Año 2024 Nº 25

CORTES DE CASTILLA-LA MANCHA • UNIVERSIDAD DE CASTILLA-LA MANCHA

Anuario

Parlamento y Constitución

Protección De Datos En Aplicación De Sistemas De Inteligencia Articial Conforme Al Rgpd

Data Protection In Artificial Intelligence Systems Application According To Gdpr

María Pérez-Ugena Coromina
Universidad Rey Juan Carlos
maria.perezugena@urjc.es
ORCID 0000-0002-2724-6882

Cómo citar/Citation

Pérez-Ugena, M., "Protección de datos en aplicación de sistemas de inteligencia artificial conforme al RGPD", en *Parlamento y Constitución. Anuario*. Cortes de Castilla – La Mancha – UCLM, nº 25, 2024

Recibido: 03-03-2024
Aceptado: 1-06-2024

Resumen*:* El objeto de este trabajo es llevar a cabo un análisis de la regulación del régimen de protección de datos en lo que afecta al uso la inteligencia artificial, de acuerdo con lo que establece el RGPD. Se plantea si los cambios que conllevan la aparición disruptiva de esta tecnología exigen nuevas normas reguladoras, más allá del RGPD, que vengan a garantizar un ámbito de privacidad. Se hace referencia, como una de las cuestiones claves, a la necesidad de implementar medidas de seguridad. El trabajo se detiene en la capacidad de oponerse al tratamiento de datos automatizados, así como a la creación de perfiles y la diferencia entre ambos. Las conclusiones resaltan la importancia de un enfoque ético y responsable en el desarrollo y aplicación de la IA, priorizando el respeto a los derechos individuales y la protección de la privacidad.

Palabras clave: Inteligencia artificial, derecho, protección de datos.

Abstract: The aim of this work is to carry out an analysis of the regulation of the data protection regime as it affects the use of artificial intelligence, in accordance with what is established by the GDPR. It is questioned whether the changes brought about by the disruptive emergence of this technology require new regulatory standards, beyond the GDPR, to ensure a realm of privacy. One of the key issues mentioned is the need to implement security measures. The study focuses on the ability to object to automated data processing, as well as the creation of profiles and the difference between the two. The conclusions highlight the importance of an ethical and responsible approach in the development and application of AI, prioritizing respect for individual rights and privacy protection.

Key words: Artificial intelligence, right, data protection.

SUMARIO

1. Introducción.

En la era digital el desarrollo de los sistemas de inteligencia artificial (IA), que conlleva nuevas técnicas de recopilación y tratamiento de datos masivos, exige, necesariamente, fortalecer el sistema de normas éticas y jurídicas que afectan a la privacidad y, más en concreto, al régimen protección de datos personales.[1] Las capacidades de los nuevos sistemas, inimaginables hasta la aparición disruptiva de la inteligencia artificial, obligan a procesar ingentes cantidades de datos a una enorme velocidad. Es preciso plantearse si la regulación actual es suficiente para garantizar el cumplimiento de los derechos que garantizan la privacidad a través de la protección de los datos personales.[2] El problema surge como consecuencia de que el Derecho va siempre después de la tecnología y una vez que se toma conciencia de los problemas que surgen con los nuevos desarrollos tecnológicos[3]. Esta realidad se ha evidenciado, de forma impensable hasta el momento, con la aparición de la inteligencia artificial.

A efectos de análisis de la cuestión, es preciso tener en cuenta, de una parte, las dificultades que implica el desarrollo tecnológico en el intento de salvaguardar la privacidad y la confidencialidad en un entorno marcado por el uso masivo de tecnologías que utilizan IA y que actúan gracias a la recopilación, procesamiento y análisis de enormes conjuntos de datos mediante algoritmos avanzados[4]. Además, existen una serie de problemas añadidos, derivados de la aplicación territorial de las leyes en el mundo global de actuación de Internet.[5] Lo que exige tener en cuenta los problemas de aplicación en otros sistemas jurídicos en los que los derechos del ámbito de la privacidad no obtienen el mismo grado de protección. De manera que los distintos ordenamientos jurídicos, han optado por soluciones diferentes con el fin de adaptarse a la rápida evolución de la IA, en la búsqueda de un equilibrio entre la innovación tecnológica y la preservación de los derechos fundamentales. Se parte de la descripción del marco general de protección de datos existente en la Unión Europea, así como de la necesidad de controlar el cumplimiento de la normativa en las distintas etapas de actuación de la IA. Se tienen en cuenta los derechos de los titulares de los datos, así como la necesidad de contar con el consentimiento, pese a las dificultades que esto supone en este contexto.

1 En este sentido, la UNESCO en su Recomendación sobre la ética de la inteligencia artificia, adoptada el 23 de noviembre de 2021 ha señalado a este respecto: *"La privacidad, que constituye un derecho esencial para la protección de la dignidad, la autonomía y la capacidad de actuar de los seres humanos, debe ser respetada, protegida y promovida a lo largo del ciclo de vida de los sistemas de IA"*. En: https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence (Obtenido en 2 de febrero de 2024)

Es igualmente clave la cuestión de la seguridad de los datos, que se pone en relación con la responsabilidad y la rendición de cuentas en el contexto de sistemas de IA. La opacidad inherente a ciertos algoritmos, que se relaciona con la falta de transparencia[6] y la toma de decisiones autónoma obligan a establecer marcos legales claros que definan la responsabilidad tanto de los desarrolladores, como de los usuarios o entidades regulatorias.

De entre los distintos derechos del ámbito del *habeas data* se interesa especialmente este trabajo por el de oposición frente a las decisiones automatizadas, sin intervención humana, basadas únicamente en algoritmos. Para su análisis se hace referencia a los casos más significativos y las decisiones jurisprudenciales al respecto. Junto con las decisiones automatizadas, toma especial relevancia la elaboración de perfiles[7], dirigida a la evaluación de datos personales para analizar o predecir aspectos que pueden tener una finalidad muy distinta de los iniciales. Se trata de una cuestión que es especialmente relevante como consecuencia del desarrollo de sistemas IA.

Finalmente, se analizan las bases del modelo de responsabilidad en el tratamiento de datos, mediante un sistema de responsabilidad proactiva, que conlleva ciertas obligaciones y amplia la responsabilidad de los responsables del tratamiento de datos.

En conclusión, este estudio tiene como objetivo proporcionar una base para el análisis crítico de la relación entre protección de datos e inteligencia artificial, con relación al desarrollo de marcos normativos que aborden los problemas derivados del necesario control de datos en la tecnología, que ha supuesto el desarrollo de sistemas de inteligencia artificial.

2. Marco básico regulador en la Unión Europea

El derecho a la protección de datos para garantizar la libertad frente a las potenciales agresiones a la dignidad y la libertad de las personas ante el uso ilegítimo del tratamiento mecanizado de datos[8] cuenta con un marco regulador, que parte del contenido del art.8 de la Carta de los Derechos Fundamentales de la

6 COTINO HUESO, L. CASTELLANOS CLARAMUNT, J. (2022) *Transparencia y explicabilidad de la Inteligencia Artificial.* Tirant Lo Blanch. Valencia

7 Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA. https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

8 LUCAS MURILLO DE LA CUEVA, P. (2.000) *"*Las vicisitudes del derecho de la protección de datos personales*"* en *Revista Vasca de Administración Pública.* Vol. 2, n.o 58, pp. 211-242

Unión Europea, adoptada el 7 de diciembre de 2000[9]. Establece los principios básicos para el tratamiento adecuado de los datos personales y brinda a las personas el derecho de acceso y rectificación de sus datos.

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de manera leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

Además, este derecho se ha reforzado con la entrada en vigor del Reglamento General de Protección de Datos. (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 cuanto al tratamiento y la libre circulación de datos personales (RGPD), y establece normas más detalladas y rigurosas sobre la protección de datos en la Unión Europea[10]. Se recogen principios y obligaciones específicas para proteger los datos personales y garantizar el control de las personas sobre su información.[11]

En España, el régimen de protección de datos deriva de un derecho de creación doctrinal que encuentra su fundamento constitucional en el mandato al legislador contenido en el artículo 18.4 de la CE, en el que se trata de limitar "el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el ejercicio de sus derechos", además de que guarda relación directa con el contenido del artículo 10.1 CE que dispone que *"la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás, son fundamento del orden político y de la paz social"*. Es, pues, tal y como ha reconocido el TC a partir de la STC 254/1993, una garantía constitucional, como forma de respuesta a una nueva forma de amenaza a la dignidad y a los derechos de la persona. Es

9 El Convenio número 108 del Consejo de Europa, de 1981 modificado por protocolo de 2018, se ocupa de la protección de las personas físicas en el ámbito de protección del tratamiento de datos personales. También en este sentido el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea.

10 Este Reglamento deroga la Directiva 95/46/CE

11 El concepto de dato personal responde a una definición, que aparece recogida en el artículo 4.1 del RGPD *"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;"*

un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también es, en sí mismo, un derecho autónomo, distinto al derecho a la intimidad y que implica capacidad de control sobre los datos. Es, por tanto, un derecho autónomo, un derecho en sí mismo, al que hace referencia el TC de manera más clara es la STC 292/2000 al distinguirlo del derecho a la intimidad al que atribuye un*a función distinta y por consiguiente, que también su objeto y contenido difieran».*

A partir del mandato al legislador contenido en el artículo 18.4 para la limitación del uso de la informática y como consecuencia de su desarrollo doctrinal, se crea el derecho de autodeterminación informativa, que tiene rango de derecho fundamental en cuanto afecta al derecho a la vida privada contenido de manera más general en el artículo 18 CE, aunque se trate de un derecho autónomo y distinto, con una naturaleza propia. Con este fundamento se crea un régimen de protección de datos, que resulta de la transposición del RGPD, regulado mediante Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. (LOPDGDD) que parte de considerar "dato de carácter personal" cualquier información concerniente a personas físicas identificadas o identificables.

La Ley establece ciertos principios exigibles a cualquier tipo de tratamiento, incluidos aquellos basados en IA y que utilicen algoritmos. Define un marco de desarrollo de las actuaciones de los responsables basado en la gestión de los riesgos para los derechos y las libertades de los interesados y la rendición de cuentas, o capacidad de demostrar el cumplimiento de las obligaciones impuestas por la normativa.

3. Protección de datos en cada ciclo de vida de sistemas de inteligencia artificial

En el contexto de la IA, basada en el uso del *big data,* es esencial que los sistemas cumplan con los principios propios del régimen de protección de datos y se diseñen de manera que traten de proteger la privacidad,[12] desde el inicio, y en todas sus etapas. Esto implica implementar medidas técnicas y organizativas para garantizar la seguridad de los datos, obtener el consentimiento informado de las personas cuando sea necesario, y ofrecer transparencia sobre cómo se utilizan los

12 GARRIGA DOMÍNGUEZ, A (2015). *Nuevos retos para la protección de datos personales en la Era del Big Data y de la computación ubicua* Madrid: Dykinson, pp. 25-30

datos y las decisiones que toma el sistema de IA. [13]

Los sistemas IA son tecnologías de procesamiento de la información. De acuerdo con la definición dada por la UNESCO Se caracteriza porque *"integran modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la predicción y la adopción de decisiones en entornos materiales y virtuales. Los sistemas de IA están diseñados para funcionar con diferentes grados de autonomía, mediante la modelización y representación del conocimiento y la explotación de datos y el cálculo de correlaciones".*[14] La inteligencia artificial se relaciona de forma clara con el *big data.* Lo necesita para desarrollar sus funcionalidades, ya que se nutre de la gran cantidad de datos recopilados para entrenar modelos, mediante algoritmos de aprendizaje automático y tomar decisiones basadas en patrones y correlaciones[15]. Esta sinergia permite a la inteligencia artificial realizar tareas como el procesamiento de lenguaje natural, la visión por computadora y la toma de decisiones predictivas con un alto grado de precisión.[16]

Debe tenerse en cuenta que no siempre la inteligencia artificial involucra datos personales en alguna fase de su ciclo de vida ni toma decisiones que repercuten exclusivamente en las personas a través de procesos automatizados. Puede hacerse referencia a supuestos en que sistemas de IA no incorporan datos personales, como los utilizados en el control de calidad de productos industriales o aquellos empleados en la toma de decisiones relacionadas con transacciones financieras. De esta forma, si un componente de IA se dedica al tratamiento de datos personales, a la elaboración de perfiles o a la toma de decisiones concernientes a personas físicas, está sujeto al RGPD En ausencia de estas circunstancias,

13 Recomendación sobre la ética de la inteligencia artificial, adoptada el 23 de noviembre de 2021 por la UNESCO. *La privacidad, que constituye un derecho esencial para la protección de la dignidad, la autonomía y la capacidad de actuar de los seres humanos, debe ser respetada, protegida y promovida a lo largo del ciclo de vida de los sistemas de IA*

14 *Ibidem.*

15 Los algoritmos pueden definirse como un "*conjunto de instrucciones o reglas definidas y no-ambiguas, ordenadas y finitas que permite, típicamente, contestar una pregunta, tomar una decisión, solucionar un problema, realizar un cómputo, procesar datos o llevar a cabo alguna tarea*". Estos procedimientos computacionales toman uno o varios valores de entrada y generan uno o varios valores de salida, por lo tanto, son instrumentos que no intentan establecer un vínculo causal entre una variable específica y su efecto, sino que producen un resultado". *Guía de auditoría algorítmica. Éticas-consulting.* https://www.eticasconsulting.com/eticas-consulting-guia-de-auditoria-algoritmica-para-desarrollar-algoritmos-justos-y-eficaces/ (Obtenido el 2 de febrero de 2024)

16 COTINO HUESTO, L. (2017) "Big data e inteligencia artificial, una aproximación a su tratamiento jurídico desde los derechos fundamentales", en: *Dilemata,* 24, pp.131-150

dicha sujeción al RGPD no se requiere.[17]

Bajo una perspectiva integral de los posibles procesos involucrados en una solución basada en inteligencia artificial (IA), se pueden identificar distintas fases en las cuales datos personales pueden estar presentes a lo largo del ciclo de vida de dicha solución: [18] En primer lugar, fase de entrenamiento de un modelo de IA, en la que se pueden emplear datos personales, especialmente, en el caso de modelos basados en técnicas de aprendizaje automático (Machine Learning). Esta actividad en sí misma constituye un proceso de tratamiento de datos. Una segunda etapa es la de validación. En esta se pueden realizar tratamientos de datos personales al emplear datos correspondientes a situaciones reales con el propósito de evaluar experimentalmente la eficacia del modelo. El conjunto de datos utilizado en esta fase puede diferir de aquel utilizado en el entrenamiento (si es que se ha empleado un conjunto de datos de datos personales) y, en algunos casos, la validación puede ser llevada a cabo por una entidad externa para auditar o certificar el modelo. De la misma forma, cuando una solución de IA se convierte en un componente o módulo distribuido a terceros para su integración en sus propios procesos, puede haber una comunicación de datos personales si la solución de IA contiene datos personales o si existe la posibilidad de obtenerlos. Además, podría haber patrones en el modelo que permitan la identificación de una persona en concreto. [19]

Durante diversas actividades de explotación de una solución de IA es posible encontrar tratamientos de datos personales, que incluyen distintas situaciones. Aunque, si la persona interesada dispone de la IA como un componente de su propiedad, podría aplicarse la excepción doméstica[20]. Los datos pueden, igualmente, ser utilizados para mejorar el sistema de IA. Sin embargo, si se comparten estos datos con terceros, pueden surgir comunicaciones de datos, tratamientos de almacenamiento, ajustes en el modelo o incluso nuevas comunicaciones si estos datos se incorporan al modelo y se comparten con otros terceros.

Por último, la retirada del servicio puede adoptar dos enfoques distintos: la del componente de IA debido a su obsolescencia en todos los procesos en los que

17 Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA. https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

18 *Ibidem.*

19 *Ibidem.*

20 En estos casos no resulta aplicable el RGPD "*la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades"* y, las que resultaran *"sin conexión alguna con una actividad profesional o comercial"*.

se implementa, o la decisión de un usuario específico de no utilizar el sistema de IA. Este usuario puede ser tanto una entidad como una persona física, y esta elección puede tener repercusiones en la eliminación de datos, ya sea a nivel local, centralizado o distribuido, y en la portabilidad del servicio. [21]

En estas distintas etapas los Principio del formularioEn tEsistemas algorítmicos necesitan someterse a evaluaciones apropiadas en relación con su impacto en la privacidad. Estas evaluaciones están previstas en el artículo 35 del RGPD y deben abarcar, de igual manera, las consideraciones sociales y éticas relacionadas con su empleo, además de abogar por un enfoque innovador en la gestión de la privacidad desde la fase de concepción. Los responsables en el ámbito de la inteligencia artificial deben asumir la responsabilidad tanto en la concepción como en la ejecución de los sistemas de IA, garantizando de esta forma la protección de la información personal a lo largo de todo el ciclo de vida de dichos sistemas.[22]

Cada etapa se considera un proceso de tratamiento y, en consecuencia, está sujeta al cumplimiento del RGPD. En etapas posteriores del ciclo de vida de la solución de inteligencia artificial, como su integración en un proceso de tratamiento, se requiere una evaluación para determinar si se están tratando datos personales, al menos en lo que respecta a la solución de inteligencia artificial. Si se determina que no se están tratando datos personales, posiblemente debido a su eliminación o anonimización,[23] es necesario demostrar la efectividad de estos procedimientos y evaluar el riesgo potencial de reidentificación.[24] Así, con el objetivo de garantizar la ausencia de tratamiento de datos personales en las etapas posteriores del ciclo de vida, como la integración de la solución de inteligencia artificial en un proceso de tratamiento, es necesario demostrar que la eliminación o anonimización de los datos personales es efectiva y evaluar el posible riesgo de reidentificación que pueda existir. [25]

21 Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA. https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

22 Recomendación sobre la ética de la inteligencia artificial, adoptada el 23 de noviembre de 2021 por la UNESCO

23 El artículo 4.5 del RGPD define la seudonimización como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*".

24 Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA. https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

25 *Ibidem.*

4. Condiciones y derechos de los titulares respecto del tratamiento de datos personales en inteligencia artificial

Al uso de la inteligencia artificial le son aplicables las disposiciones generales de protección de datos. El «tratamiento» debe entenderse como *cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción* (art. 4.2 RGPD)

Además, la IA está sujeta a otras regulaciones, principalmente, la llamada Ley de IA, que tiene como objetivo principal regular de manera horizontal el campo de la IA .Se trata de un sector muy regulado, en el que confluyen normas de distinta naturaleza, como lógica consecuencia de su naturaleza compleja.[26]

El tratamiento debe cumplir con ciertas condiciones. Debe ser lícito, tal y como señala el RGPD, en su artículo 5. A estos efectos, es necesario, de acuerdo

26 La regulación propuesta se centra en los riesgos asociados con la IA, con un enfoque humanista y centrado en la protección de los derechos fundamentales. Tiene en cuenta la probabilidad de daños derivados, especialmente de la IA generativa. Las cuatro categorías de riesgo son: inaceptable, elevado, limitado y mínimo. Así, se acordó prohibir: a) "sistemas de categorización biométrica que utilicen características sensibles (por ejemplo, creencias políticas, orientación sexual o raza); b) la "extracción no dirigida de imágenes faciales" de Internet o grabaciones de circuito cerrado de televisión (CCTV) para crear bases de datos de reconocimiento facial; c) "sistemas de reconocimiento de emociones" en el lugar de trabajo y en instituciones educativas; d) "sistemas de crédito social" basados en el comportamiento social o características personales; y e) "sistemas que manipulen el comportamiento humano" para quebrantar su libre albedrío o que exploten las vulnerabilidades de las personas (por su edad, discapacidad o situación socio-económica). Junto con los sistemas prohibidos, se relacionan otros a los que se considera de riesgo mínimo y los de alto riesgo. Los primeros únicamente quedan sometidos a obligaciones básicas de transparencia, en particular la necesidad de garantizar la accesibilidad a su documentación técnica. Con carácter voluntario, eso sí, las empresas podrán someterse a códigos de conducta adicionales para estos sistemas de IA. Los sistemas de IA clasificados como de alto riesgo forman parte de este grupo porque conllevan un posible daño a la salud, la seguridad, los derechos fundamentales, el medio ambiente, la democracia y el Estado de derecho. Se incluyen, también, los que se usen para influir en resultados electorales y la conducta de los votantes, que quedan sujetos, adicionalmente, a una serie de medidas. En primer lugar, la evaluación y mitigación de riesgos, de entre la cuales, exige una evaluación de impacto sobre derechos fundamentales. Además, exige las garantías de alta calidad de los datos empleados. Una medida que permita el control son los registros de actividad. Exige, igualmente medidas apropiadas de supervisión humana. Y, por último, la información y control ciudadano, en forma de explicaciones sobre las decisiones basadas en este tipo de sistemas que afecten a sus derechos y derecho a presentar quejas sobre este tipo de sistemas.

con el RGPD, que se cumpla, al menos, una de las condiciones recogidas en dicha norma. Se hace referencia a que la persona haya otorgado su consentimiento para que sus datos personales sean procesados con fines específicos. También será lícito si el procesamiento es indispensable para la ejecución de un contrato en el cual la persona afectada es parte, o para la implementación de medidas precontractuales a petición de ésta. O si el procesamiento es esencial para el cumplimiento de una obligación legal que recae sobre el responsable del tratamiento. Así como en aquellos casos en que sea necesario para proteger los intereses vitales de una persona física. Además de si el procesamiento es esencial para cumplir con una tarea de interés público o en el ejercicio de poderes públicos otorgados al responsable del tratamiento. Por último, será lícito, conforme al RGPD si el procesamiento es necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que dichos intereses no prevalezcan sobre los derechos y libertades fundamentales que requieren protección de datos personales, en particular en supuestos de minoría de edad[27].

Además, se exigen otros requisitos. Los datos deben ser tratados para la finalidad que se hubiera señalado al momento de su recopilación. Debe haber proporcionalidad, de forma que el tratamiento sea apropiado de acuerdo con la finalidad y que utilice la información que sea imprescindible y necesaria. Además, los datos deben estar limitados, de acuerdo con el principio de minimización de datos. La calidad de los datos es un requisito de todo tratamiento. Lo que significa que deben ser veraces, exactos y adecuados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento, debiéndose garantizar la confidencialidad y seguridad de los datos. Los responsables del tratamiento responden proactivamente de que se cumplan esos requisitos, y de demostrarlo.

Uno de los problemas que plantea el uso de inteligencia artificial es que el propio funcionamiento de la IA se basa en hacer nuevos usos de los datos que fueron obtenidos de manera primaria para otros fines. De ahí que, el principio de la necesaria coherencia del tratamiento con la finalidad exija un test de compatibilidad, que en caso de que no se produzca necesitaría del consentimiento. O de, en su caso un proceso de anonimización, que, a su vez, exige, para que realmente sea efectivo, que el tratamiento se haga según otros criterios, como el de proporcionalidad.

27 Esta disposición no se aplica al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones

El consentimiento es una pieza clave en el tratamiento de los datos, independientemente de que éstos estén sometidos a una mayor o menor protección. El RGPD lo define (art. 4.11) como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*"

El uso de IA a menudo implica la recopilación y el procesamiento de datos personales sin un consentimiento informado adecuado. Lo que incluye una comprensión o conciencia de la forma en que se utilizan los datos y de las implicaciones completas de proporcionar el consentimiento. Los consentimientos pueden hacerse depender de un conjunto complejo de términos y condiciones legales que son difíciles de entender, lo que hace que dar su consentimiento sea una acción poco informada. Esto es especialmente problemático cuando se trata de servicios en línea, donde a menudo se recopilan datos personales para mejorar la experiencia del usuario o con fines publicitarios. En definitiva, en estas situaciones, no hay un control real de los datos personales. Por lo que el consentimiento se convierte algo simbólico y poco operativo.[28]

La recopilación y procesamiento de datos sin consentimiento adecuado también pueden dar lugar a un riesgo claro de abuso de datos. Los datos personales pueden utilizarse de formas que las personas afectadas nunca habrían aprobado si hubieran entendido completamente las implicaciones. Esto puede incluir la venta de datos a terceros, el perfilado de usuarios para fines de publicidad dirigida o incluso el uso de datos para tomar decisiones importantes, como la elegibilidad para seguros o empleos. Lo que afecta al principio fundamental de autonomía y control sobre los propios datos personales. La complejidad radica en que muchas veces es difícil otorgar consentimiento cuando las finalidades de uso de los datos son desconocidas o poco claras, al igual que los algoritmos específicos que se emplearán, que también suelen ser opacos para el individuo. Esto lleva a cuestionar la viabilidad de obtener un consentimiento válido para el tratamiento de una cantidad ilimitada de datos. Se ha sugerido, por estos motivos, reservarlo para casos específicos donde sea posible comprender plenamente las implicaciones del tratamiento de datos.[29]

Desde el punto de vista de los derechos que se reconocen a los titulares de datos personales, el RGPD hace referencia a los derechos de transparencia, in-

28 GÓMEZ ABEJA, L. (2022). "Inteligencia artificial y derechos fundamentales". En *Inteligencia artificial y filosofía del derecho*. Murcia: Laborum. pp 91-114.
29 COTINO HUESTO, L. (2017) "Big data .." *Ob. cit.* pp. 131-150

formación, acceso, rectificación, supresión, limitación, oposición y portabilidad. Quizá el que tenga una especial relevancia en el ámbito de la IA es el relacionado con el derecho de oposición y la toma de decisiones automatizadas, como consecuencia de que las decisiones automatizadas pueden tener un impacto profundo y directo en la vida de las personas. El derecho de oposición supone una oportunidad para evitar esas decisiones a quienes entienden que son injustas, inexactas o discriminatorias, protegiendo así sus derechos e intereses.

Además de los riesgos que suponen, de una manera general, la recopilación y uso excesivo de datos que requiere la IA para entrenar y mejorar sus algoritmos a efectos de privacidad es necesario tener en cuenta que no todos los datos tienen el mismo valor a efectos de su protección. Merecen especial protección los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales. El artículo 9 del RGPD se refiere como datos de categorías especiales aquellos "*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 la orientación sexual de una persona física*". [30]

Junto con los problemas derivados de la recopilación y uso excesivo de datos, existe un riesgo de discriminación y sesgos, derivado de su uso inadecuado.[31] Los sistemas de IA pueden estar sujetos a sesgos inherentes en las bases de datos, lo que puede resultar en decisiones discriminatorias[32]. Si las bases de datos utilizados para entrenar los algoritmos contienen sesgos o reflejan desigualdades existentes, la IA puede perpetuar y amplificar esos sesgos al tomar decisiones automatizadas. Esto plantea problemas que aumentan su gravedad de acuerdo con los efectos de las decisiones en el ámbito de los derechos.

5. Principio de proactividad

La proactividad, como principio relacionado con los datos, tal y como lo en-

30 De acuerdo con el RGPD, el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física

31 Sobre los sesgos, vid. EGUÍLUZ CASTAÑEIRA. J.A. (2020) Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales", *Estudios de Deusto,* 68, pp. 325-368.

32 PEREZ-UGENA, M. *El derecho al olvido frente a buscadores de Internet.* Dykinson 2024. P.10

tiende el RGPD incluye referencias a la transparencia, información, comunicación y seguridad. La seguridad de los datos y su posible vulnerabilidad es una de las cuestiones más problemáticas respecto del uso de IA y el aprendizaje autónomo, que funcionan gracias al almacenamiento y procesamiento de estos datos. La falta de protección puede derivar, no sólo en la pérdida de control sobre datos personales o restricción de derechos, sino discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física[33]. El RGPD hace referencia a esta cuestión en su artículo 4.12. Define la violación de la seguridad de los datos personales como la que *"ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*

Relacionado con lo anterior, uno de los riesgos más claros es el que plantea la falta de transparencia y explicabilidad derivados de la dificultad de comprender la toma de decisiones respecto de los datos[34]. Estos principios de transparencia y explicabilidad son fundamentales en la regulación de protección de datos[35] y exigen que la información sea clara, accesible, fácil de entender y, cuando sea necesario, visualizada[36].

La falta de transparencia en el funcionamiento de la inteligencia artificial, especialmente en ciertos tipos de sistemas, a los que se incluyen en las denominadas "cajas negras", plantea la posibilidad de que una operación sea en parte incomprensible para sus creadores[37]. En otras palabras, algunos enfoques de IA pueden ser percibidos de forma que los diseñadores no pueden explicar completamente cómo se desarrollan ciertas decisiones y comportamientos de la IA[38]. Es-

33 COTINO HUESO, L. CASTELLANOS CLARAMUNT, J. (2022) *ob cit.*

34 COTINO HUESO, L. (2019) "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho" en *Revista Catalana de Derecho Público.* nº 58. Junio.

35 Art. 22 RGPD, 9.1 Convenio 108 del Consejo de Europa,

36 MEDINA GUERRERO, M. (2022) "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales", en *Teoría y realidad constitucional*, núm. 49, pp. 141-171.

37 VESTRI G, (2021) La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, (56), 368-398

38 Existen ciertas normas que hacen referencia al respeto ético a la obtención de información destinada a surtir bases algorítmicas particularmente la norma ISO sobre la información tecnológica.

ta opacidad plantea, a su vez, el problema de responsabilidad respecto de los hechos realizados, o de los daños derivados, por un sistema IA. En los casos en que la inteligencia artificial actúa de manera autónoma y sus acciones resultan incomprensibles incluso para quienes la diseñan, surge la interrogante de quién es el responsable de los resultados de esas acciones. Se plantea si el responsable es aquel que diseñó la inteligencia artificial, quien la programó o la propia inteligencia artificial como entidad emergente, además de posibles supuestos de corresponsabilidad, a la hora de determinar en quién recae, en definitiva, la responsabilidad de los hechos o resultados generados por la inteligencia artificial. Para lograr una mejor trazabilidad hay ciertos aspectos fundamentales como la información clara y transparente del sistema de información y su fiabilidad; medidas de supervisión humana, y unos sistemas sólidos, seguros y precisos. La falta de transparencia también podría mermar la posibilidad de impugnar eficazmente las decisiones basadas en resultados producidos por los sistemas IA y, por lo tanto, podría vulnerar, entre otros, el derecho a un juicio imparcial y a un recurso efectivo, y limitar los ámbitos en los que estos sistemas pueden utilizarse legalmente.

Este principio cobra especial importancia en situaciones en las que resulta complicado para las personas entender quién está recopilando sus datos, con qué fines y cómo se utilizan. Resulta evidente en la publicidad en línea, donde a menudo se recopilan datos de los usuarios para dirigir anuncios de manera específica. Además, es fundamental utilizar un lenguaje claro y sencillo. En lugar de sumergirse en una explicación técnica y complicada sobre cómo operan los algoritmos y el aprendizaje automático, la persona encargada de gestionar los datos debe optar por proporcionar información de manera clara y detallada.[39]Principio del formulario

En definitiva, los algoritmos, especialmente aquellos que incorporan técnicas de aprendizaje artificial, tienen la capacidad de integrar y procesar cantidades masivas de datos, incluyendo datos de carácter personal y sensibles[40]. No obstante, estos algoritmos a menudo poseen un diseño y funcionamiento particularmen-

39 Recomendaciones de buenas prácticas contenidas en el Anexo 1 Grupo de trabajo sobre protección de datos del artículo 29 https://www.aepd.es/documento/wp251rev01-es.pdf Se proponen los siguientes ejemplos: *las categorías de datos que se han utilizado o se utilizarán en la elaboración de perfiles o el proceso de toma de decisiones; Por qué estas categorías se consideran pertinentes; Cómo se elaboran los perfiles utilizados en el proceso de decisiones automatizadas, incluidas las estadísticas utilizadas en el análisis; Por qué este perfil es pertinente para el proceso de decisiones automatizadas; Cómo se utiliza para una decisión relativa al interesado. En general, esta información será más pertinente para el interesado y contribuirá a la transparencia del tratamiento*

40 ARELLANO TOLEDO, W. (2019) "El derecho a la transparencia algorítmica en big data e inteligencia artificial", en *RGDA Iustel*, nº 50, febrero.

te complejo y opaco, lo que dificulta comprender y controlar cómo se tratan estos datos[41]. Lo que se conoce como "*explicabilidad"* es consecuencia de la opacidad de los algoritmos, del hecho de que algunos sistemas de IA, como las redes neuronales profundas, sean intrínsecamente complejos y difíciles de entender.[42] Los titulares de datos personales pueden tener dificultades para comprender cómo se toman las decisiones y qué datos se utilizan para ello, lo que dificulta su capacidad para ejercer su derecho a la privacidad y tomar decisiones informadas sobre el uso de sus datos.

Además, como se ha señalado, los daños pueden producirse no solo en un plano individual, sino afectar de forma masiva a los derechos de grupos sociales. Incluso el perjuicio puede resultar invisible para el derecho fundamental desde la óptica individual del titular del derecho y afectar de forma colectiva. Por lo que es preciso tener en cuenta la dimensión colectiva de los derechos, así como los fundamentos en la dignidad y el libre desarrollo de la personalidad.[43] Las evaluaciones de riesgos que se realicen deben incluir esa dimensión colectiva del posible daño.

6. Decisiones automatizadas

La capacidad de verificar la exactitud de los datos utilizados. Como resultado, al configurar perfiles de riesgo, se abría la posibilidad de establecer conexiones involuntarias basadas en prejuicios o sesgos. [44].

Siempre que se permita el tratamiento automatizado se deben proporcionar garantías apropiadas, como informar a la persona interesada, permitirle expresar su opinión, explicar la decisión tomada después de la evaluación y darle la oportunidad de impugnar esa decisión. . Los artículos 13 y 14 del GDPR reconocen este derecho referido a "la existencia de toma de decisiones automatizada". Esto implica que la decisión generada debe tener efectos comparables a los que se derivarían de una decisión que tenga consecuencias legales, cuando se aplica a la persona sometida a este tratamiento.

41 Guía de auditoría algorítmica. Éticas-consulting. https://www.eticasconsulting.com/wp-content/uploads/2021/01/Eticas-consulting.pdf (Obtenido el 3 de marzo de 2024)

42 ORTIZ ZÁRATE ALCARAZ, L. (2022) "Explicabilidad de la inteligencia artificial". En *Eunomía. Revista en Cultura de la Legalidad*. nº 22, pp. 328-344, p. 334 .

43 COTINO HUESTO, L. (2017) "Big data .." *ob. cit.*

44 COTINO HUESO, L. (2020) «SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020», *La Ley Privacidad,* nº 4, mayo.

Muchas decisiones automatizadas en realidad involucran cierto grado de intervención humana, sin embargo, para considerarse como tal, tiene que ser activa y no solo un gesto simbólico, es decir, tiene que tener un grado determinado de relevancia y capacidad. Para ello, se recomienda valorar la participación de una persona en el proceso de decisión examinando diferentes aspectos, como su autoridad, competencia, capacidad, diligencia o independencia. Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes. Además, el responsable del tratamiento debe identificar y registrar el grado de participación humana en el proceso de toma de decisiones y en qué punto se produce esta.[45]

7. Elaboración de perfiles.

El tratamiento automatizado de datos también abarca la elaboración de perfiles[46], que es la evaluación de datos personales para analizar o predecir aspectos que pueden tener una finalidad muy distinta, relacionados, por ejemplo, con el ámbito laboral, la situación económica, la salud, preferencias personales, fiabilidad, comportamiento, ubicación o movimientos de una persona, cuando estas evaluaciones pueden tener consecuencias legales significativas o un impacto similar.[47]

> *"Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". (Art.4.4 RGPD)*

45 Vid entrada en la Web de la Agencia Española de Protección de datos sobre " Evaluación de la intervención humana en las decisiones automatizadas" https://www.aepd.es/prensa-y-comunicacion/blog/evaluacion-de-la-intervencion-humana-en-las-decisiones-automatizadas (Obtenido el 4 de marzo de 2024)

46 Debe ser una forma automatizada de tratamiento, incluyen aquellos tratamientos que tienen participación parcialmente humana. Debe llevarse a cabo respecto a datos personales; Y el objetivo de la elaboración de perfiles debe ser evaluar aspectos personales sobre una persona física. Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA.
https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

47 Los campos del sector bancario y financiero, la asistencia sanitaria, la fiscalidad, los seguros, la mercadotecnia y la publicidad son ejemplos típicos en los cuales se lleva a cabo de manera recurrente la elaboración de perfiles para enriquecer el proceso de toma de decisiones.

El tratamiento automatizado y la creación de perfiles pueden solaparse. Es frecuente que estas dos actividades estén relacionadas, ya que un proceso inicial de toma de decisiones automatizadas puede evolucionar hacia un proceso basado en la creación de perfiles, dependiendo de cómo se utilicen los datos. Las decisiones automatizadas se refieren a tomar decisiones utilizando tecnología sin la intervención de seres humanos. Estas decisiones se pueden basar en diferentes tipos de datos, como la información proporcionada por las personas (como respuestas a un cuestionario), datos observados sobre las personas (como la ubicación registrada a través de una aplicación) o datos derivados o inferidos, como un perfil existente de una persona (por ejemplo, una calificación crediticia). La automatización de decisiones puede, o no, incluir la creación de perfiles de las personas. La creación de perfiles implica recopilar información detallada sobre una persona, pero no siempre se utiliza para tomar decisiones automatizadas[48].

Teóricamente son cuestiones distintas. El tratamiento automatizado se daría ante un servicio de atención al cliente de una compañía de telecomunicaciones, por ejemplo, que utiliza un sistema automatizado para rastrear y registrar las quejas de los clientes. Cuando un cliente presenta una queja a través de un formulario en línea o a través de una llamada automatizada, el sistema registra automáticamente la queja y asigna un número de seguimiento. Luego, el sistema puede generar respuestas automatizadas o notificaciones de estado a lo largo del proceso de resolución de la queja sin intervención humana directa. La elaboración de perfiles se daría por la misma compañía de telecomunicaciones, al realizar un análisis de perfiles de sus clientes para identificar tendencias y preferencias. Utilizan datos de facturación, historiales de llamadas y patrones de uso para crear perfiles de clientes. Con estos perfiles, la compañía puede personalizar sus ofertas y promociones. Por ejemplo, pueden identificar a los clientes que son propensos a cambiar de proveedor y dirigir ofertas especiales hacia ellos para retenerlos. Esta elaboración de perfiles se basa en el análisis de datos, pero no implica decisiones automáticas como el tratamiento automatizado de las quejas. En re-

48 Recomendaciones de buenas prácticas contenidas en el Anexo 1 Grupo de trabajo sobre protección de datos del artículo 29 https://www.aepd.es/documento/wp251rev01-es.pdf Se plantea el siguiente ejemplo: *La imposición de multas por exceso de velocidad únicamente sobre la base de las pruebas de los radares de velocidad es un proceso de decisiones automatizadas que no implica necesariamente la elaboración de perfiles. Sin embargo, puede convertirse en una decisión basada en la elaboración de perfiles si los hábitos de conducción de la persona se supervisan a lo largo del tiempo y, por ejemplo, la cuantía de la multa impuesta es el resultado de una evaluación que implique otros factores, como si el exceso de velocidad es un caso de reincidencia o si el conductor ha cometido otras infracciones de tráfico recientemente.*

sumen, el tratamiento automatizado implica la toma de decisiones automáticas sin intervención humana significativa, como respuestas automáticas a las quejas, mientras que la elaboración de perfiles, para actuar de forma más eficiente, realiza un análisis de datos para entender a los clientes y personalizar ofertas, pero las decisiones basadas en estos perfiles generalmente involucran la intervención humana para implementar estrategias específicas[49].

La creación de perfiles tiene el potencial de perpetuar los estigmas preexistentes y fomentar la fragmentación social. De manera paralela, puede encajonar a una persona en una etiqueta específica[50], restringiendo sus opciones a las sugerencias preestablecidas. Este fenómeno puede minar la libertad de elección de las personas, limitando, por ejemplo, sus decisiones sobre productos y servicios. La creación de perfiles puede conllevar predicciones erróneas, mientras que, en otros casos, puede dar lugar a la negación de servicios y bienes, perpetrando así una discriminación injustificada. El RGPD establece disposiciones con el propósito de garantizar que la práctica de elaboración de perfiles y la toma de decisiones automatizadas, ya sea con o sin la elaboración de perfiles, se realicen de manera que no conlleven un impacto injustificado en los derechos. Entre estas disposiciones se incluyen la imposición de requisitos específicos en cuanto a transparencia y equidad, así como la asignación de mayores responsabilidades en términos de proactividad. También, la definición de bases legales específicas para el procesamiento de datos. El otorgamiento de derechos individuales para oponerse a la elaboración de perfiles, en particular con fines de marketing. Y, por último, la exigencia de llevar a cabo una evaluación de impacto en la protección de datos en los casos en que se pongan especialmente en riesgo los derechos y libertades.

La elaboración de perfiles está formada por tres elementos: debe ser una forma automatizada de tratamiento, debe llevarse a cabo respecto a datos personales y el objetivo de la elaboración de perfiles debe ser evaluar aspectos personales sobre una persona física[51]. Implica un proceso de tratamiento automatizado, aunque no excluye la participación humana en la definición de dichos perfiles. Este procedimiento se basa en deducciones estadísticas y se utiliza comúnmente para predecir comportamientos o características de personas a partir de datos re-

49 SORIANO ARNANZ, A. (2021): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", en: *Revista General de Derecho Administrativo,* núm. 56.

50 TÉLLEZ AGUILERA, A. (2001) *Nuevas tecnologías, intimidad y protección de datos*, Edisofer, Madrid,

51 Recomendaciones de buenas prácticas contenidas en el Anexo 1 Grupo de trabajo sobre protección de datos del artículo 29 https://www.aepd.es/documento/wp251rev01-es.pdf (Obtenido el 4 de febrero de 2024)

colectados de diversas fuentes, considerando similitudes estadísticas con otras.

Según el RGPD, la creación de perfiles se define como el procesamiento automatizado de datos personales con el fin de evaluar aspectos personales, especialmente para analizar o prever aspectos de las personas. El término "evaluar" implica que la creación de perfiles involucra algún tipo de valoración o juicio sobre alguien. Sin embargo, es preciso destacar que la mera clasificación de personas en función de datos conocidos como edad, sexo y altura no siempre constituye una creación de perfiles, ya que esto dependerá de la finalidad de dicha clasificación. Por ejemplo, una empresa podría clasificar a sus clientes en función de su edad o género con fines estadísticos y para obtener una visión general de su base de clientes, sin realizar predicciones o sacar conclusiones sobre una persona en particular. En este caso, la finalidad no es evaluar las características individuales, por lo que no se consideraría una creación de perfiles[52].

En textos anteriores, en los que se inspira el RGPD, se recoge que la elaboración de perfiles puede implicar tres fases distintas. La primera, referida a la recogida de datos. Una segunda, de análisis automatizado para identificar correlaciones. Y la tercera, a la aplicación de la correlación a una persona para identificar características de comportamientos presentes o futuros. Los responsables que llevan a cabo la elaboración de perfiles deberán garantizar que cumplen los requisitos del RGPD respecto a todas estas fases.[53]

El RGPD, como se ha señalado, exige transparencia en el tratamiento de datos personales, así como que los responsables del tratamiento proporcionen información clara y accesible a los interesados para que estos comprendan cómo se utilizan sus datos personales. En la elaboración de perfiles y el tratamiento de decisiones automatizadas se aplican los principios del régimen de protección de datos. El proceso de elaboración de perfiles, que implica la creación de datos derivados o inferidos sobre las personas a partir de datos personales existentes, a menudo es invisible para la persona cuyos datos se están procesando. Estos datos "nuevos" no son proporcionados directamente por la persona, lo que puede hacer que sea difícil para las personas comprender cómo se toman decisiones automatizadas basadas en estos perfiles.

52 *Ibidem.*

53 La Recomendación CM/Rec(2010)13mdel Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd2a (Obtenido el 3 de febrero de 2024)

De acuerdo con el artículo 12, apartado 1 del RGPD, el responsable del tratamiento de datos está obligado a proporcionar a las personas una información que sea concisa, transparente, inteligible y de fácil acceso. Esta información debe ser proporcionada a los interesados para que comprendan cómo se están tratando sus datos personales. El RGPD busca así garantizar que la elaboración de perfiles se realice de manera transparente, se evite la posible discriminación y se asegure el derecho de comprender y cuestionar las decisiones automatizadas que se toman con base en estos perfiles.

Al conectar la creación de perfiles con el *big data* debe tenerse en cuenta el efecto que conlleva la enorme cantidad de datos que se utilizan. No se trata solo de identificar características compartidas en un grupo para establecer patrones generales que puedan ser sometidos a una mayor evaluación. En el uso de la IA este enfoque se transforma en predicciones mucho más específicas y personalizadas para cada persona. De lo que deriva el riesgo sobre cómo estas predicciones pueden ser utilizadas, ya que podrían llevar a decisiones perjudiciales basadas en suposiciones sobre las inclinaciones futuras de las personas en lugar de sus acciones reales. Esta práctica afecta a la autonomía y la dignidad humana y conlleva un riesgo de discriminación. Por lo tanto, es crucial buscar un equilibrio entre la utilidad de las predicciones basadas en datos masivos y la protección de los derechos individuales.[54]

El principio de lealtad y transparencia en el tratamiento de datos personales y, más en concreto, en el contexto de la elaboración de perfiles, es fundamental para garantizar la inexistencia de sesgos. La elaboración de perfiles puede ser desleal si se utiliza de manera discriminatoria o injusta. La elaboración de perfiles puede, también, suponer la utilización de datos personales que se recogieron originalmente para otra finalidad. El tratamiento adicional deberá estar en consonancia con los objetivos originales para los cuales se obtuvieron los datos, y esto dependerá de varios factores, que incluyen la información proporcionada inicialmente por el encargado del tratamiento al interesado.

Estos factores se encuentran recogidos en el (RGPD) y se pueden resumir de la siguiente manera: La relación entre los fines para los cuales se recopilaron los datos y los propósitos de su tratamiento posterior; El contexto en el cual se recolectaron los datos y las expectativas razonables de los interesados en cuanto a su uso futuro; La naturaleza de los datos en cuestión; Las posibles repercusiones para los interesados derivadas del tratamiento adicional; Las garantías implementadas por el responsable del tratamiento para garantizar un proceso de tratamiento

54 GARRIGA DOMÍNGUEZ, A. (2018) "La elaboración.." *Ob. cit.* pp. 116 y 136

justo y prevenir cualquier impacto negativo.

En el proceso de elaboración de perfiles, es esencial aplicar el principio de minimización de datos, lo que significa recolectar y retener solo la cantidad mínima de información necesaria para cumplir con el propósito establecido previamente. Por ejemplo, para un perfil de comportamiento de compra, solo deberían recopilarse datos de transacciones relevantes y no información adicional innecesaria. De esta forma, al limitar la cantidad de datos personales recopilados, se reduce el riesgo de violaciones de privacidad y abusos de datos. Es responsabilidad de los encargados del tratamiento de datos garantizar el cumplimiento del principio de minimización de datos, así como cumplir con los requisitos relacionados con los principios de limitación de la finalidad y limitación del período de conservación. Además, los responsables deben ser capaces de explicar y justificar de manera clara la necesidad de recopilar y retener datos personales, o considerar la utilización de datos agregados, datos anónimos o, cuando sea suficientemente protector, datos seudoanonimizados en el proceso de elaboración de perfiles. De esta forma se trata de busca equilibrar las oportunidades comerciales con la protección de la privacidad.

Otra exigencia en el tratamiento de datos frente a decisiones automatizadas y elaboración de perfiles es la limitación del plazo de conservación. Se refiere a la necesidad de que solo se retengan datos personales durante el tiempo estrictamente necesario para cumplir con el propósito inicial de su recopilación. Esto implica que los datos deben ser eliminados o anonimizados una vez que ya no se requieran para dicho propósito, garantizando así la protección de la privacidad y los derechos de las personas. Estos propósitos pueden incluir la prestación de un servicio, el cumplimiento de obligaciones legales, la investigación u otros fines legítimos. En el ámbito de la IA la limitación del plazo de conservación de los datos cobra especial importancia por varias razones. De una parte, por el riesgo de violaciones de seguridad y acceso no autorizado. En sistemas de IA, donde se manejan grandes volúmenes de datos, limitar el plazo de conservación ayuda a minimizar estos riesgos, protegiendo así la integridad de los datos y la privacidad de los individuos. Además, por la mitigación de sesgos y desactualización, que conlleva que los modelos de IA se entrenen y operen con datos relevantes y actuales, mejorando así la precisión y equidad en la elaboración de perfiles. Y, de forma general, se viene a dar cumplimiento al contenido del RGDP, lo que deriva en una base fundamental para hacer efectiva la transparencia en sistemas IA.

Es especialmente relevante y preocupante por las enormes posibilidades de control que supone, la utilización de datos biométricos. Los datos biométricos son, de acuerdo con la definición del RGPD "*datos personales obtenidos a par-*

tir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (artículo 4)

Estos datos pueden ser de naturaleza estática o dinámica, y en algunos casos, se utilizan sistemas multimodales que combinan ambas características. La biometría estática incluye la identificación de características físicas de una persona que no cambian con el tiempo. Algunos ejemplos son el uso de iris y retina de los ojos, la geometría facial o las huellas dactilares. En el caso de la biometría dinámica, estos datos biométricos se centran en características conductuales o de comportamiento que pueden cambiar con el tiempo. Ejemplos de datos biométricos dinámicos incluyen la voz, la firma o la dinámica de escritura. Por último, la biometría multimodal es una categoría que combina tanto las características estáticas como las dinámicas para lograr una identificación más robusta y precisa. Los sistemas biométricos multimodales utilizan múltiples fuentes de datos biométricos para confirmar la identidad de una persona.

La implementación de sistemas que utilizan datos biométricos, como el reconocimiento facial, el reconocimiento de voz o la autenticación mediante huellas dactilares, se ha vuelto cada vez más común en aplicaciones como sistemas de pago, sistemas de seguridad y autenticación de usuarios. Sin embargo, es fundamental que estos sistemas se regulen adecuadamente para garantizar la protección de la privacidad. El RGPD los regula dentro de las categorías especiales de datos personales del artículo 10.

La aplicación de sistemas IA conlleva un riesgo muy fuerte para la privacidad en el uso de los datos biométricos. La llegada de la inteligencia artificial representa un avance significativo, completamente distinto al uso tradicional de la videovigilancia, al que, hasta el momento, se viene refiriendo su aplicación práctica de manera particular. Actualmente, gracias a la IA, se puede comparar instantáneamente las imágenes de las personas captadas con listas de individuos buscados, o incluso generar grandes volúmenes de datos procesados de forma automatizada para diversos fines. Es evidente que la regulación habitualmente insuficiente de la videovigilancia no puede brindar una cobertura legal adecuada a estos nuevos desarrollos. Por lo que se necesitan nuevas normas de cumplimiento normativo con análisis de riesgos en las que se determinen las condiciones para el uso de estos sistemas.[55]Principio del formularioFinal del formulario

55 COTINO HUESO L. (2023) "Sistemas de inteligencia artificial con reconocimiento facial y datos

La precisión en el manejo de datos biométricos es vital en sistemas de IA como reconocimiento facial o dactilar. Si la IA no identifica correctamente a una persona, se genera un perfil erróneo antes de realizar el proceso principal. Por ejemplo, un sistema de reconocimiento facial podría tener dificultades para identificar a una persona con rasgos faciales poco comunes. Esto podría llevar a un perfilado erróneo y a la exclusión de estas personas de ciertos servicios o espacios. Los sistemas de IA precisos se traducen en sistemas con datos que cumplen con el requisito de exactitud. Lo que resulta fundamental para evitar discriminación y garantizar una IA inclusiva. El responsable del tratamiento debe ser consciente de las limitaciones de la IA y ofrecer mecanismos alternativos para evitar la exclusión de usuarios, minimizar errores, incluir algoritmos más robustos y ofrecer alternativas a los usuarios que no puedan ser identificados por el sistema de IA. Lo que, a su vez, se relaciona con la transparencia y explicabilidad de los sistemas IA.

Es por último necesaria la referencia a las diferencias entre los sistemas europeos y estadounidense respecto de esta cuestión. Es reseñable cómo la opción de la UE se conecta con el derecho de los ciudadanos a conocer y controlar el poder público al dar un mayor peso al derecho de motivación algorítmica. En cambio, en el Derecho estadounidense, la falta de regulación ha llevado a que la protección de secretos comerciales prevalezca sobre el derecho al conocimiento, favoreciendo a las empresas privadas.[56]

8. Responsabilidad en el tratamiento de datos: el modelo de la responsabilidad proactiva.

El encargado del tratamiento de datos, de acuerdo con el RGPD, debe implementar medidas técnicas, legales y organizativas adecuadas para asegurar y demostrar la conformidad con la normativa de protección de datos personales. Esto implica considerar la naturaleza, alcance, contexto y propósitos del tratamiento, así como los riesgos para los derechos y libertades. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

biométricos. Mejor regular bien que prohibir mal" *El cronista del estado social y democrático de derecho* núm. 100.

56 MIINICON G. (2021) Towards an "Algorithm Constitutional by Design" *Biolaw journal* 1pp. 381 a 403.

Además, es necesario que el responsable del tratamiento realice un análisis de los riesgos para los derechos, de forma que garantice y pueda demostrar el cumplimiento de los principios que justifican el uso de datos personales a lo largo de su ciclo de vida, desde la adquisición hasta la eliminación o anonimización. En consecuencia, esto requiere una actitud consciente, diligente y proactiva por parte de las organizaciones en todos los procesos de tratamiento de datos personales, que le obliga a poner en marcha medidas de distinto tipo y alcance para la protección de los derechos. Todo ello, de acuerdo con un enfoque preventivo, basado en un sistema de responsabilidad proactiva que obliga al encargado del tratamiento a anticiparse a los riesgos y a adoptar medidas para prevenirlos.[57]

De forma general, se puede concluir que el Reglamento ha supuesto un avance importante, pero debería ser más sencillo y comprensible para los responsables del tratamiento; Definir con mayor claridad los requisitos que deben aplicarse para cumplir con el modelo de responsabilidad proactiva. Es necesario establecer mecanismos de control efectivo para garantizar que se cumple con el RGPD. Además, pese a que el Reglamento hace referencia a la responsabilidad de los responsables del tratamiento, a quienes señala como responsables proactivos, es en la ciudadanía donde parece descansar en la responsabilidad, activa, respecto del tratamiento de los datos[58]. Lo que no resulta adecuado para proteger un derecho fundamental, además de que a la persona se le presumen una serie de conocimientos que puede, muy bien, no tener[59]. Por último, el Reglamento abusa de conceptos jurídicos indeterminados y realiza abundantes remisiones a normativas internas[60] Resulta necesario establecer medidas de control efectivo, de corrección, responsabilidad, rendición de cuentas y transparencia relativas al tratamiento de los datos.

9. Conclusiones

57 Recomendaciones de buenas prácticas contenidas en el Anexo 1 Grupo de trabajo sobre protección de datos del artículo 29 https://www.aepd.es/documento/wp251rev01-es.pdf

58 Se señalan ciertos elementos rectores de la responsabilidad proactiva: La identificación de una responsabilidad en el tratamiento; El análisis del riesgo para los derechos y libertades; El estudio de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; El despliegue de medidas para la gestión del riesgo, medidas de privacidad por defecto y desde diseño, medidas de seguridad, de gestión de incidentes, etc. Vid documento de la AEDP sobre adecuación del régimen de protección de datos a sistemas IA. https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf (Obtenido el 5 de febrero de 2024)

59 GOMEZ ABEJA, L: "inteligencia.." *Ob. cit.* pp. 91-114 espc. P.102

60 *Ibidem.*

La irrupción de la Inteligencia Artificial (IA) en diversos sectores trae consigo un enorme potencial transformador. Su capacidad para automatizar tareas, predecir resultados y perfilar riesgos abre un enorme abanico de posibilidades. Sin embargo, la aplicación de la IA también presenta importantes riesgos, especialmente, en materia de protección de datos. La recopilación y almacenamiento masivo de datos personales, los sesgos y la discriminación algorítmica, la falta de transparencia y explicabilidad en los algoritmos, y el acceso y control de los datos por parte de las personas son algunos de los principales riesgos que se deben afrontar.

Para garantizar un uso responsable de la IA, es necesario un marco legal sólido que regule su aplicación, priorizando la protección de datos. Este marco debe basarse en principios éticos claros como la transparencia, la explicabilidad, la no discriminación y la minimización de datos, en un sistema regulado por distintas normas sectoriales, que se unen al régimen establecido en el Reglamento General de Protección de Datos de la Unión Europea.

A lo largo del trabajo se han analizado las situaciones que permiten la toma de decisiones automatizadas, y el derecho a oponerse a las que se basen únicamente en algoritmos, con las condiciones que se determinan. Se concreta la forma en que se interpreta el derecho a la participación humana en la toma de decisiones algorítmicas, lo que implica que debe haber una persona que pueda escuchar y atender las objeciones del interesado y modificar la decisión automatizada inicial si fue injusta, sesgada o incorrecta.

Se diferencia la decisión automatizada de la creación de perfiles, llegando a la conclusión de que responden a dos acciones distintas, al menos teóricamente, pese a que se solapen en la práctica. Al poner en relación la creación de perfiles con el *big data* debe tenerse en cuenta el efecto que conlleva la enorme cantidad de datos que se utilizan. No se trata solo de identificar características compartidas en un grupo para establecer patrones generales que puedan ser sometidos a una mayor evaluación. En el uso de la IA este enfoque se transforma en predicciones mucho más específicas y personalizadas para cada persona. De ahí deriva el riesgo de evaluación que exige garantías claras de oposición, conforme al régimen de protección de datos.

Es fundamental establecer mecanismos de control y supervisión para auditar el uso de la IA y garantizar su cumplimiento con la normativa de protección de datos. El responsable del tratamiento deberá asumir una posición proactiva, conforme al RGPD, que exige una actuación compleja dirigida a una protección más real de los datos, pese a sus enormes dificultades.

REFERENCIAS BIBLIOGRÁFICAS.

ARELLANO TOLEDO, W. (2019) "El derecho a la transparencia algorítmica en big data e inteligencia artificial", en *RGDA Iustel*, nº 50, febrero.

BALAGUER CALLEJÓN. F. (2023) *La constitución del algoritmo* Fundación Giménez Abad. Zaragoza,. 2ºed.

CASTELLANOS CLARAMUNT J; MONTERO CARO, M.D. (2020) "Perspectiva constitucional de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales" *Ius et scientia* Vol. 6, núm. 2 pp. 72-82.

COTINO HUESTO, L.. (2023) "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal" *El cronista del estado social y democrático de derecho* núm. 100.

-(2020) «SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020», *La Ley Privacidad,* nº 4, mayo.

-(2017) "Big data e inteligencia artificial, una aproximación a su tratamiento jurídico desde los derechos fundamentales", en: *Dilemata,* 24, pp.131-150

-(2019) "Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho" en *Revista Catalana de Derecho Público.* Núm. 58.

COTINO HUESO, L. CASTELLANOS CLARAMUNT, J. (2022) *Transparencia y explicabilidad de la Inteligencia Artificial.* Tirant Lo Blanch. Valencia

EGUÍLUZ CASTAÑEIRA. J.A. (2020) Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales", *Estudios de Deusto,* 68, pp. 325-368.

GARRIGA DOMÍNGUEZ, A. (2018) "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el RGPD" *Revista Derechos y Libertades* , núm. 38. Madrid: Dykinson, pp. 116 y 136

- (2015) Nuevos retos para la protección de datos personales en la Era del Big Data y de la computación ubicua Madrid: Dykinson.

GÓMEZ ABEJA, L. (2022). "Inteligencia artificial y derechos fundamentales".

En *Inteligencia artificial y filosofía del derecho* (pp. 91-114). Murcia: Laborum.

HERNANDEZ PEÑA, J.C. (2022) *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza.* Aranzadi.

LUCAS MURILLO DE LA CUEVA, P. (2000) *"*Las vicisitudes del derecho de la protección de datos personales*"* en *Revista Vasca de Administración Pública.* Vol. 2, n.o 58, pp. 211-242;

MARTINEZ GARAI, L. (2018) "Peligrosidad, algoritmos y due process: el caso state v loomis" UNED. *Revista de Derecho Penal y Criminología,* 3.a Época, núm. 20

MEDINA GUERRERO, M. (2022) "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales", en *Teoría y realidad constitucional*, núm. 49, pp. 141-171.

MIINICON G. (2021) Towards an "Algorithm Constitutional by Design" *Biolaw journal* 1.pp. 381 a 403.

ORTIZ ZÁRATE ALCARAZ, L. (2022) "Explicabilidad de la inteligencia artificial". En *Eunomía. Revista en Cultura de la Legalidad*. nº 22, pp. 328-344, p. 334 .

PALMA ORTIGOSA, A. (2022) *Decisiones automatizadas y protección de datos personales. Especial atención a los sistemas de inteligencia artificial.* Dykinson.

PEREZ-UGENA, M. *El derecho al olvido frente a buscadores de Internet.* Dykinson 2024. P.10

PEREZ-UGENA A, M. "Implicaciones constitucionales de las nuevas tecnologías" *Revista de Derecho Político,* núm. 54, 2002, págs. 153-196

SORIANO ARNANZ, A. (2021): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", en: *Revista General de Derecho Administrativo,* nº. 56.

TÉLLEZ AGUILERA, A. (2001) *Nuevas tecnologías, intimidad y protección de datos*, Edisofer, Madrid,

VESTRI G, (2021) La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista Aragonesa de Administración Pública*, (56), 368-398