qué órgano debe presentarse, la legislación en la que se fundamenta el tratamiento. También debe informar, en el caso de decisiones automatizadas, de los riesgos, la lógica que sigue el sistema y sus posibles consecuencias.[100]
- **Derecho de rectificación**: Confiere a los interesados el derecho a solicitar al responsable del tratamiento la rectificación de sus datos, si estos fueran inexactos o

[98] REGLAMENTO (UE) 2016/679... Cit., considerando (47), (48) y (49)
[99] REGLAMENTO (UE) 2016/679 …Cit., artículo 7 y considerando (32)
[100] REGLAMENTO (UE) 2016/679... Cit., artículo 15 y considerando (63)

estuvieran desactualizados, o a completarlos si es que fuera necesario, de forma rápida y sencilla, sin dilaciones indebidas[101].

- **Derecho de supresión:** También conocido como derecho al olvido, confiere a los interesados la facultad de solicitar la eliminación de sus datos personales a los responsables del tratamiento, para que dejen de tratarse y sean eliminados. Para poder ejercerlo deben cumplirse unas determinadas circunstancias, como que se trate de una retención de datos ilícita, o si los datos ya no son necesarios para los fines del tratamiento, o si los interesados retiran su consentimiento, o si se oponen al tratamiento automatizado de sus datos. En los entornos *online*, los responsables del tratamiento deben asegurarse de que se elimine todo enlace o acceso a los datos suprimidos[102].
- **Derecho a la limitación del tratamiento:** Proporciona al interesado el derecho a que se limite el tratamiento de sus datos, no se eliminan sus datos, sino que dejan de ser procesados, de tal manera que sí que quedan almacenados. Este derecho se emplea cuando un interesado solicite la corrección de la inexactitud de sus datos, mientras se verifican y actualizan quedan almacenados, pero no se suprimen. Asimismo, se invoca cuando el interesado pretende que se almacenen sus datos, pero no sean tratados, cuando por ejemplo los necesite para presentar una reclamación. Los encargados del tratamiento, normalmente para facilitar la limitación del tratamiento, trasladan esos datos a otro sistema, con el objetivo de que queden almacenados y no sean tratados por error, o si se encuentran en internet, retirarlos del acceso público[103].
- **Derecho a la portabilidad de los datos:** El interesado tiene derecho a recibir los datos personales que haya facilitado a un responsable y transmitirlo a otro responsable o, si es posible, que directamente un responsable se los envíe a otro responsable si eso es técnicamente posible. Solo opera en los casos que la base jurídica del tratamiento sea el propio consentimiento del interesado o resulte necesario para la ejecución de un contrato, se exceptúan los casos de obligación legal o de interés público[104]. Este derecho se ejercita cuando una persona quiere cambiar de una empresa de la cual es cliente a otra y solicita que sus datos sean enviados a la otra empresa.

4.2.1. Derecho de oposición y decisiones individuales automatizadas

A lo largo del trabajo ya han expuesto las posibilidades que ofrecen los sistemas de IA y el concepto, funcionamiento y riesgos de las decisiones individuales automatizadas y la elaboración de perfiles. El RGPD tiene en cuenta estos riesgos y configura el derecho de oposición.

[101] REGLAMENTO (UE) 2016/679 ... Cit., artículo 16
[102] REGLAMENTO (UE) 2016/679... Cit., artículo 17 y considerandos (65) y (66)
[103] REGLAMENTO (UE) 2016/679... Cit., artículo 18 y considerando (67)
[104] REGLAMENTO (UE) 2016/679... Cit., artículo 20 y considerando (68)

A los interesados se les debe informar explícitamente de su derecho a oponerse al tratamiento de sus datos, incluida la elaboración de perfiles, cuando la legitimación del tratamiento se basa en el interés público o el interés legítimo del responsable del tratamiento. Si ejercitan ese derecho, la consecuencia inmediata será cesar, al menos temporalmente, el procesamiento de sus datos, incluida la elaboración de perfiles hasta que el caso sea analizado. En ese análisis se realizará una ponderación más minuciosa del interés público o legitimo respecto a los derechos y libertades del interesado, no bastará con que se demuestre que existe una base legítima, sino que se añade que ésta sea necesaria, apremiante e imperiosa. En el caso visto anteriormente de la pandemia por Covid 19 está claro que existe una necesidad apremiante, pero cuando la legitimación se base en motivos puramente económicos no será suficiente[105].

Este derecho también permite oponerse sin condiciones en todo momento al tratamiento de los datos utilizados para la mercadotecnia directa, es decir, la publicidad personalizada, incluido el *marketing online,* esa oposición se debe comunicar al responsable del tratamiento, que cesará de tratar los datos personales del interesado con esos fines, incluida la elaboración de perfiles dirigido a la mercadotecnia directa[106].

Las personas tienen derecho a no ser sometidas a decisiones que únicamente se basen en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, cuando no tengan supervisión humana y estas decisiones le afecten jurídica o significativamente de forma similar[107]. Con relación a lo que se considera efectos jurídicos, si bien el articulado del RGPD no lo específica, se consideran aquellos que afecten al estatuto jurídico de las personas o a sus derechos en relación con un contrato, como por ejemplo la cancelación de un contrato, la denegación de una prestación o la denegación de la admisión en un país. En cuanto a las que afectan significativamente de forma similar, para ser consideradas como tal, deben afectar de una forma relevante al comportamiento, circunstancias o las elecciones de las personas afectadas, como, por ejemplo, la denegación del acceso a un crédito, la denegación de acceso a un puesto de trabajo, a la asistencia sanitaria o al acceso a una universidad. Incluso en la elaboración de perfiles destinados a la mercadotecnia directa podría considerarse que afectan significativamente cuando se produce una monitorización de las personas mediante dispositivos o sitios web y usen las vulnerabilidades de las personas para ofrecerles publicidad[108].

Sin embargo, no es un derecho absoluto y existen excepciones a esta prohibición general, que se resumen básicamente en:

- Si la decisión es necesaria para la ejecución de un contrato: La mera existencia de un contrato no lo legitima, sino que se debe demostrar que, dada la naturaleza del

[105] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., Págs. 20 y 21
[106] REGLAMENTO (UE) 2016/679... Cit., artículos 21.2, 21.3 y considerando (70)
[107] REGLAMENTO (UE) 2016/679... Cit., artículo 22.1
[108] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., págs. 23 y 24

contrato y la cantidad de datos a procesar, no hay otro método efectivo y resulta necesaria la automatización del procesado de los datos[109].

- Si la decisión se basa en una norma de la Unión o de un Estado miembro[110].
- Si el interesado da su consentimiento explícito[111]: El RGPD no aclara en su articulado ni en los considerandos el concepto de consentimiento explícito.

En cualquier caso, al responsable del tratamiento se le exige tomar las medidas adecuadas para proteger los derechos e intereses legítimos de los interesados, a proporcionar un mínimo de supervisión humana al tratamiento de la información personal y a facilitar la información y medios de impugnación a los interesados[112].

4.2.2. Limitaciones de los derechos

Todos los derechos y principios que conforman la protección de datos explicados anteriormente no son absolutos, sino que tienen ciertas limitaciones bajo circunstancias concretas.

Siempre que sean medidas necesarias, concretas y proporcionadas en el contexto de una sociedad democrática, se podrán limitar los derechos cuando resulte imprescindible para: la protección de la seguridad del Estado, la defensa, la seguridad y la salud pública, la prevención y la investigación, el enjuiciamiento de delitos o infracciones penales, la ejecución de demandas civiles o el interés público en general. No obstante, esa limitación se llevará a cabo mediante una ley que especifique y determine detalladamente todos los aspectos sobre el tratamiento de los datos, la finalidad, la duración del plazo de conservación y toda la información relevante a efectos de garantizar la transparencia respecto a los ciudadanos[113].

4.3. Obligaciones del responsable y del encargado del tratamiento

En este apartado se analizarán algunas de las obligaciones más relevantes que afectan a los responsables y a los encargados del tratamiento de los datos personales. Cabe diferenciar a estas dos figuras, el responsable será toda persona física, jurídica o autoridad pública que por sí misma o conjuntamente con otros, determine los fines y los medios del tratamiento de los datos y, por otra parte, el encargado del tratamiento será otra persona física, jurídica o autoridad pública que trate datos personales por cuenta del responsable[114]. Se deben dar dos condiciones para ser encargado, que sea una autoridad jurídica independiente del

[109] GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales… Cit., pág. 25 y 26.
[110] REGLAMENTO (UE) 2016/679... Cit., artículo 22.2b
[111] REGLAMENTO (UE) 2016/679 ... Cit., artículo 22.2c
[112] REGLAMENTO (UE) 2016/679... Cit., artículo 22.3 y considerando (71)
[113] REGLAMENTO (UE) 2016/679... Cit., artículo 23 y considerando (73)
[114] REGLAMENTO (UE) 2016/679... Cit., artículos 4.7 y 4.8

responsable y que el tratamiento se realice por cuenta ajena[115]. En síntesis, el responsable determina la finalidad y el modo del tratamiento de los datos y el encargado es contratado por cuenta ajena para realizar el tratamiento en función de las directrices impuestas por el responsable. En todo caso, tanto si hablamos de responsables o encargados, mayoritariamente hablamos de empresas y las obligaciones que les impone el RGPD para el tratamiento de los datos personales.

4.3.1. Principio de responsabilidad proactiva o "*accountability*"

El principio de responsabilidad proactiva introducido en el artículo 5.2 del RGPD implica un cambio de estrategia de los legisladores, ante la falta de recursos y eficacia de autoridades independientes del control a la hora de supervisar el cumplimiento de la legislación en materia de protección de datos. El RGPD impone una serie de deberes y obligaciones a los responsables del tratamiento de datos, que tendrán que adaptarse a un modelo de gestión basado en códigos de conducta que determinan de qué modo se deben organizar y ejercer el tratamiento de los datos, con el objetivo de tener un mayor control de su actividad y de facilitar la comprobación del correcto cumplimiento de sus obligaciones[116]. De esta manera, los responsables del tratamiento tienen que aplicar unas medidas técnicas y organizativas internas apropiadas y eficaces para garantizar la adecuación y el respeto a los principios y los derechos que protege el RPGD, así como demostrarlo cuando se le solicite[117]. A través de este principio y del cumplimiento de las obligaciones impuestas, se pretende que las empresas tengan un papel activo y sean capaces de demostrar por qué las medidas adoptadas son adecuadas y eficaces[118].

Un claro ejemplo de la aplicación de este principio es la obligación del registro de las actividades del tratamiento, que no solo debe identificar los agentes que intervienen en el tratamiento y los responsables o encargados, sino que se tiene que llevar un registro minucioso de toda la actividad relativa y vinculada al tratamiento de los datos, con la finalidad de poder demostrar el cumplimiento del Reglamento y facilitar la supervisión de la autoridad de control y la presentación de reclamaciones de los usuarios[119].

Por otra parte, pese a que es facultativo y no obligatorio, se incita a las asociaciones u otros organismos que representan a las empresas involucradas con el tratamiento de datos a

---

[115] GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 1/2010 sobre conceptos de "responsable del tratamiento" y "encargado del tratamiento", 16 febrero 2010, WP 169, Pág. 27 Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf

[116] MARTÍNEZ MARTÍNEZ, R., "El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto" En: GARCIA MAHAMUT, R y TOMÁS MALLÉN, B (Edit.): *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de derechos digitales.* Valencia 2019, Tirant lo Blanch ISBN: 978-84-1313-429-1 págs. 316 a 323

[117] REGLAMENTO (UE) 2016/679... Cit., artículo 28 y considerandos (74) y (78)

[118] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25, protección de datos desde el diseño y por defecto. Versión 2.0, octubre 2020 Pág. 30 Disponible en: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

[119] REGLAMENTO (UE) 2016/679... Cit., artículo 30 y considerando (82)

elaborar códigos de conducta, que respeten los límites del RGPD y faciliten su aplicación y supervisión, incluyendo obligaciones especificas en base a las características del tratamiento utilizado y los riesgos derivados para los derechos y libertades de los interesados. Esos códigos de conducta están sujetos a su comprobación y aprobación por la autoridad de control competente, pero no siempre es necesaria una elaboración propia, sino que se permite que las empresas se adhieran a códigos ya existentes[120]. Asimismo, existe otro mecanismo potestativo para reforzar la transparencia y la seguridad jurídica, las certificaciones. Ofrecen un sello o una marca distintiva a los responsables o encargados del tratamiento que se sometan a un control y evaluación de su actividad, si cumplen los requisitos se les proporcionará una marca distintiva durante un periodo de 3 años[121], lo cual genera confianza y les permite distinguirse de otras empresas y sirve de garantía para los usuarios. Todas las obligaciones impuestas en el RGPD se basan en el principio de proactividad, como analizarán en el siguiente apartado.

4.3.2. Protección de datos desde el diseño y por defecto

La obligación de proteger los datos desde el diseño y por defecto introduce la protección de los datos durante todo el ciclo de vida de una IA, desde la concepción y el diseño hasta su retirada, los responsables del tratamiento deberán acreditar que han tomado todas las medidas y garantías necesarias para asegurar la efectividad de los principios, derechos y libertades que introduce el RGPD[122].

Estas medidas deben ser adecuadas teniendo en cuenta el estado de la técnica, su coste de aplicación y naturaleza, el contexto y los fines del tratamiento y los riesgos que conlleva para las personas. Se tomarán ya desde el diseño de la IA, utilizando técnicas para la minimización de datos como la seudonimización[123]. El concepto de estado de la técnica refiere a que los responsables del tratamiento deben tener en cuenta el estado actual y las posibilidades de la tecnología a la hora de determinar las medidas adecuadas para garantizar la protección de los datos, por lo tanto, deben estar al corriente de los avances tecnológicos y los riesgos implícitos en esa tecnología[124]. Se exige, además, no solo la correcta adecuación de las medidas a la tecnología actual, sino que sean efectivas, teniendo en cuenta el contexto y los medios necesarios para el tratamiento de los datos, deben ser lo suficientemente sólidas para poder aplicarlas en caso de que se produzca un incremento del riesgo[125].

En cuanto a las medidas por defecto, deben ser adecuadas para que solo se traten los datos imprescindibles para cada uno de los fines determinados, deberá prever la cantidad de datos

[120] REGLAMENTO (UE) 2016/679 ... Cit., artículos 40, 41 y considerando (98)
[121] REGLAMENTO (UE) 2016/679... Cit., artículo 42 y considerando (100)
[122] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25… Cit., pág. 5
[123] REGLAMENTO (UE) 2016/679... Cit., artículo 25.1 y considerando (78)
[124] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25… Cit., págs. 8 y 9
[125] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25… Cit., págs. 7 y 8

necesarios, el plazo de conservación de los datos y, sobre todo, la accesibilidad a estos, en particular deben asegurar que no se producirán intromisiones ilegítimas sin la intervención del interesado de terceras personas[126]. La accesibilidad de terceras personas es un factor clave en los sistemas de IA que operan *online,* sea a través de motores de búsqueda o las redes sociales, por ello se obliga al responsable del tratamiento a limitar la accesibilidad de los datos y ofrecer al interesado la opción de intervenir antes de que sus datos sean accesibles en la internet púbica para terceros. Para ello existen varias vías, si el tratamiento se basa en el consentimiento se puede requerir para la publicación de sus datos al acceso público o también, dar el control de la accesibilidad al interesado, pudiendo establecer configuraciones de privacidad que les permita controlar el acceso público[127], como por ejemplo cuando un usuario de una red social solo permite el acceso a su perfil a sus seguidores.

Estas obligaciones son aplicables para todos los responsables, independientemente del volumen y la complejidad del tratamiento que se lleva a cabo o las dimensiones de la empresa, por lo que es aplicable a las pequeñas y medianas empresas[128].

4.3.3. Evaluación de impacto relativa a la protección de datos

Cuando los responsables del tratamiento ya tienen definida la finalidad y el modo de tratar los datos personales teniendo en cuenta las consideraciones anteriores, se deben analizar los riesgos inherentes de ese tratamiento para la privacidad de las personas. Cuando sea probable que un determinado tipo de tratamiento de datos ya sea por su alcance, la naturaleza de la tecnología empleada, contexto y el tipo de finalidad perseguida suponga un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento estará obligado, antes de proceder a iniciar el tratamiento de los datos, a realizar una evaluación del impacto del tratamiento de esas operaciones respecto a la protección de datos de las personas. Esa evaluación debe incluir las medidas y garantías para minimizar los riesgos y garantizar la protección de datos en los términos establecidos en el RGPD[129]. Implica la obligación de analizar los riesgos, atendiendo a las consecuencias probables y la gravedad de estas respecto al tratamiento de los datos para los derechos y libertades de las personas, y a tomar las medidas necesarias para gestionar esos riesgos y reducirlos[130]. Esa obligación no es aplicable a todos los tratamientos de datos, solo a los de alto riesgo, no obstante, incluso aunque no sea obligatorio en el momento inicial al tratamiento de los datos, no exime a los responsables de mantener una evaluación continua de los riesgos durante el ciclo de vida de la IA y el tratamiento de los datos, así como identificar la probabilidad de

[126] REGLAMENTO (UE) 2016/679 …Cit., artículo 25.2 y considerando (78)
[127] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25… Cit., pág. 14
[128] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25… Cit., págs. 4 y 6
[129] REGLAMENTO (UE) 2016/679... Cit., artículo 35.1 y considerando (90)
[130] GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, revisadas 4 octubre 2017, WP 248 rev.01. pág. 7 Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

que en algún momento el tratamiento suponga un alto riesgo[131]. Esa evaluación se puede realizar para un único tratamiento específico o para varios, si tienen naturaleza y riesgos conexos[132].

La evaluación será obligatoria debido al alto riesgo inherente de los siguientes tratamientos de datos:

- Los que analicen y evalúen aspectos personales basados en tratamientos automatizados, incluida la elaboración de perfiles y cuyas decisiones afecten jurídicamente o de forma similar a las personas[133].
- Los tratamientos a gran escala de datos personales de categorías especiales de datos o datos relativos a sanciones o condenas penales, como datos médicos o relativos a menores de edad[134].
- Observación sistemática a gran escala de un acceso público[135].
- Datos relativos a interesados vulnerables, como niños, empleados, discapacitados o personas mayores que no puedan ser capaces de autorizar y denegar el acceso a sus datos[136].

No es necesario que se cumplan todos estos supuestos, en ocasiones con que su cumpla uno será suficiente, se debe valorar adecuadamente el riesgo por el responsable del tratamiento y justificar motivadamente en caso de no apreciar necesidad de ello[137].

En caso de que el responsable del tratamiento haya designado un delegado de protección de datos deberá consultar su asesoramiento para la confección y aprobación de la evaluación[138]. También, en caso de ser obligatoria la evaluación, se deberá facilitar a la autoridad de control antes del tratamiento de los datos, que deberá examinar su adecuación al RGPD para poder autorizar el tratamiento de los datos, o asesorar sobre los cambios que se deben introducir en caso de que la evaluación no se ajuste al RGPD[139].

Respecto al contenido mínimo que debe incluir la evaluación, es el siguiente[140]:

- Descripción de las operaciones de tratamiento previstas, de los fines del tratamiento y del interés legítimo perseguido, cuando proceda.
- Evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento elegidas respecto la adecuación con la finalidad perseguida.
- La correcta identificación de los riesgos y su afectación probable a los derechos y libertades de las personas.

---

[131] GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto… Cit., pág. 7
[132] REGLAMENTO (UE) 2016/679… Cit., artículo 35.1
[133] REGLAMENTO (UE) 2016/679 ... Cit., artículo 35.3a y considerando (91)
[134] REGLAMENTO (UE) 2016/679... Cit., artículo 35.3b y considerando (91)
[135] REGLAMENTO (UE) 2016/679... Cit., artículo 35.3c y considerando (91)
[136]GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto… Cit., pág. 11
[137] GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto… Cit., págs. 12 y 13
[138] REGLAMENTO (UE) 2016/679... Cit., artículo 35.2
[139] REGLAMENTO (UE) 2016/679... Cit., artículo 36
[140] REGLAMENTO (UE) 2016/679... Cit., artículo 35.7

- Las medidas y garantías que se ofrecen para minimizar los riesgos identificados, incluyendo todas las medidas de seguridad necesarias.

4.3.4. Delegado de protección de datos

La figura del delegado de protección de datos es especialmente relevante, ya que permite garantizar la rendición de cuentas a través de sus actuaciones como intermediario entre las empresas, los interesados y las autoridades de control, así como también a la hora de facilitar el cumplimiento del RGPD, a través de las evaluaciones de impacto y las auditorías de datos[141].

Sin embargo, no siempre resulta obligatoria su designación, aunque en todo caso los obligados a designarlo son el encargado y el responsable del tratamiento de los datos[142], siempre que se den estos supuestos:

- Que el tratamiento lo lleve a cabo una autoridad u organismo público, aunque se exceptúan los tratamientos de los tribunales de justicia o de las autoridades judiciales[143].
- Que el tratamiento y la actividad de los responsables y encargados consistan en operaciones que, por su naturaleza, alcance o fines, requieran una observación habitual y sistemática a gran escala de las personas[144], incluida la elaboración de perfiles. Para poder determinar si un tratamiento implica ese tipo de observación a gran escala se debe atender al volumen de los datos, sea la cifra total de personas afectadas o una proporción de población, la variedad de datos analizados de esas personas, el tiempo de duración y la permanencia de la observación, así como el alcance geográfico de la actividad del tratamiento[145]. Un ejemplo de este tipo de tratamientos sería el tratamiento de datos personales para publicidad *online* directa basada en el análisis de motores de búsqueda, como *google*[146].
- Que la actividad consista en el tratamiento de datos a gran escala de categorías especiales de datos o sanciones e infracciones penales[147].

Para ser delegado no se exige ningún requisito o titulación específica, dependerá del tipo de tratamiento y de los fines perseguidos en cada caso, sin embargo, es recomendable tener conocimientos jurídicos en materia de protección de datos[148]. No necesariamente tiene que formar parte de la plantilla de la empresa del encargado o del responsable, se puede contratar

[141] GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre los delegados de protección de datos (DPD), revisada 5 abril 2017, WP 243 rev.01 Pág. 4 Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf
[142] REGLAMENTO (UE) 2016/679... Cit., artículo 37.1
[143] REGLAMENTO (UE) 2016/679... Cit., artículo 37.1a y considerando (97)
[144] REGLAMENTO (UE) 2016/679... Cit., artículo 37.1b y considerando (97)
[145] GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre los delegados… Cit., Pág. 8
[146] GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre los delegados… Cit., Pág. 9
[147] REGLAMENTO (UE) 2016/679... Cit., artículo 37.1c y considerando (97)
[148] REGLAMENTO (UE) 2016/679... Cit., artículo 37.5 y considerando (97)

mediante un contrato de servicios[149], en cualquier caso, los delegados no serán responsables en caso de un incumplimiento del RGPD, pues los responsables seguirán siendo el encargado y/o el responsable del tratamiento[150].

Entre sus funciones más destacadas, se encuentran las de asesorar e informar al encargado o responsable del tratamiento de las medidas adecuadas para garantizar el cumplimiento del RGPD, supervisar que las actuaciones sean conformes al reglamento, confeccionar o asesorar en la realización de evaluaciones de impacto, y ser el nexo de comunicación entre la empresa y la autoridad de control[151].

4.3.5. Seguridad

Una vez se ha producido la evaluación de los riesgos del tratamiento de los datos conforme a lo señalado en apartados anteriores, los responsables y encargados del tratamiento aplicarán las medidas técnicas y organizativas necesarias, pertinentes y efectivas para garantizar un nivel de seguridad adecuado a los riesgos[152], para ello esas medidas deben incluir:

- Técnicas de seudonimización, de cifrado de datos o de anonimización para dificultar la identificabilidad de las personas con respecto a sus datos personales[153].
- Medidas técnicas y organizativas capaces de asegurar la confidencialidad y la integridad de los datos y de los sistemas donde se encuentren almacenados, para prevenir su destrucción, alteración o el acceso no autorizado[154].
- Sistemas que permitan recuperar la disponibilidad y acceso de los datos en caso de incidencia[155].
- Mecanismos de vigilancia y eficacia que controlarán regularmente el funcionamiento de los sistemas de seguridad[156].

Mantener una seguridad adecuada es imprescindible, ya que las violaciones de seguridad pueden causar daños y perjuicios a las personas, como pérdida de datos sensibles como financieros, suplantación de la identidad, pérdida del control sobre sus datos personales, pérdida de la confidencialidad, intromisiones ilegítimas en su intimidad, discriminación o restricción de sus derechos entre otros muchos perjuicios[157]. Frente a la gravedad de las posibles consecuencias, se exige a los responsables y encargados del tratamiento que actúen sin dilación ante una brecha de seguridad, imponiéndoles la obligación de comunicar dicha situación a la autoridad de control competente, en un plazo inferior a setenta y dos horas. En esa comunicación se debe describir la violación de seguridad, los hechos relacionados

[149] REGLAMENTO (UE) 2016/679... Cit., artículo 37.6 y considerando (97)
[150] GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre los delegados… Cit., Pág. 5
[151] REGLAMENTO (UE) 2016/679... Cit., artículo 39
[152] REGLAMENTO (UE) 2016/679... Cit., artículo 32.1
[153] REGLAMENTO (UE) 2016/679... Cit., artículo 32.1a y considerando (83)
[154] REGLAMENTO (UE) 2016/679... Cit., artículo 32.1b y considerando (83)
[155] REGLAMENTO (UE) 2016/679... Cit., artículo 32.1c
[156] REGLAMENTO (UE) 2016/679 ... Cit., artículo 32.1d
[157] REGLAMENTO (UE) 2016/679... Cit., considerando (85)

con la misma, los efectos que ha producido y las medidas que se han tomado para mitigar los efectos[158].

Esa exigencia no opera con la misma intensidad respecto al deber de comunicación de los encargados o responsables frente a los interesados, ya que para que sea necesaria, debe existir un riesgo alto y probable de vulneración de sus derechos y libertades[159]. Sin embargo, en algunas ocasiones incluso pese a la existencia de ese riesgo no será necesaria la comunicación individualizada; como en los casos en los que se hayan cifrado los datos para preservar su seguridad y estos sean ilegibles, cuando se haya subsanado la violación a través de medidas posteriores y se haya extinguido el riesgo, o cuando suponga un esfuerzo desproporcionado, en cuyo caso bastará con un comunicado oficial público de la empresa que ha sufrido la vulneración de seguridad[160]. No obstante, la autoridad de control podrá requerir si lo estima oportuno a los responsables o encargados del tratamiento, la notificación a los interesados afectados[161]. En todo caso, de producirse la comunicación, informará debidamente a los interesados de las circunstancias de la violación de seguridad y recomendaciones de actuación para mitigar los posibles efectos adversos, así como mantendrán una comunicación estrecha para facilitar la cooperación con la autoridad de control competente[162].

4.4. Incumplimiento y sanciones

4.4.1. Autoridad de control

Cada Estado miembro de la Unión debe nombrar una o varias autoridades públicas independientes[163], en el caso de España, ese organismo designado es la Agencia Española de Protección de Datos[164].

El RGPD le atribuye a la autoridad de control muchas funciones, por destacar algunas[165]:

- Controlar la aplicación del reglamento.
- Asesorar a los gobiernos e instituciones públicas.
- Asesorar y sensibilizar a los encargados y responsables del tratamiento de sus obligaciones.
- Cooperar y compartir información con otras autoridades de control.
- Investigar sobre el reglamento y elaborar guías de su aplicación.
- Mantenerse actualizado sobre los cambios tecnológicos que puedan afectar al tratamiento de datos personales y a las nuevas tecnologías de comunicación e información y prácticas comerciales.

[158] REGLAMENTO (UE) 2016/679... Cit., artículos 33.1, 33.5 y considerando (85)
[159] REGLAMENTO (UE) 2016/679... Cit., artículo 34.1
[160] REGLAMENTO (UE) 2016/679... Cit., artículo 34.3
[161] REGLAMENTO (UE) 2016/679... Cit., artículo 34.4
[162] REGLAMENTO (UE) 2016/679…Cit., considerando (86)
[163] REGLAMENTO (UE) 2016/679... Cit., artículo 51.1
[164] LEY ORGÁNICA 3/2018 … Cit, artículos 44 y ss.
[165] REGLAMENTO (UE) 2016/679... Cit., artículo 57.1

- Examinar los códigos de conducta y las evaluaciones de impacto y pronunciarse sobre su adecuación al Reglamento.
- Imposición de multas administrativas por incumplimiento del RGPD.

En especial, la función que cabe destacar es que se encargan de tratar las reclamaciones presentadas por las personas físicas o por organismos, investigar el motivo de la reclamación e informar del resultado al interesado. Las reclamaciones pueden realizarse vía web mediante un formulario y de forma gratuita[166].

4.4.2. Reclamaciones

Las personas que consideren que han sufrido una vulneración de su derecho a la protección de datos mediante el incumplimiento del RGPD, sin perjuicio de la potestad de acudir a los tribunales de justicia, pueden presentar una reclamación ante la autoridad de control situada en el Estado miembro donde resida habitualmente, trabaje, o donde se produzca la infracción[167]. Si la reclamación se fundamenta en una decisión o resolución vinculante de la autoridad de control, el interesado podrá acudir a los tribunales de justicia del país donde esté establecida esa autoridad de control para su impugnación[168]. Asimismo, los interesados están facultados para actuar judicialmente frente a los responsables o encargados del tratamiento de los datos, ejerciendo la tutela judicial efectiva ante los tribunales donde éstos tengan algún establecimiento, empresa matriz o sucursal, o donde el interesado tenga su residencia habitual[169].

4.4.3. Indemnizaciones

La reclamación de los interesados puede generar el derecho a recibir una indemnización del responsable o el encardado del tratamiento de los datos por los daños y perjuicios sufridos, ya sean materiales o inmateriales, entendidos en sentido amplio, como consecuencia de una infracción de las normas contenidas en el RGPD[170]. Ese sentido amplio a la hora de valorar la naturaleza de los daños y perjuicios juga a favor de los interesados, ya que al no estar tasados estrictamente no se excluye ningún supuesto específico y en todo caso será analizada la situación. Podría entrar en esa categoría tanto alguna pérdida económica, patrimonial o cualquier intromisión en la privacidad que cause algún daño moral, que por su naturaleza puede ser muy variado.

La reclamación debe ir dirigida contra el responsable o encargado del tratamiento y, como en cualquier reclamación civil, aparte de identificar al causante o responsable del daño, debe demostrar el incumplimiento de alguna disposición del RGPD, probar el daño causado, el

[166] REGLAMENTO (UE) 2016/679... Cit., artículos 57.1f, 57.2 y 57.3
[167] REGLAMENTO (UE) 2016/679…Cit., artículo 77.1 y considerando (141)
[168] REGLAMENTO (UE) 2016/679... Cit., artículo 78 y considerando (141)
[169] REGLAMENTO (UE) 2016/679... Cit., artículo 79
[170] REGLAMENTO (UE) 2016/679... Cit., artículo 82.1 y considerando (146)

nexo de causalidad entre el incumplimiento y el daño, así como la imputabilidad de la acción u omisión al responsable o encargado.

Conviene señalar, que el daño no solo se puede fundamentar en el incumplimiento manifiesto del RGPD, sino que también en actos delegados o ejecutivos[171], que por el principio de responsabilidad proactiva sean de obligado cumplimiento para los responsables o encargados.

En cuanto a los sujetos responsables del daño que tienen el deber de satisfacer al interesado la indemnización, dependerá de su participación o de su diligencia a la hora de cumplir la normativa. El responsable del tratamiento será causante del daño si ha participado en la operación que lo ha causado y se ha producido por incumplir la normativa, por su parte, el encargado responderá si ha participado en la operación y ha actuado incumpliendo la normativa o ha desarrollado su actuación al margen y en contra de las instrucciones que le dio el responsable del tratamiento[172]. Si la participación es conjunta, al margen de que se pueda valorar el grado de responsabilidad de cada uno, responderán conjuntamente y de forma solidaria, sin perjuicio de la facultad de cualquiera que satisfaga la indemnización de actuar y reclamar dichas cantidades al otro sujeto[173].

En todo caso, se exige que las indemnizaciones, de ser pertinentes, sean suficientes para la reparación total y efectiva de los daños sufridos[174].

Al margen de la indemnización a los perjudicados, las empresas se pueden enfrentar a multas administrativas y sanciones por el incumplimiento del RGPD. Las multas administrativas las impone la autoridad de control competente y las cuantías varían en función de la naturaleza de la infracción, de las características de la operación y de las medidas adoptadas para tratar de subsanar o mitigar los efectos del incumplimiento[175]. Dependiendo de esas circunstancias, esas cuantías pueden variar entre diez millones de euros como máximo o el 2% del volumen de negocio total anual de la empresa, hasta los veinte millones de euros como máximo o el 4% del volumen de negocio total anual[176].

En cuanto a las sanciones, las establecen los Estados miembros en sus legislaciones y, en todo caso, deben ser proporcionadas, efectivas y disuasorias[177].

[171] REGLAMENTO (UE) 2016/679... Cit., considerando (146)
[172] REGLAMENTO (UE) 2016/679... Cit., artículo 82.2 y considerando (146)
[173] REGLAMENTO (UE) 2016/679... Cit., artículos 82.4, 82.5 y considerando (146)
[174] REGLAMENTO (UE) 2016/679... Cit., considerando (146)
[175]REGLAMENTO (UE) 2016/679... Cit., artículo 83
[176] REGLAMENTO (UE) 2016/679... Cit., artículos 83.4 y 83.5
[177] REGLAMENTO (UE) 2016/679... Cit., artículo 84

CONCLUSIONES

En el presente trabajo no se han abordado todas las cuestiones posibles, ni siquiera se ha realizado un análisis completo del RGPD, solo lo más relevante, con lo que se podría profundizar mucho más. Este trabajo debe servir como una introducción a los aspectos básicos que rigen la IA y la protección de datos, pero permite llegar a una serie de conclusiones.

Es innegable que la tecnología y, concretamente, la IA nos hace la vida más fácil y nos aporta unas posibilidades con las que ni hubiéramos podido soñar hace apenas 40 años. Ha quedado claro mediante la exposición de sus usos y aplicaciones actuales los beneficios que aporta a la sociedad, sin embargo, también se han señalado los riesgos sociales, éticos y para la intimidad personal que conllevan.

En ese sentido, a pesar de la pertinencia de normas promulgadas por la UE que prohíben entre otras cuestiones, la discriminación y el sesgo, a nuestro juicio se quedan prácticamente en una enumeración de normas dispositivas y de principios generales, que, aunque son de obligado cumplimiento y cuentan con mecanismos de garantías y reclamaciones, en el fondo no ofrecen una solidez suficiente, al no concretar medidas y obligaciones concretas que permitan un control adecuado. Sobre todo, en cuanto a que no se aporta una solución tangible al problema de la opacidad, lo que dificulta enormemente concretar en base a que se a ejecutado una determinada decisión automatizada, que puede repercutir en los derechos y libertades de las personas, negándole el acceso a contratos, servicios o subvenciones.

A corto plazo estos sistemas van a ser capaces de sustituir a los seres humanos y a destruir millones de empleos, sobre todo en el sector servicios, atención al cliente, y centros logísticos, entre otros, como las propias administraciones públicas. Hay que tener en cuenta que aún no se han explotado todas las posibilidades que pueden llegar a ofrecer estos sistemas, pero las empresas ya están implementando estas tecnologías por el ahorro en el personal y la optimización de la productividad que ofrecen. No hay por ahora ningún plan de contingencia o de actuación, que plantee soluciones ante este cambio socioeconómico que, sobre todo, afectará a los trabajadores menos cualificados pero que podrían llegar a sectores insospechados como la administración de justicia.

Hoy en día, la sociedad dispone de una gran variedad de dispositivos inteligentes, plataformas y herramientas que ofrecen servicios de comunicación, entretenimiento y consumo de bienes e información, el uso de los cuales contratamos mediante el pago de una suscripción o mediante la aceptación de sus términos y condiciones del servicio. En el fondo, sea mediante pago o con contraprestación mediante el acceso a nuestros datos personales como hemos visto en el presente trabajo, estamos suscribiendo un contrato de adhesión, del cual como usuarios somos la parte débil. En todos estos sistemas están integrados la IA, que tratan nuestros datos personales. Aunque el consentimiento y la aceptación de esos términos legitima el procesamiento y el tratamiento de los datos personales de los usuarios, esa aceptación no siempre se sustenta en un consentimiento debidamente informado y una transparencia integral. Para ello, el RGPD exige un lenguaje sencillo y claro donde se especifiquen también los riesgos, pero si observamos los términos

y condiciones al contratar o registrarnos en algún servicio, no se detallan con una claridad suficiente para ser comprendido por cualquier persona. Además, la normativa carece de mecanismos que permitan comprobar la efectividad de ese proceso de información.

De ese problema se deriva que en muchas ocasiones, las personas no sean conscientes del tratamiento de sus datos y la inclusión de estos en la elaboración de perfiles, hecho que se traduce en la dificultad de ejercitar el derecho de oposición a ese tratamiento y de los riesgos éticos y para la privacidad inherentes de este tipo de practicas como el sesgo, la discriminación, la utilización de las vulnerabilidades de las personas con fines de mercadotecnia y la monitorización del comportamiento de las personas.

Otra base que legitima el tratamiento de los datos personales es el interés legítimo de las empresas, respecto a esta cuestión el RGPD es poco especifico, en relación con que elementos se tienen en cuenta a la hora de poner en la balanza la protección de los derechos y libertades de las personas y el interés económico de una empresa. Esto se traduce en la existencia de una dificultad valorativa a la hora de determinar cuando es aceptable ese interés legítimo y cuando no procede. El RGPD debería dar mas certidumbre a esta cuestión.

Por otra parte, es cierto que la incorporación en el RGPD del principio de responsabilidad proactiva aporta cierta seguridad jurídica y facilita el control de las actuaciones de las empresas respecto al tratamiento de los datos personales, pero se queda a medio camino de representar una garantía real y efectiva. Este hecho se deduce, sobre todo, de las obligaciones de respetar la privacidad desde el diseño y, por defecto, de la elaboración de evaluaciones del impacto del tratamiento de los datos. Aunque son dos elementos muy relevantes y permiten, en cierto modo, garantizar desde el momento en el que se concibe el tratamiento y en función del riesgo que represente, la protección de datos durante todo el ciclo de vida de la IA, se deja en manos de las empresas la elaboración de las medidas que considere oportunas para conseguirlo. En este sentido, consideramos que se deberían pautar reglas y medidas concretas en función del tipo de tratamiento y del riesgo que represente, a modo de códigos de conducta. La adhesión o la elaboración de códigos de conducta es voluntario en el RGPD, consideramos que para armonizar la actuación de las empresas y para ofrecer una garantía real y efectiva, la actuación y el tratamiento de los datos deben estar integrados en códigos de conducta estrictos.

En esa línea, la figura del delegado de protección de datos también es útil y debería ser obligatorio en todo caso su nombramiento, a efectos de asegurar que un profesional con conocimientos jurídicos y técnicos supervise y asesore en todo momento la actuación de las empresas.

Respecto a las personas y sus derechos, el RGPD específica y detalla los mismos, aporta mecanismos de reclamación en caso de daños y perjuicios, pero no acaba de garantizar mecanismos realmente efectivos para hacer valer esos derechos.

A nuestro juicio, el marco jurídico actual no garantiza la protección real y efectiva de nuestros datos personales, ni aporta soluciones tangibles para los riesgos éticos, morales, ni para la intimidad de las personas, por los motivos expuestos anteriormente.

El RGPD es en ocasiones ambiguo, poco concreto y deja muchos aspectos importantes a la interpretación. Es cierto que la lectura de los considerandos aporta algo de información extra que el articulado no incluye, pero no deja de ser más descriptivo que explicativo.

Hay que tener en cuenta que el Derecho va por detrás de los cambios sociales, las normas que den respuesta a los cambios y necesidades de la sociedad siempre van a llegar tarde. Este hecho se acentúa mas, si cabe, cuando hablamos de derecho y tecnología, ya que ésta avanza a un ritmo vertiginoso. No obstante, el Derecho tiene que dar respuesta a las necesidades y problemas que plantea el uso de la tecnología y es positivo que desde la UE se esté trabajando en ello. El RGPD es solo un punto de partida, queda un largo camino por recorrer, empezando por una normativa más detallada, completa e imperativa, sin olvidar que desde la UE como institución se debe concienciar e informar debidamente a las personas respecto a la importancia de sus datos personales.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción., febrero 2020. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Guía de buenas prácticas en protección de datos para proyectos de big data. mayo 2017. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

BOTANA AGRA, J.M., "Protección jurídica de algoritmos y programas de ordenador". En: GARCÍA VIDAL, A. (Dir.): *Big Data e internet de las cosas. Nuevos retos para el Derecho de la competencia y de los bienes inmateriales*. Valencia: Tirant lo Blanch, 2020, ISBN: 13 9788413781925.

CABALLERO VILLARASO, J., TABARES, A.R., GAVILÁN LEÓN, F.J., BUENA GARCÍA, M. y DÍAZ VEGA, F.J., Aplicación de algoritmos genéticos y sistemas expertos en medicina asistencial. Aplicaciones clínicas de la inteligencia artificial. AETSA 2009/6. Disponible en: https://www.aetsa.org/download/publicaciones/antiguas/AETSA_2009-6_Algoritmos_geneticos.pdf

COMISIÓN EUROPEA, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa. COM (2018) 237 final, Bruselas, 25.4.2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0237&from=ES

COMISIÓN EUROPEA, Directrices éticas para una IA fiable. Grupo independiente de expertos de alto nivel sobre inteligencia artificial. 8 de abril de 2019. Disponible en: https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

COMISIÓN EUROPEA, Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica. Bruselas 19.2.2020 COM (2020) 64 final. Pág. 2. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, Directrices 4/2019 relativas al artículo 25, protección de datos desde el diseño y por defecto. Versión 2.0, octubre 2020 Disponible en: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

GRUPO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, revisadas 4 octubre 2017, WP 248 rev.01 Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 1/2010 sobre conceptos de "responsable del tratamiento" y "encargado del tratamiento", 16 febrero 2010, WP 169. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 4/2007 sobre el concepto de datos personales (WP29). WP 136. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a efectos del Reglamento 2016/679, WP251rev.01, 6 Febrero 2018. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Directrices sobre los delegados de protección de datos (DPD), revisada 5 abril 2017, WP 243 rev.01.Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 05/2014 sobre técnicas de anonimización. WP216. 10 abril 2014. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, 9 de abril 2014, WP 217, Pág. 30 Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

LÓPEZ ONETO, M., *Fundamentos para un derecho de la inteligencia artificial. ¿Queremos seguir siendo humanos?* Tirant lo Blanch, 2020. ISBN: 978-84-1336-884-9. Pág. 51.

MARTÍNEZ MARTÍNEZ, R., "El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto" En: GARCIA MAHAMUT, R y TOMÁS MALLÉN, B (Edit.): *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de derechos digitales.* Valencia 2019, Tirant lo Blanch ISBN: 978-84-1313-429-1 págs. 316 a 323

MATEO BORJE, I., "La robótica y la inteligencia artificial en la prestación de servicios jurídicos" En: NAVAS NAVARRO, S. (Dir): *Inteligencia Artificial. Tecnología Derecho*. Tirant lo Blanch, 2017. ISBN: 13 9788491697213.

MERCHÁN MURILLO; A., "Retos regulatorios en torno a la Inteligencia Artificial". *Pensar, revista de ciencias jurídicas.* Nº23, 2018.

NAVAS NAVARRO, S., "Datos personales y mercado" En: NAVAS NAVARRO, S. (Dir): *Inteligencia Artificial. Tecnología Derecho*. Tirant lo Blanch, 2017. ISBN: 13 9788491697213.

ONU, Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. CNUDMI/UNICTRAL. Aspectos jurídicos de los contratos inteligentes y la inteligencia artificia1. Presentado por Chequia, New York, 25/06/2018, Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V18/037/81/PDF/V1803781.pdf?OpenElement

PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, 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)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.pdf

PETTERI ROUHIAINEN, L. Inteligencia Artificial. 101 cosas que debes saber sobre nuestro futuro. Editorial planeta, 2018. ISBN: 978-84-17568-08-5.

PINO DÍEZ, R., GÓMEZ GÓMEZ, A., y DE ABAJO MARTÍNEZ, N. *Introducción a la ingeniería Artificial: Sistemas Expertos, Redes Neuronales Artificiales y Computación Evolutiva*. Servicio de publicaciones de la Universidad de Oviedo 2001 ISBN: 84-8317-249-6.

SORIANO ARNANZ, A. "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos". *Revista de derecho público: Teoría y Método*. Marcial Ponts ediciones jurídicas y sociales, nº 3, 2021. ISSN: 2695-7191.

Normativa

Carta de Derechos Fundamentales de la Unión Europea, diciembre 2000. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

CONSTITUCIÓN ESPAÑOLA, 1978. Artículos 10.1 y 18.4. BOE núm. 311, de 29/12/1978.

Directiva 95/46/ CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales. BOE núm. 298, de 14/12/1999.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE, núm. 294, de 6 de diciembre de 2018, pp. 119788 a 119857.

Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales. BOE, núm. 262, de 31 de octubre de 1992, págs.37037 a 37045.

PARLAMENTO EUROPEO, Proposal for a regulation of the European Parliament and of the council. laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Brussels, 21.4.2021. COM(2021) 206 Final. 2021/0106 (COD) Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206&qid=1620488018088

PARLAMENTO EUROPEO, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales. Bruselas 9.12.2015. COM(2015) 634 final. 2015/0287 (COD). Considerando (13) Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015PC0634&from=EN

REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Tratado de Funcionamiento de la Unión Europea. Versión consolidada 30.3.2010. Disponible en: https://www.boe.es/doue/2010/083/Z00047-00199.pdf

Jurisprudencia

STC 292/2000, de 30 de noviembre de 2000, Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

Webs

Página web de Apple, donde explican las características y funciones de su reloj. Disponible en: https://www.apple.com/es/apple-watch-series-6/