Pérez-Llorca

TECHLAW

Inteligencia artificial

ENERO 2024

Un reto para las compañías y para los reguladores

Raúl Rubio

Socio de Propiedad Intelectual, Industrial y Tecnología

rrubio@perezllorca.com
+34 91 353 45 59

María Chávarri

Abogada de Propiedad Intelectual, Industrial y Tecnología

mchavarri@perezllorca.com
+34 91 423 67 28

_ RAÚL RUBIO Y MARÍA CHÁVARRI

Interacción de la inteligencia artificial con la protección de datos personales

La inteligencia artificial ("**IA**") procesa información para aprender, adaptarse y realizar predicciones o recomendaciones. Los algoritmos utilizados en este ámbito, especialmente en su variante de aprendizaje automático, requieren de ingentes cantidades de datos para su entrenamiento.

Aunque es cierto que no todas las herramientas de IA necesitan hacer uso de datos personales, en muchos otros supuestos la información utilizada está conectada directa o indirectamente con el tratamiento de datos de personas físicas. La amplitud con la que se define en la Unión Europea, a través del Reglamento General de Protección de Datos ("**RGPD**") el concepto de dato personal[1] y la manera en que se interpreta esta definición por parte de los reguladores, obliga a considerar el riesgo de tratar datos personales incluso en usos de la IA más industriales o desconectados del individuo, como el internet de las cosas (IoT[2]).

Incluso cuando se tratan **datos anonimizados**, los estrictos criterios regulatorios nos obligan a cuestionar en qué medida dicha anonimización puede ser considerada suficiente como para escapar del ámbito de aplicación de la normativa de protección de datos.

> ***Aunque los datos sean anonimizados, el rigor de la regulación existente nos hace reflexionar sobre la efectividad de esta anonimización para determinar si realmente se excluye del alcance de las leyes de protección de datos.***

Al mismo tiempo, la **irreversibilidad** de la anonimización puede plantear retos a la hora de poder evaluar la calidad de las inferencias de ciertas herramientas de IA. En otras palabras, la recolección ilimitada de datos personales puede llegar a dificultar la capacidad de explicar completamente el adecuado funcionamiento de un sistema de IA. Cuanto más personalizados y exhaustivos son los datos, más efectivos pueden ser los patrones y conocimientos que la IA puede generar.

> ***Aquí radica el primer punto de fricción: la recolección y uso masivo de datos personales choca con algunos de los principios cardinales de la protección de datos***

Por lo tanto, es importante encontrar un equilibrio entre la minimización del tratamiento de datos personales y la necesidad de recopilar datos suficientes

1 Según el artículo 4.1 del RGPD, dato personal es "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".

2 Un ejemplo común de uso de IA en el internet de las cosas (IoT) -que aparentemente no trata datos personales, pero que en la práctica sí lo hace- es la monitorización del tráfico y el transporte. Los sistemas de IA en IoT pueden recopilar datos sobre la ubicación, el movimiento y los patrones de viaje de los usuarios, lo que, aunque inicialmente parezca no estar vinculado a datos personales, puede de hecho revelar información personal si se analiza en detalle. Por ejemplo, a través de la recopilación y análisis de datos de tráfico y movilidad, se pueden inferir patrones de comportamiento y preferencias individuales, lo que implica el tratamiento de datos personales.

para garantizar la explicabilidad[3] y transparencia de los sistemas de IA.

La evaluación de la base de legitimación para el tratamiento de datos, el cumplimiento del deber de informar sobre las características de dicho tratamiento, la limitación de la finalidad, la privacidad por defecto y desde el diseño o la seguridad, son algunos de los otros retos a los que se deben enfrentar desarrolladores, comercializadores y usuarios de la IA cuando se utilizan datos de carácter personal.

Teniendo en cuenta la interrelación entre IA y protección de datos, en este documento trataremos de analizar de forma breve y concisa: **(i)** la valoración que los reguladores europeos de protección de datos y, en particular, el Comité Europeo de Protección de Datos ("**CEPD**"), han llevado a cabo con respecto al futuro Reglamento de IA ("**Reglamento de IA**"); **(ii)** el posicionamiento de estos reguladores con respecto a la IA y el propio impacto de la regulación vigente de protección de datos; y **(iii)** algunas de las correlaciones del futuro Reglamento de IA con la normativa de protección de datos personales.

1. Valoración del futuro Reglamento de IA por parte de los reguladores de datos

A través del Dictamen conjunto 5/2021[4], el CEPD -en el que se encuentran representadas las autoridades nacionales de protección de datos de todos los Estados miembros- y el Supervisor Europeo de Protección de Datos ("**SEPD**"), apoyaban ya en junio de 2021 la iniciativa del legislador de abordar el uso de IA en la UE. No profundizaremos en los detalles de este documento, ya que se basa en una evaluación realizada mucho antes de los recientes cambios de enfoque del futuro Reglamento de IA, los cuales surgieron a raíz de las últimas negociaciones entre los colegisladores europeos. Sin embargo, destacaremos algunos aspectos que nos pueden ayudar a vislumbrar cuales podrían ser en el futuro las tensiones entre los dos ámbitos regulados, el de la IA y el de los datos personales, que a partir de ahora deberán coexistir:

- El CEPD y el SEPD hacen hincapié en que **el cumplimiento de los requisitos de protección de datos debe ser controlado de manera independiente**, conforme al art. 16 del Tratado de Funcionamiento de la Unión Europea[5].

- Se objeta implícitamente la posibilidad de que los espacios de pruebas o "sandboxes" puedan permitir excepciones al cumplimiento de la normativa de datos y se señala que el cumplimiento del RGPD y del Reglamento de protección de datos para las instituciones, órganos y organismos de la Unión Europea (RPDUE) debería ser una condición previa para entrar en el **mercado europeo** como producto con el marcado CE.

Los supervisores de datos europeos reivindican el papel de las Autoridades de Protección de Datos (APD) en el desarrollo y establecimiento de normas armonizadas y especificaciones comunes y se sugiere que las APD deberían ser designadas como autoridades nacionales de supervisión en materia de IA.

- Piden una prohibición general del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también con respecto a la forma de caminar, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, en cualquier contexto.

- Se cuestiona el papel predominante de la Comisión en el Comité Europeo de Inteligencia Artificial–al entender que es necesario que el organismo europeo de IA sea independiente de cualquier influencia política-, y se pide más autonomía para tal organismo, así como garantías de que pueda actuar por iniciativa propia.

- Los supervisores de datos europeos reivindican el papel de las Autoridades de Protección de Datos ("**APD**") en el desarrollo y establecimiento de normas armonizadas y especificaciones comunes, sugiriendo que las APD sean designadas como autoridades nacionales de supervisión en materia de IA.

- Para el CEPF y el SEPD, el conflicto entre la autonomía de la toma de decisiones por parte de las máquinas que subyace al concepto de IA y los derechos a la privacidad y la protección de datos personales es una preocupación importante.

- Se resalta la importancia de la supervisión humana, especialmente en los sistemas de inteligencia artificial que procesan datos personales, crucial para garantizar el cumplimiento del derecho a no estar sujeto a una decisión basada únicamente en el procesamiento automatizado.

3 La "explicabilidad" de los sistemas de IA se refiere a la capacidad de comprender y explicar cómo y por qué un sistema toma decisiones o realiza acciones específicas. Este concepto es especialmente importante en el contexto de algoritmos complejos, como los que se basan en aprendizaje profundo (*deep learning*), donde las decisiones pueden ser tomadas por modelos que son intrínsecamente difíciles de interpretar.

4 CEPD-SEPD: Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial), disponible en el siguiente enlace: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_es

5 El art. 16 establece que: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.; 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."

- Se acoge con satisfacción el enfoque basado en los factores de riesgo, el cual se aplica a todos los sistemas de IA. No obstante, los reguladores consideran que opción de proporcionar una lista exhaustiva de sistemas de IA de alto riesgo podría generar un efecto blanco y negro "con escasa capacidad de atracción de situaciones de alto riesgo", socavando el enfoque general de la propuesta de Reglamento y que se basa en factores de riesgo[6].

- El uso de sistemas de IA para la identificación biométrica remota de las personas en espacios de acceso público supone un riesgo elevado de intrusión en la vida privada, por lo que consideran que es necesario un enfoque más estricto. El uso de estos sistemas en aeropuertos y estaciones, por ejemplo, implicaría tratar datos de muchas personas para identificar solo a unas pocas, lo que plantea problemas de proporcionalidad, transparencia y legalidad según la legislación de la UE. Aún no se ha resuelto cómo informar adecuadamente a las personas ni cómo garantizar sus derechos, afectando la privacidad y libertades en espacios públicos. Asimismo, entienden que este tipo de sistemas llevan aparejadas consecuencias irreversibles en las expectativas de la población de conservar su anonimato en espacios públicos.

- El uso de la IA para inferir emociones de una persona física es muy indeseable y debería prohibirse, excepto en determinados casos de uso específicos, como sería su utilización con fines de salud o investigación, con las correspondientes garantías, límites y condiciones que ofrece la normativa de protección de datos.

Por su parte, varias autoridades nacionales de protección de datos se han adherido formalmente al Dictamen del CEPD y el SEPD[7] o, como en el caso de Italia, han publicado sus propias opiniones formales con enfoques muy similares[8].

2. Interpretación del RGPD en relación con la IA

El CEPD, por el momento, no ha publicado ninguna opinión formal interpretando el RGPD en el ámbito específico de la IA, al contrario de los reguladores de diferentes Estados miembros, que sí lo han hecho.

Las autoridades nacionales de Italia, Francia y, sobre todo, España están siendo las más activas en el establecimiento de un marco regulatorio de* softlaw *sobre la protección de datos y la inteligencia artificial.

La extensión de este documento no nos permite detenernos en las actuaciones de todos ellos, si bien, a continuación, destacaremos algunas de las actividades desarrolladas en este ámbito por Francia, Italia, Alemania y España.

2.1. Francia

En Francia, la Commission Nationale de l'Informatique et des Libertés ("**CNIL**") creó en enero de 2023 un departamento específico de IA para fortalecer su experiencia en estos sistemas y su comprensión de los riesgos para la privacidad, seguido poco después de un Plan de Acción[9]. El regulador ha identificado las siguientes áreas como prioritarias para el Servicio de Inteligencia Artificial y el Laboratorio de Innovación Digital de la CNIL:

- La equidad y transparencia del procesamiento de datos subyacente en el funcionamiento de estas herramientas.

- La protección de datos disponibles públicamente en la web contra el uso de scraping para el diseño de herramientas.

- La protección de datos transmitidos por los usuarios al utilizar estas herramientas, desde su recopilación (a través de una interfaz) hasta su posible reutilización y procesamiento a través de algoritmos de aprendizaje automático.

- Las consecuencias para los derechos de los individuos sobre sus datos, tanto en relación con los recopilados para el aprendizaje de modelos como los proporcionados por esos sistemas, como contenido creado en el caso de la IA generativa.

- La protección contra sesgos y discriminación que puedan ocurrir.

- Los desafíos de seguridad de estas herramientas.

La CNIL también ha puesto en marcha un sandbox propio para dar apoyo a tres proyectos que utilizan IA en beneficio de los servicios públicos y un programa de apoyo mejorado para tres empresas medianas innovadoras (scale-ups), incluyendo una especializada en la provisión de conjuntos de datos y modelos de inteligencia artificial.

Finalmente, destaca la publicación por parte del regulador francés de unas guías informativas[10] sobre la creación de bases de datos con IA, las cuales estuvieron sujetas a consulta pública hasta el 15 de diciembre de 2023[11]. Las

6 El CEPD y el SEPD no parecen tener en cuenta la inseguridad jurídica que podría provocar una indefinición con respecto a lo que se considera sistema de alto riesgo.

7 Intelligence artificielle: l'avis de la CNIL et de ses homologues sur le futur règlement européen, disponible en: https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen

8 Memoria del Garante per la protezione dei dati personali - COM 2021(206) Proposta di regolamento (UE) sull'intelligenza artificiale, disponible en: https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751565

9 Artificial intelligence: the action plan of the CNIL, disponible en: https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil

10 Las guías se encuentran disponibles en el siguiente enlace: https://www.cnil.fr/fr/les-fiches-pratiques-ia

11 Disponible en: https://www.cnil.fr/fr/intelligence-artificielle-la-cnil-ouvre-une-consultation-sur-la-constitution-de-bases-de-donnees

guías buscan apoyar a los agentes del ecosistema de la IA en sus esfuerzos por cumplir la legislación sobre protección de datos personales, y proporcionan respuestas concretas, ilustradas con ejemplos, a las cuestiones jurídicas y técnicas relacionadas con la aplicación del RGPD a la IA. En particular, responden a preguntas relativas a la aplicación de los principios de finalidad, minimización y el período de conservación de las bases de datos, así como las normas aplicables a la investigación científica y a la reutilización de las bases de datos.

2.2. Alemania

El supervisor federal de protección de datos en Alemania, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit ("**BfDi**"), inició un proceso de consulta pública del 30 de septiembre de 2021 al 17 de diciembre de 2021, cuyas conclusiones fueron presentadas en un informe al año siguiente[12]. Más recientemente, el BfDi publicó la Declaración del Comisario Federal de Protección de Datos y Libertad de Información sobre la audiencia pública de la Comisión de Asuntos Digitales del Bundestag alemán el 24 de mayo de 2023 sobre "Inteligencia Artificial Generativa[13]".

2.3. Italia

En Italia, las actuaciones de su regulador, Garante per la protezione dei dati personali ("**Garante**"), se han centrado por el momento en el sector sanitario, a través de la publicación de un Decálogo para la implementación de servicios de salud nacionales a través de sistemas de inteligencia artificial[14]
. A nivel divulgativo, el Garante ha publicado una serie de vídeos para analizar la IA y su relación con la protección de datos[15].

2.4. España

En el caso de **España**, la reacción de la Agencia Española de Protección de Datos ("**AEPD**") a la IA ha sido pionera. Ya en febrero de 2020 publicó una Guía para adaptar al RGPD los productos y servicios que utilicen inteligencia artificial[16]. En ella se recogen las condiciones que deben cumplir estas tecnologías para garantizar y demostrar que el tratamiento efectuado se adecúa al RGPD, marcando las exigencias de la AEPD de cara a garantizar la calidad y la privacidad de estos sistemas. También recuerda que el cumplimiento del RGPD exige a los modelos de IA cierto nivel de madurez, de forma que se pueda determinar objetivamente la adecuación de los tratamientos y la existencia de medidas para gestionar sus riesgos.

a. El tratamiento de datos personales en las distintas fases de los sistemas de IA

La guía destaca la posibilidad de que existan tratamientos de datos personales en todas las fases del ciclo de vida de los sistemas de IA. De esta manera, podemos encontrarnos con las posibilidades:

a) **Entrenamiento**: El entrenamiento del sistema de IA con datos personales constituye un tratamiento en sí mismo.

b) **Validación**: Existe tratamiento si se utilizan datos que representan la situación real del tratamiento para evaluar experimentalmente la eficacia y calidad del modelo. La validación se realiza en la determinación de la capacidad del sistema de IA para realizar predicciones precisas y útiles en situaciones del mundo real.

c) **Despliegue**: Se produce un tratamiento de datos cuando el sistema de IA incluya datos personales o exista alguna manera de obtenerlos.

d) **Inferencia**: Existe tratamiento de datos personales cuando se utilicen datos del interesado en el sistema de IA para obtener un resultado, cuando se utilicen datos de terceros para obtener un resultado, o cuando datos o inferencias del interesado se almacenen.

e) **Decisión**: Se va a producir un tratamiento de datos personales con la mera decisión sobre un interesado que lleve a cabo en el sistema de IA.

f) **Evolución**: Se va a producir un tratamiento de datos personales cuando se utilicen los mismos para refinar el modelo del sistema de IA[17].

g) **Retirada**: Se puede producir la retirada del servicio por dos motivos; por un lado, el componente de IA se retira por obsoleto en todos los tratamientos en los que se implemente; o bien,

12 Bericht über das öffentliche Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr, disponible en: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Konsultationsbericht.pdf?__blob=publicationFile&v=5

13 Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Ausschuss für Digitales des Deutschen Bundestages am Mittwoch, 24. Mai 2023, 14:30 – 16:30 Uhr, zum Thema „Generative Künstliche Intelligenz", disponible en: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Generative-K%C3%BCnstliche-Intelligenz.pdf?__blob=publicationFile&v=2

14 Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale, disponible en https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/a5c4a24d-4823-e014-93bf-1543f1331670?version=2.0

15 Disponibles en: https://www.youtube.com/GARAntedatipersonaliGP

16 Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, disponible en: https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf

17 En caso de que nos encontremos ante una evolución realizada en el componente adquirido por el propio interesado, de forma aislada y autónoma, se aplicaría la excepción doméstica, salvo que se envíen a terceros los datos personales, ya que se estaría produciendo una comunicación de datos.

un usuario del sistema de IA decide no utilizar dicho componente.

La AEPD considera que cualquier solución técnica de IA que trate datos personales deberá incorporar ciertos parámetros de control de la calidad que deben poder ser acreditados para poder cumplir con los requisitos básicos de "accountability", transparencia y legalidad. Como ejemplos de dichos parámetros de control el supervisor español cita los siguientes:

- Precisión, exactitud o medidas de error requeridos por el tratamiento.
- Requisitos de calidad en los datos de entrada al componente IA.
- Precisión, exactitud o medidas de error efectivas de la solución IA en función de la métrica adecuada para medir la bondad de esta.
- Convergencia del modelo, cuando nos encontremos con entrenamiento y soluciones adaptativas.
- Consistencia entre los resultados del proceso de inferencia.
- Predictibilidad del algoritmo.
- Cualquier otro parámetro de evaluación del componente IA.

La AEPD considera que para cumplir con los requisitos fundamentales de responsabilidad ("accountability"), transparencia y legalidad, cualquier sistema de IA que maneje datos personales necesita integrar y demostrar ciertos estándares de calidad.

Además, la AEPD ha elaborado un documento donde desarrollan controles específicos para las auditorías de tratamientos de datos personales que utilizan IA para analizar y garantizar la protección de datos[18]. Esta guía se enfoca en la adecuación del tratamiento según los principios de protección de datos y ofrece notas metodológicas para estas auditorías.

b. El rol del responsable del tratamiento en los sistemas de IA

El regulador español también incide en la necesidad de distinguir con claridad las responsabilidades con respecto al tratamiento de los datos. En los sistemas de IA en los que se traten datos personales, el responsable del tratamiento será aquella persona física, jurídica, autoridad pública u otro, que tome la decisión de realizar el tratamiento de datos personales y que determine los medios y las finalidades del tratamiento.

En las distintas etapas de un sistema de IA podrán ostentar el rol de responsable del tratamiento distintas figuras:

i) **Fases de desarrollo, entrenamiento y validación**: La entidad que defina los fines de los componentes del sistema de IA y decida sobre los datos que se van a emplear en la fase de entrenamiento. Si el desarrollador es un tercero y esta toma las decisiones sobre los datos personales que se utilizan para entrenar los componentes de IA para sus propios fines también será considerado responsable.

ii) **Despliegue**: En caso de que la solución de IA sea un componente comercializado a otra entidad y se lleve a cabo un tratamiento de datos personales en el contexto de la solución de IA, tanto la entidad comercializadora como la entidad que compra la solución son responsables del tratamiento, produciéndose entre ellas una comunicación de datos personales[19].

iii) **Inferencia/perfilado**: La entidad que decide tratar los datos de los interesados a través de la solución de IA para sus propios fines[20].

iv) **Decisión**: La entidad que toma las decisiones automatizadas sobre los interesados para sus propios fines.

v) **Evolución o reentrenamiento**: La entidad que decide tratar los datos de los interesados a través de los sistemas de IA[21]. La entidad que determina la evolución de un componente del sistema de IA en base a los datos (cedidos directamente por los interesados o bien por la entidad que les proporciona el servicio) es considerado responsable del tratamiento.

18 Requisitos para Auditorías de Tratamientos que incluyan IA, disponible en: https://www.aepd.es/documento/requisitos-auditorias-tratamientos-incluyan-ia.pdf

19 Esto no aplica en caso de que la solución se comercialice a personas físicas, en este caso, únicamente ostentará el rol de responsable del tratamiento la entidad comercializadora

20 Esto no aplica en caso de que se lleve a cabo por una persona física sobre sus propios datos personales o los datos de las personas de su entorno para una actividad exclusivamente personal.

21 En caso de que comunique a una tercera entidad los datos personales de los usuarios del sistema de IA, la entidad será responsable de la comunicación de datos, siempre y cuando no exista una relación de responsable-encargado.

La decisión de emplear, dentro de un proceso de tratamiento de datos personales, una solución técnica basada en IA recae en la figura del responsable del tratamiento, que es el que va a definir los medios y fines del tratamiento de datos personales. El responsable va a tener que decidir entre las distintas soluciones tecnológicas que considere la más apropiada.

El responsable del tratamiento, en ningún caso, podrá eludir su responsabilidad, transfiriéndosela al propio sistema de IA.

c. Obligaciones que ha de cumplir el responsable del tratamiento de datos en una solución de IA

i) El cumplimiento de los principios rectores en materia de protección de datos

Conviene recordar que, en los sistemas de IA, el responsable del tratamiento ha de cumplir con todos y cada uno de los principios rectores en materia de protección de datos[22]. Sin embargo, resulta especialmente importante en el contexto de los sistemas de IA el principio de exactitud[23] ya que la inexactitud de los datos puede comprometer no solo el tratamiento de datos personales, sino también el funcionamiento del sistema de IA en sí mismo. El principio de exactitud ha de estar presente en todo el tratamiento (tanto en los datos de entrada, en los datos intermedios y en los datos de salida), pero es esencial en los datos de entrada, ya que puede dar lugar a sesgos que no forman parte del sistema de IA en sí[24].

ii) El deber de información a los interesados del RGPD y la obligación de transparencia del Reglamento de IA

El RGPD establece que cada responsable del tratamiento debe proporcionar a los interesados la información que se establece en los artículos 13 y 14 del RGPD para cumplir con el deber de información. En caso de que el interesado esté sometido a la toma de decisiones automatizadas o a la elaboración de perfiles[25], **el responsable del tratamiento debe, además, informar sobre la lógica aplicada y sobre la importancia y las consecuencias previstas**[26]. Por lo cual, **el responsable del tratamiento debe facilitar información que permita al interesado entender el comportamiento del tratamiento que se está produciendo de sus datos personales en los sistemas de IA** que implican la toma de decisiones automatizadas y/o la elaboración de perfiles[27].

3. Correlaciones del Reglamento de IA con el RGPD

Aunque actualmente no es posible realizar un análisis exhaustivo de la interacción entre el Reglamento de IA y el RGPD -debido a que el texto final de tal reglamento no ha sido publicado a la fecha de elaboración de este documento-, nos centraremos en lo establecido respecto a las obligaciones de transparencia, el ejercicio de derechos y la gestión de riesgos. Abordaremos los requisitos de cumplimiento desde las perspectivas de los datos y la IA, resaltando los enfoques diferenciados que se presentan a continuación.

a) Obligaciones de transparencia

Por lo cual, no sería suficiente cumplir con el principio de transparencia que propone el Reglamento de IA para cumplir con el deber de información establecido en el RGPD al responsable del tratamiento.

b) Ejercicio de derechos de los interesados en los sistemas de IA

El responsable del tratamiento deberá cumplir con el deber de atender los derechos de los interesados que se establece en el RGPD (acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de la toma de decisiones automatizadas)[28], debiendo establecer todos aquellos mecanismos y procedimientos necesarios para poder atender a las solicitudes de derechos que reciban. Dichos mecanismos deben ser adecuados a la dimensión del tratamiento que se esté llevando a cabo como consecuencia de la utilización de sistemas de IA.

En los sistemas de IA son especialmente importantes los derechos de los interesados que puedan estar tratándose en relación con la elaboración de perfiles y/o la toma de decisiones automatizadas.

Sin embargo, en los sistemas de IA también destaca el **derecho de supresión**, que implica el cumplimiento del principio de minimización de datos cuando la etapa de entrenamiento de los sistemas de IA ha finalizado, por ejemplo. También resulta interesante destacar la

22 Recogidos en el artículo 5 del RGPD.

23 Recogido en el artículo 5.1.d) del RGPD.

24 Lo cual se desarrolla en el Considerando 71 del RGPD.

25 A los que se hace referencia en el artículo 22 del RGPD.

26 Artículo 13.2 f) del RGPD.

27 Por ejemplo, el responsable del tratamiento podría informar acerca de los siguientes extremos: la calidad de los datos de entrenamiento y el tipo de patrones que se utilicen; los datos empleados para la toma de decisiones; la importancia relativa que tiene cada uno de los datos en la toma de decisiones; o los perfilados utilizados y sus implicaciones, etc.

28 Artículos 15 y siguientes del RGPD.

Obligación de transparencia

	Según el RGPD	Según el Reglamento de IA
Obligación de transparencia	Informar acerca del tratamiento de datos personales y el impacto que el tratamiento tiene en los derechos y libertades.	Informar con la trazabilidad y explicabilidad adecuadas, concienciando a los usuarios de que se comunican o interactúan con un sistema de IA, informando debidamente a los usuarios sobre las capacidades y limitaciones de dicho sistema de IA e informando a las personas afectadas de sus derechos.
Sujeto activo	El responsable del tratamiento	Diseñador del sistema de IA; desarrollador del sistema de IA; proveedor del sistema de IA; usuario que implemente el sistema de IA
Sujeto pasivo	El interesado	El usuario del sistema de IA
Tipo de información proporcionada	La establecida en el RGPD en relación con el deber de información , de manera que los interesados sean conscientes de los riesgos, de la existencia de la elaboración de perfiles y de las consecuencias de la misma, de los fines, de los derechos, de las garantías y de cualquier otra información que sea necesaria para garantizar un tratamiento leal y transparente, teniendo en cuenta las circunstancias específicas y el contexto en el que se tratan los datos personales.	Relacionada con la explicabilidad de los sistemas de IA, la documentación, el mantenimiento de registros y con el suministro de información sobre la manera de utilizar dicho sistema de IA. Debe ser suficiente para: (i) Permitir a los usuarios que despliegen el sistema de IA cumplir con sus obligaciones normativas. (ii) Advertir a las personas físicas que están interactuando con sistemas de IA.

obligación del responsable del tratamiento de atender el **derecho de rectificación** de los datos generados por los perfiles elaborados por la solución de IA. Asimismo, en caso de que existan datos inexactos de entrenamiento en el modelo de IA que puedan contener datos inexactos de personas que puedan ser reidentificadas, pudiendo asociar a dichas personas una información errónea es necesario cumplir con el **derecho de rectificación**.

Los principios de transparencia en el Reglamento de IA y en el RGPD tienen significados diferentes, establecen obligaciones distintas, aplican (en ocasiones) a sujetos diferentes, se refieren a tipos de información distinta y se dirigen a (en ocasiones) destinatarios distintos.

Asimismo, cuando el tratamiento se efectúa por medios automatizados, el RGPD también establece el derecho del interesado a recibir los datos personales que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica y a transmitirlos a otro responsable cuando la legitimación se basa en el consentimiento o en la necesidad contractual. El responsable del tratamiento que incluya sistemas de IA debe evaluar si los tratamientos concretos que lleva a cabo están sujetos a la obligación de proporcionar la portabilidad de los datos.

c) La gestión de riesgos y las evaluaciones de impacto

El responsable del tratamiento debe de llevar a cabo un análisis del riesgo del tratamiento teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personales físicas. En función de este análisis, el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme al RGPD[29], debiendo revisar y actualizar las medidas cuando sean necesarias. En el caso de los sistemas de IA, con el objetivo de determinar el nivel de riesgo de un tratamiento, el responsable del tratamiento deberá tener en cuenta lo siguiente:

29 Según lo dispuesto en el artículo 24 del RGPD.

i) Los riesgos derivados del tratamiento en sí mismo, siendo el más común el derivado del sesgo en los sistemas de toma de decisiones sobre las personas o su discriminación.

ii) Los riesgos derivados del tratamiento en relación con el contexto social y los efectos colaterales que se pueden derivar de él.

Los sistemas de IA, por su propia naturaleza, pueden entrañar un alto riesgo para los derechos y libertades de los interesados y, por tanto, en la mayoría de los casos, el responsable del tratamiento deberá llevar a cabo una evaluación de impacto en materia de protección de datos ("**EIPD**")[30], en concreto, cuando se lleve a cabo la elaboración de perfiles, basados en tratamientos automatizados. Así, el responsable del tratamiento deberá identificar todas las decisiones tomadas en las distintas fases del tratamiento, detallarlas, analizar los parámetros de funcionamiento y evaluar los efectos que tienen sobre los interesados.

En el caso de que un sistema de IA sea considerado de alto riesgo[31], el implementador de dicho sistema debe realizar una evaluación de impacto en materia de derechos fundamentales[32]. Cuando el implementador deba llevar a cabo una evaluación de impacto relativa a la protección de datos, la evaluación de impacto en materia de derechos fundamentales se llevará a cabo junto con la evaluación de impacto relativa a la protección de datos.

4. Conclusiones y posible plan de acción

4.1. Conclusiones

La regulación de datos de carácter personal impacta significativamente el desarrollo y aplicación de la IA. Esta interacción entre esta normativa legal y una tecnología en evolución como la IA puede ser desglosada en distintos aspectos esenciales:

a) **Base legal para el tratamiento de datos**: El RGPD en la Unión Europea requiere que el tratamiento de datos personales esté respaldado por una base de legitimación lícita, que puede incluir el consentimiento, pero también otras como el interés legítimo, el cumplimiento de obligaciones legales o el interés público. Esto significa que la IA debe operar sobre datos personales basados en una de estas bases legales, lo que puede limitar la disponibilidad de ciertos conjuntos de datos para el desarrollo, entrenamiento y explotación de los sistemas de IA.

b) **Finalidad de la recolección de datos**: Las regulaciones de protección de datos personales exigen que los datos se recolecten para fines específicos, explícitos y legítimos. La IA, que a menudo encuentra nuevas aplicaciones y correlaciones en los datos existentes, debe adaptar su funcionamiento para no transgredir esta limitación, lo que puede representar un desafío en la expansión de sus capacidades y aplicaciones.

c) **Minimización de datos**: Aunque los sistemas de IA tienen la capacidad de procesar grandes volúmenes de datos, la regulación sobre protección de datos exige que solo se recolecten los datos estrictamente necesarios para el propósito establecido. Esto puede afectar la manera en que los algoritmos de IA acceden y utilizan los datos, fomentando enfoques más selectivos y centrados en la minimización de la información personal utilizada.

d) **Transparencia y explicabilidad**: Las regulaciones sobre protección de datos demandan transparencia y la posibilidad de explicar las decisiones basadas en datos personales. Esto impulsa el desarrollo de IA explicable o interpretable, que permita comprender el razonamiento detrás de las acciones y decisiones automatizadas que afectan a los individuos.

e) **Derecho al olvido**: Las regulaciones otorgan a los individuos el derecho a solicitar la eliminación de sus datos personales. Esto plantea un desafío técnico para los sistemas de IA, especialmente aquellos que han integrado estos datos en sus modelos predictivos o en la generación de conocimiento.

f) **Seguridad de los datos**: La IA puede funcionar tanto como una herramienta para fortalecer la seguridad de los datos como un objetivo para aquellos que buscan explotar vulnerabilidades en la protección de datos. La regulación deberá desarrollarse en los próximos años para proteger la integridad de los datos pero también para tratar de establecer estándares para el uso seguro de la IA.

g) **Responsabilidad y gobernanza** de datos: La regulación de datos personales demanda una clara asignación de responsabilidades en el tratamiento de datos. En el caso de la IA, esto significa que los desarrolladores y operadores de sistemas de IA deben establecer mecanismos de gobernanza robustos para garantizar el cumplimiento normativo.

En resumen, la regulación de datos personales plantea una serie de restricciones y desafíos que deben ser considerados en el ciclo de vida completo de los sistemas de IA. No obstante, estos marcos regulatorios también promueven prácticas que pueden mejorar la confianza del público en la IA, al asegurar un manejo ético y responsable de los datos personales. La innovación tecnológica en IA, por lo tanto, debe coexistir con una gestión de datos personales que respete los

30 Siempre y cuando se den las condiciones establecidas en el artículo 35 del RGPD.

31 Según se establece en el artículo 6 y siguientes del Reglamento de IA.

32 En virtud de lo establecido en el artículo 29 bis del Reglamento de IA.

derechos individuales y las demandas legales, un equilibrio que no solo es posible, sino fundamental para el desarrollo sostenible y ético de la Inteligencia Artificial.

> ***La regulación de datos personales plantea una serie de restricciones y desafíos que deben ser considerados en el ciclo de vida completo de los sistemas de IA.***

4.2. Plan de acción

A continuación, presentamos un posible plan de acción para organizaciones que desarrollan o utilizan sistemas de IA que tratan datos de carácter personal:

a) **Evaluar la base de legitimación lícita**: Identificar y documentar claramente la base legal que justifica el uso de datos personales en los sistemas de IA, asegurándose de cumplir con los requisitos establecidos por la normativa de protección de datos.

b) **Integrar principios de protección de datos en el diseño del sistema de IA**: Implementar el concepto de "privacidad por diseño" desde el inicio del ciclo de vida del sistema de IA, garantizando que la recopilación, la minimización, el tratamiento y la seguridad de los datos estén alineados con los principios y obligaciones legales.

c) **Desarrollar mecanismos de transparencia y explicabilidad**: Priorizar el desarrollo de sistemas de IA que puedan explicar de manera clara y comprensible sus decisiones basadas en datos personales, permitiendo a los individuos entender y cuestionar las acciones automatizadas.

d) **Establecer procedimientos para la gestión de derechos de los titulares de datos**: Implementar procesos para responder de manera efectiva a solicitudes de acceso, rectificación, eliminación y oposición de datos personales, en línea con los requerimientos de la normativa de protección de datos.

e) **Capacitación y concientización sobre protección de datos**: Proporcionar formación especializada a los profesionales involucrados en el desarrollo y uso de sistemas de IA, promoviendo una cultura de respeto por la privacidad y la protección de datos personales.

f) **Integrar EIPD**: Realizar EIPD para analizar y mitigar los riesgos asociados al uso de datos personales en los sistemas de IA, colaborando estrechamente con los responsables de privacidad dentro de la organización.

g) **Gobernanza de datos y responsabilidad**: Establecer estructuras de gobernanza sólidas que definan claramente las responsabilidades y los procedimientos para el tratamiento de datos personales en el contexto de la IA, asegurando la supervisión y rendición de cuentas en todas las etapas del proceso.

h) **Monitorización y adaptación continua**: Implementar sistemas de monitorización y evaluación que permitan identificar posibles desviaciones con respecto a los requisitos legales y las mejores prácticas en protección de datos, con el fin de realizar ajustes oportunos y garantizar el cumplimiento continuo.

Es importante resaltar que, a diferencia del futuro Reglamento de IA, la normativa de protección de datos aplicable a este ámbito ya está plenamente en vigor. Por ello, al seguir este plan de acción, las organizaciones podrán garantizar que el desarrollo y la explotación de sistemas de IA se alineen con los principios de protección de datos personales, promoviendo la confianza pública y mitigando los riesgos legales y éticos asociados al uso de estas tecnologías.

Diferencias en las evaluaciones de impacto de riesgos en datos personales e IA

	EIPD	Evaluación de impacto en materia de derechos fundamentales
Sujeto activo	El responsable del tratamiento	El usuario que implemente el sistema de IA
¿Cuándo debe llevarse a cabo?	Cuando sea probable que un tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.	Cuando el sistema de IA sea considerado de alto riesgo.
¿Qué elementos debe contener?	Como mínimo: • Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento y, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; • Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; • Una evaluación de los riesgos para los derechos y libertades de los interesados; y • Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el Reglamento de IA, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.	Como mínimo: • Una descripción clara de la finalidad prevista para la que se utilizará el sistema de IA; • Una descripción clara del ámbito geográfico y temporal previsto de utilización del sistema de IA; • Las categorías de personas físicas y grupos que puedan verse afectados por la utilización del sistema de IA; • Una verificación de que la utilización del sistema de IA es conforme a Derecho en materia de derechos fundamentales; • El impacto razonablemente previsible en los derechos fundamentales de poner en uso el sistema de IA de alto riesgo; • Los riesgos de perjuicio específicos que puedan afectar a personas marginadas o a grupos vulnerables; • Las repercusiones negativas razonablemente previsibles del uso del sistema de IA en el medio ambiente; • Un plan detallado sobre cómo se mitigarán los perjuicios y el impacto negativo en los derechos fundamentales; • El sistema de gobernanza que pondrá en marcha el usuario que implemente el sistema de IA, incluida la vigilancia humana, la tramitación de reclamaciones y las vías de recurso.
¿Cuándo debe llevarse a cabo?	Antes del inicio del tratamiento de datos personales. En sistemas de IA, antes del diseño, selección o implementación de la solución de IA para un determinado tratamiento.	Antes de la puesta en funcionamiento del sistema de IA
¿Debe comunicarse a la autoridad de supervisión?	No	Sí, a la autoridad nacional de supervisión, cuando el usuario que implemente el sistema de IA no sea una pyme.
¿Debe comunicarse a las partes interesadas?	No, se podrá recabar la opinión de los interesados en relación con el tratamiento previsto	Si, cuando el usuario que implemente el sistema de IA no sea una pyme.

Pérez-Llorca

TECHLAW

Inteligencia artificial

ENERO 2024

Un reto para las compañías y para los reguladores

Barcelona
-
Brussels
-
Lisbon
-
London
-
Madrid
-
New York
-
Singapore

perezllorca.com