Deusto Journal of Human Rights
Revista Deusto de Derechos Humanos

No. 14/2024

DOI: https://doi.org/10.18543/djhr142024

ARTICLES / ARTÍCULOS

Impacto de la inteligencia artificial en los derechos de los interesados: una perspectiva práctica

Impact of artificial intelligence on data subjects' rights: a practical overview

María Luisa González Tapia
https://doi.org/10.18543/djhr.3198
Fecha de publicación en línea: diciembre de 2024

Copyright (©)

Deusto Journal of Human Rights / Revista Deusto de Derechos Humanos is an Open Access journal; which means that it is free for full and immediate access, reading, search, download, distribution, and reuse in any medium only for non-commercial purposes and in accordance with any applicable copyright legislation, without prior permission from the copyright holder (University of Deusto) or the author; provided the original work and publication source are properly cited (Issue number, year, pages and DOI if applicable) and any changes to the original are clearly indicated. Any other use of its content in any medium or format, now known or developed in the future, requires prior written permission of the copyright holder.

Derechos de autoría (©)

Deusto Journal of Human Rights / Revista Deusto de Derechos Humanos es una revista de Acceso Abierto; lo que significa que es de libre acceso en su integridad inmediatamente después de la publicación de cada número. Se permite su lectura, la búsqueda, descarga, distribución y reutilización en cualquier tipo de soporte sólo para fines no comerciales y según lo previsto por la ley; sin la previa autorización de la Editorial (Universidad de Deusto) o la persona autora, siempre que la obra original sea debidamente citada (número, año, páginas y DOI si procede) y cualquier cambio en el original esté claramente indicado. Cualquier otro uso de su contenido en cualquier medio o formato, ahora conocido o desarrollado en el futuro, requiere el permiso previo por escrito de la persona titular de los derechos de autoría.

Impacto de la inteligencia artificial en los derechos de los interesados: una perspectiva práctica

Impact of artificial intelligence on data subjects' rights: a practical overview

María Luisa González Tapia
Ramón y Cajal Abogados. España
mlgonzalez@ramoncajal.com
ORCiD: https://orcid.org/0009-0007-5281-5219

https://doi.org/10.18543/djhr.3198

Fecha de recepción: 30.05.2024
Fecha de aceptación: 25.10.2024
Fecha de publicación en línea: diciembre de 2024

Cómo citar / Citation: González Tapia, María Luisa. 2024. «Impacto de la inteligencia artificial en los derechos de los interesados: una perspectiva práctica». *Deusto Journal of Human Rights*, n. 14: 313-339. https://doi.org/10.18543/djhr.3198

Resumen: Los denominados derechos del interesado, que aparecen regulados en el Capítulo III del Reglamento (UE) 2016/679, constituyen una de las principales herramientas puestas a disposición de los individuos para conseguir el control efectivo sobre sus datos personales. Entre dichos derechos figuran los de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento, además del poco ejercitado hasta la fecha derecho a no ser objeto de decisiones automatizadas. Como norma general, estos

derechos son directamente exigibles frente al responsable del tratamiento, que debe dar una respuesta formal dentro un plazo definido, incluso en aquellos supuestos en que corresponda la denegación de la solicitud. Este artículo analiza los cambios que la sucesiva implantación de sistemas de inteligencia artificial puede provocar en las peticiones de los afectados y los problemas prácticos a los que, previsiblemente, se enfrentarán los responsables del tratamiento que deban darles respuesta. En particular, resalta la importancia de realizar una adecuada interpretación y aplicación del artículo 22 del citado Reglamento (UE) 2016/679, relativo a decisiones automatizadas.

Palabras clave: Inteligencia artificial, protección de datos, derechos de los interesados, obligaciones del responsable del tratamiento, decisiones automatizadas.

Abstract: The so-called data subjects 'rights, regulated in Chapter III of Regulation (EU) 2016/679, are one of the most relevant guarantees available to individuals to gain effective control over their personal data. These rights include the rights of access, rectification, erasure, objection, portability and restriction of processing, in addition to the hitherto little-exercised right not to be subject to automated decisions. As a general rule, these rights are directly enforceable against the controller, who must provide a formal response within a defined period of time, even in those cases where a refusal of the request is appropriate. This article analyses the changes that the successive implementation of artificial intelligence systems may bring about in the requests of data subjects and the practical problems that data controllers who have to respond to them will probably face. In particular, it highlights the importance of a proper interpretation and application of Article 22 of Regulation (EU) 2016/679 on automated decisions.

Keywords: Artificial intelligence, data protection, data subjects' rights, data controller's obligations, automated decisions.

1. **Los derechos de los interesados**

1.1. *Los derechos de los interesados, una garantía de control de los datos personales*

El Capítulo III del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD o Reglamento General de Protección de Datos) está dedicado a lo que se denominan "Derechos de los Interesados". Se inicia con el artículo 12 que recoge una serie de normas generales aplicables a todos ellos. En los preceptos siguientes, se regulan uno a uno los derechos propiamente dichos:

- Derecho a recibir información sobre el tratamiento (artículos 13 y 14).
- Derecho de acceso del interesado (artículo 15).
- Derecho de rectificación (artículos 16 y 19).
- Derecho de supresión o "derecho al olvido" (artículos 17 y 19).
- Derecho a la limitación del tratamiento (artículos 18 y 19).
- Derecho a la portabilidad de datos (artículo 20).
- Derecho de oposición (artículo 21).
- Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles (artículo 22).

A excepción del primero y el último, los derechos del interesado tienen en común dos características básicas:

- Ser facultades del titular de los datos directamente exigibles frente al responsable del tratamiento, sin necesidad de ejercer acciones legales o presentar reclamaciones ante las autoridades de control, y
- obligar al responsable del tratamiento a una respuesta activa y formal (incluso cuando corresponda denegar la petición por forma abusiva o improcedente).

Podemos afirmar que se trata de derechos instrumentales que permiten un control real e inmediato del individuo sobre la información personal que le concierne. Constituyen, en definitiva, la materialización práctica del derecho fundamental a la protección de datos[1].

[1] Como señala Herrán (2002: 246), "el derecho a la autodeterminación informativa -como principio que otorga a la persona la posibilidad de determinar el nivel de

En este sentido, resulta relevante recordar que las Sentencias del Tribunal Constitucional 290/2000[2] y 292/2000[3], a través de la cuales comienza a definirse en nuestro ordenamiento jurídico el derecho fundamental a la protección de datos como un derecho diferenciado del derecho a la intimidad (Murillo de la Cueva 2007), resaltaron como característica del por entonces nuevo derecho las garantías de control que atribuye a las personas. Así, la Sentencia 290/2000, en su fundamento jurídico séptimo, señaló lo siguiente sobre el derecho fundamental a la protección de datos:

> (…) garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos.
>
> En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales,

protección de los datos a ella referentes- encuentra su fundamento y su esencia en el reconocimiento de los derechos individuales con que la legislación otorga tutela a los interesados en la protección de datos personales. Los principios generales de protección de datos orientan y configuran la licitud del tratamiento de los datos personales, estableciendo los criterios elementales a seguir en el mismo. Las garantías individuales en la protección de datos constituyen instrumentos jurídicos al alcance de los interesados en defensa de sus derechos y libertades más esenciales".

[2] Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre (BOE n. 4, de 4 de enero de 2001). La sentencia resuelve los recursos de inconstitucionalidad acumulados n. 201/93, 219/93, 226/93 y 236/93, que fueron interpuestos, respectivamente, por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por D. Federico Trillo, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra los arts. 6.2, 19.1, 20.3, 22.1 y 2.1, 24, 31, 39.1 y 2, 40.1 y 2, y Disposición final tercera de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD). Disponible en https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274

[3] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (BOE n. 4, de 4 de enero de 2001). La sentencia resuelve el recurso de inconstitucionalidad n. 1463-2000, interpuesto por el Defensor del Pueblo, contra los arts. 21.1 y 24.1 y 2 de la LORTAD. Disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

> partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes.

Teniendo en cuenta lo anterior, no parece extraño que, desde los primeros textos internacionales sobre protección de datos, se hayan reconocido ciertas facultades de control al interesado sobre el tratamiento que efectúa una determinada entidad o Administración Pública, si bien su formulación no ha sido siempre la misma. Han experimentado una evolución en su contenido, en cierta medida acorde a los nuevos usos de los datos personales y a las tecnologías o medios empleados por los responsables[4].

1.2. *Aspectos prácticos del ejercicio de los derechos del interesado. Evolución desde la Directiva 95/46/CE al Reglamento General de Protección de Datos*

El antecedente inmediato del actual marco normativo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE), regulaba, en sus artículos 12 a 15, un catálogo de derechos de los interesados dividido en dos bloques:

— Cuatro derechos activos: acceso, rectificación, supresión y oposición.
— Dos garantías adicionales que, en principio, deberían ser desplegadas por el responsable del tratamiento sin necesidad

[4] En las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y el Desarrollo Económico de 1980 y, sobre todo, en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (Convenio 108), aparecen ya unos derechos activos del titular de los datos que suponen un control práctico del tratamiento en los términos a los que nos hemos referido en los párrafos anteriores. En el Convenio 108, se denominan "garantías complementarias para las personas concernidas". Además, del acceso, se reconoce la facultad de rectificar o borrar aquellas informaciones que sobre su persona están siendo tratadas, con posibilidad de recurrir (no se aclara si a la jurisdicción ordinaria o a una autoridad independiente) en caso de que su petición no sea atendida.

de una petición previa del titular de los datos: el derecho de información y el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa.

Durante los más de 20 años de aplicación de la citada norma y de sus leyes de transposición nacional, hablar de los derechos de los interesados significaba referirse a las facultades activas del primer bloque, que de manera muy resumida habilitaban al afectado para:

— solicitar que se le entregue una copia de los datos personales o se le informe de qué datos se están tratando;
— modificar datos incorrectos o desactualizados;
— pedir la supresión de los recogidos y almacenados por un responsable, y
— oponerse a la realización de determinados tratamientos, fundamentalmente, los relacionados con actividades comerciales.

El derecho de información se ha venido considerando más bien un deber del responsable del tratamiento, y no será objeto de análisis en este trabajo. Por su parte, el derecho a no verse sometido a determinadas decisiones automatizadas no ha tenido relevancia práctica hasta el momento. Como veremos, parece pensado para hacer frente a los retos actuales y, probablemente, se definirán mejor sus límites en los próximos años.

Tal y como los configuraba la Directiva 95/46/CE, los derechos activos influían en el tratamiento llevado a cabo por el responsable, que debía tomar determinadas medidas en función de lo solicitado por el titular de los datos como, por ejemplo, localizar la información referida a la persona que efectúa la petición en sus sistemas, determinar si procede suprimir o por el contrario está obligado a conservarlo, etc. En definitiva, el responsable se veía obligado a llevar a cabo una gestión de las peticiones recibidas, generalmente a través de procedimientos internos, que incluyen aspectos como:

— Establecer canales adecuados para la recepción de las peticiones.
— Formar al personal.
— Preparar modelos de respuesta.
— Acordar criterios para identificar a los solicitantes.
— Detallar supuestos de denegación de derechos.
— Desarrollar protocolos para la localización de los datos personales en los sistemas y archivos.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

La experiencia práctica consolidada con la Directiva 95/46/CE sirvió como base para que el Reglamento General de Protección de Datos reforzara y ampliara los derechos activos de los interesados, confiriéndoles mayor importancia, pero manteniendo el contenido esencial de todos ellos.

En primer lugar, como se ha indicado, el RGPD introdujo en su artículo 12 una serie de normas operativas para unificar criterios y aclarar dudas que se habían venido planteando en la resolución de solicitudes de afectados. Podemos resumir lo establecido en el referido precepto como sigue:

— Los derechos del interesado son gratuitos. No obstante, cuando las solicitudes sean infundadas o excesivas el responsable podrá cobrar un canon razonable para su ejercicio o negarse a atenderlo (artículo 12.5 del RGPD).
— Se dispone de un plazo de un mes para su atención, ampliable en dos meses adicionales por motivos justificados que han de comunicarse al afectado (art. 12.3 del RGPD).
— Deben responderse formalmente en todo caso, incluso cuando se deniegan. En este caso, se debe informar de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales (artículo 12.4 del RGPD).
— Como norma general, el afectado no debe adjuntar copia de su DNI para ejercer el derecho. No obstante, el responsable del tratamiento que tenga dudas razonables sobre la identidad de la persona que efectúa la solicitud podrá pedir que se le facilite la información adicional necesaria (art. 12.6 RGPD).

En segundo lugar, el RGPD matizó el contenido de los derechos previstos en la Directiva 96/46/CE, también con la intención de armonizar criterios y positivizar prácticas implantadas.

En tercer y último lugar, se añadieron nuevos derechos que pretendían asegurar un mayor control del individuo sobre sus datos personales: el derecho a la portabilidad y el derecho a la limitación del tratamiento.

Con todo ello, se esperaba, además de conseguir la uniformidad a la que nos hemos referido en todos los Estados miembros, dar un impulso mayor y enfatizar el papel de los derechos del interesado como instrumentos garantes del correcto tratamiento de los datos.

En algunos Estados miembros, la regulación incluida en el RGPD implicó un cambio sustancial en la atención del ejercicio de derechos. En España, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección

de Datos de Carácter Personal (LOPD) contaba con un reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre, que estableció una completísima regulación de los denominados popularmente "Derechos ARCO" (acrónimo de acceso, rectificación, cancelación y oposición). Dicho Real Decreto había clarificado supuestos de denegación de derechos, establecido plazos para su atención, y detallado los requisitos formales para su ejercicio por parte del titular de los datos (entre los que se incluía la presentación del DNI o documento equivalente, que como sabemos ya no es un requerimiento obligatorio y cuya su solicitud puede dar lugar al incumplimiento del principio de minimización). Adicionalmente, se implantó un procedimiento específico en nuestra autoridad de control para tutelar los Derechos ARCO, denominado precisamente procedimiento de tutela de derechos.

Por ello, en nuestro país el Reglamento General de Protección de Datos no conllevó un cambio brusco en la gestión de las solicitudes de derechos de los afectados. La importancia que esta gestión ha adquirido en los últimos seis años se debe, probablemente, a diversos factores. Por una parte, ha aumentado el grado de información y concienciación entre los afectados de los derechos que les reconoce la normativa de protección de datos. Por otra, los tratamientos que se realizan son cada vez más complejos, y esto conlleva mayores molestias para los afectados y, también, mayores temores (por poner algunos ejemplos, es fácil que un tercero nos grabe o nos saque una fotografía y lo cuelgue en Internet, recibimos publicidad muy dirigida con cada compra o visita que efectuamos on-line, nos puede llegar a sorprender la exactitud con la que se predicen nuestros gustos en las plataformas de contenidos, etc.).

Una actividad que parecía residual en el contexto del cumplimiento de las obligaciones en materia de protección de datos para las entidades responsables del tratamiento ha llegado a consumir una parte importante del tiempo de los profesionales de la privacidad, especialmente, por su carácter casuístico. Los interesados que ejercen los derechos, como es lógico, no están obligados a conocer la normativa y a entenderlos. Sus peticiones no encajan siempre exactamente en una de las facultades reguladas.

En definitiva, al hablar de derechos de los interesados tratamos una materia más compleja y cambiante de lo que se venía pensando hasta la fecha, como se pone de manifiesto al constatar que las primeras previsiones del legislador europeo sobre la aplicación práctica del Título III del RGPD no se han cumplido. Así, por ejemplo, el nuevo derecho a la portabilidad de datos que se presentaba como un avance importante

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

para los afectados, hasta ahora, no ha supuesto ningún beneficio tangible para los afectados con respecto al marco normativo anterior[5].

Son probablemente, los derechos "clásicos" de acceso[6] y, en menor medida, de oposición y supresión (rebautizado como "derecho al olvido") los que siguen planteando los mayores problemas a la hora de atender resoluciones de los afectados. En el caso del derecho de oposición, su relevancia y complejidad va unida a la utilización del interés legítimo como base legal que habilita determinados tratamientos.

Con la adopción de forma masiva por parte de las empresas de sistemas y modelos de Inteligencia Artificial (en adelante, IA) se empieza a intuir que se producirá un cambio muy significativo en el ejercicio de los derechos de los interesados.

Desde la perspectiva de la normativa de protección[7], como ha señalado la Agencia Española de Protección de Datos (en adelante, AEPD), los sistemas y modelos de IA son un mero instrumento en el tratamiento de datos personales. No obstante, se trata de una herramienta de enorme relevancia para la protección de datos personales, tanto por el uso masivo que puede llevar a efectuarse de ellos durante el proceso de generación y entrenamiento de sistemas y modelos de IA, como en el resultado mismo obtenido de su aplicación.

---

[5] Uno de los primeros documentos elaborados por el Grupo de Trabajo del Artículo 29 (2017) tras la aprobación del Reglamento General de Protección de Datos fue el relativo al derecho de portabilidad, donde expone lo siguiente: "Las personas que hacían uso de su derecho de acceso en virtud de la Directiva sobre protección de datos 95/46/CE, se veían limitadas por el formato elegido por el responsable del tratamiento para proporcionar la información solicitada. El nuevo derecho a la portabilidad de los datos tiene por objeto facultar a los interesados con respecto a sus propios datos personales, ya que mejora su capacidad de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro (ya sea a sus propios sistemas, a los sistemas de terceros de confianza o a los de otros responsables del tratamiento). Al afirmar los derechos personales de los individuos y el control sobre los datos personales que les conciernen, la portabilidad de los datos representa también una oportunidad para «reequilibrar» la relación entre los interesados y los responsables del tratamiento".

[6] Así lo ha reconocido el Comité Europeo de Protección de Datos (2023) dedicándole un documento.

[7] Según indica la Agencia Española de Protección de Datos (2023), "un sistema de Inteligencia Artificial (IA), o varios sistemas de IA, podría ser un medio seleccionado por un responsable para implementar operaciones de datos personales en un tratamiento. Es importante entender que la finalidad última de un tratamiento es diferente de los medios seleccionados para implementarlo. Con relación a esto, el responsable será quien determine si los resultados de un sistema de IA implicarían una decisión automática o determinará que se incluya una supervisión humana que tome la decisión final. Por lo tanto, las decisiones automatizadas no están en la naturaleza del sistema de IA, sino que son una opción elegida por el responsable".

2. La IA como herramienta para el tratamiento de datos personales

Coloquialmente, al hablar de IA nos referimos a programas informáticos que simulan la mente humana, y en particular, que tienen capacidad de aprendizaje y adaptación al entorno: pueden elaborar un texto complejo (por ejemplo, un relato) sobre unas premisas definidas, mantener una conversación en un servicio de atención al cliente, dar respuesta a preguntas en tiempo real, o generar imágenes que plasmen una descripción dada por una persona.

La IA no es una tecnología nueva pero su uso se ha generalizado de manera rápida en los últimos años. En 2017, la Comisión Europea estimaba que podría generar entre 6.5 y 12 billones de euros para el 2025 (Comisión Europea 2017). Al año siguiente, en el 2018, señalaba que

> al igual que hicieran la máquina de vapor o la electricidad en épocas anteriores, la IA está transformando nuestro mundo, nuestra sociedad y nuestra industria. El crecimiento de la capacidad informática y la disponibilidad de datos, así como los avances en los algoritmos, han convertido la IA en una de las tecnologías más estratégicas del siglo XXI (Comisión Europea 2018).

Como resulta lógico, afirmaciones como las anteriores se han visto acompañadas de la elaboración del marco regulatorio de la IA dentro en la Unión Europea. A finales de 2022, la Comisión Europea presentó dos propuestas legislativas en este sentido:

— Una propuesta de revisión de la Directiva 85/374/CE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.
— Una propuesta de norma específicamente dirigida a la IA, que acabó convirtiéndose en el Reglamento de Inteligencia Artificial aprobado por el Parlamento Europeo el pasado 13 de marzo (en adelante, RIA), y que se calificó en ese momento de "ley histórica" (Parlamento Europeo 2024).

El RIA tiene un enfoque de seguridad de producto, del que se regula su fabricación, puesta en mercado, distribución y uso. El producto en cuestión son los sistemas y modelos de IA. Los primeros (sistemas), se definen en su artículo 3 como aquellos basados

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

> en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales (DOUE 2024).

Frente a este concepto, los modelos de IA son códigos o funciones, más simplificados que los sistemas que no incluyen una variedad de componentes.

La definición legal arriba reproducida, de la que probablemente se publicarán documentos aclaratorios, incluye las mismas características básicas que forman parte de la idea que se asocia comúnmente entre los no expertos al concepto de IA: autonomía, adaptación y obtención de resultados sofisticados. Nos interesa destacar esto último, la capacidad de generar información de salida inferida de información de entrada, puesto que incide en la condición de herramienta o instrumento de los sistemas y modelos de IA, y en el valor que los datos, ya sean personales o no, tienen en su funcionamiento.

Resulta fácil imaginar que las mejoras que promete la utilización de IA en distintos campos no están exentas de riegos para los derechos y libertades de los ciudadanos. En materia de protección de datos, se debe resaltar que la IA ampliará las posibilidades de generación de contenidos y de realización de predicciones de todo tipo[8]. Tales predicciones pueden consistir en decisiones automatizadas que, por ejemplo, evalúen a los individuos considerándolos aptos o no aptos

---

[8] Según se expone en el documento elaborado conjuntamente por el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos (2021) sobre la nueva norma de inteligencia artificial*:*

> "Los datos (personales y no personales) en la IA son, en muchos casos, la premisa clave de las decisiones autónomas, lo que inevitablemente afectará a la vida de las personas a distintos niveles.
>
> Asignar a las máquinas la tarea de decidir a partir de datos creará riesgos para los derechos y libertades de las personas, afectará a su vida privada y podría perjudicar a algunos grupos o incluso a las sociedades en su conjunto. El CEPD y el SEPD subrayan que el derecho a la vida privada y a la protección de los datos personales, que contradicen con la asunción de la autonomía de decisión de las máquinas que subyace al concepto de IA, es un pilar de los valores de la UE reconocidos en la Declaración Universal de Derechos Humanos (artículo 12), el Convenio Europeo de Derechos Humanos (artículo 8) y la Carta de los Derechos Fundamentales de la UE (en lo sucesivo, «la Carta») (artículos 7 y 8). Conciliar la perspectiva de crecimiento que ofrecen las aplicaciones de IA y la centralidad y primacía de los seres humanos frente a las máquinas es un objetivo muy ambicioso, pero necesario".

para un puesto de trabajo o para obtener un determinado beneficio, o los categoricen en determinados grupos o perfiles en función de parámetros que pueden resultar erróneos o discriminatorios.

El mayor peligro consiste en que, a medida que se confía en un sistema o modelo de IA para efectuar una tarea como las indicadas, se pierde la capacidad de análisis detallado del supuesto concreto y de la relación de causalidad entre la información de la que se parte y el resultado obtenido.

El cumplimiento de las obligaciones contenidas en el RIA no exime del cumplimiento del RGPD en todas las fases en las que se utilicen datos personales. Tal y como señala su Considerando (9),

> las normas armonizadas que se establecen en el presente Reglamento deben aplicarse en todos los sectores y, en consonancia con el nuevo marco legislativo, deben entenderse sin perjuicio del Derecho vigente de la Unión, en particular en materia de protección de datos, protección de los consumidores, derechos fundamentales, empleo, protección de los trabajadores y seguridad de los productos, al que complementa el presente Reglamento. En consecuencia, permanecen inalterados y siguen siendo plenamente aplicables todos los derechos y vías de recurso que el citado Derecho de la Unión otorga a los consumidores y demás personas que puedan verse afectados negativamente por los sistemas de IA (DOUE 2024).

Por tal motivo, resulta fácil entender que la introducción de herramientas de IA afectará a distintos aspectos de la protección de datos, y en particular, a la forma en la que se atienden los derechos de los interesados que parecen en este contexto más necesarios que nunca para asegurar un control efectivo sobre los datos personales.

3. **Peculiaridades de la atención del ejercicio de derechos en tratamientos que incluyen IA**

3.1. *Rediseño de las políticas y procedimientos de atención de derechos internos*

Comenzaremos indicando que la aparición de componentes de IA en un tratamiento de datos no conlleva, en principio, ninguna excepción en lo que se refiere al ejercicio de los derechos del afectado. Así lo señala expresamente la AEPD en uno de los documentos que ha dedicado al análisis de tratamientos que incluyen IA:

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

> Los responsables que hagan uso de soluciones de IA para tratar datos personales, elaborar perfiles o tomar decisiones automatizadas, han de ser conscientes de que los interesados tienen derechos en el ámbito de la protección de datos que deben ser atendidos.
>
> Por lo tanto, durante la fase de concepción del tratamiento, los responsables han de ser conscientes de que tienen que establecer mecanismos y procedimientos adecuados para poder atender las solicitudes que reciban, y que dichos mecanismos deberán estar adecuadamente dimensionados para la escala del tratamiento que están efectuando (Agencia Española de Protección de Datos 2020).

El responsable del tratamiento, que seguramente ya dispone de procedimientos de atención al ejercicio de derechos del afectado desde antes de la aprobación del RGPD, deberá plantearse ahora nuevos supuestos.

Hemos reseñado que la gestión de derechos se ha convertido en un aspecto complejo en un gran número de organizaciones y, en este contexto, la IA supondrá un mayor nivel de dificultad. Por tanto, resulta recomendable (i) llevar a cabo un estudio detallado de las posibles peticiones de los afectados en tratamientos y (ii) documentar criterios fundamentados jurídicamente tanto en relación con la forma en la que harán efectivas solicitudes como con los supuestos en los que se denegarán.

Sin este análisis no es posible adoptar mecanismos realistas y proporcionales para garantizar el ejercicio de derechos adaptándose al nivel de riesgo de cada tratamiento. Además, se ha de tener en cuenta que la utilización de sistemas y modelos de IA en las operaciones de tratamiento tendrá que ir acompañada de la realización o revisión de los análisis de riesgos y de las evaluaciones de impacto (que probablemente se deberán efectuar por lo novedoso de la tecnología, los volúmenes de datos utilizados y el carácter potencialmente intrusivo). Estos documentos internos deberían contemplar una descripción de cómo se van a atender los derechos en cada caso.

3.2. *Principales problemas generados por la utilización de sistemas y modelos de IA en el tratamiento de datos*

Entendemos que los cinco principales problemas que surgirán en el análisis y rediseño de los procedimientos de atención al ejercicio de derechos son los siguientes:

3.2.1. Dificultad en la localización de los datos del interesado

Normalmente, esta dificultad proviene del volumen de datos tratados o su dispersión en distintos sistemas que no han sido adecuadamente inventariados. No obstante, en algunos casos, también se deberá al hecho de no conocer si se están tratando o no datos personales en una etapa concreta del proceso[9].

Por ejemplo, durante la fase de entrenamiento de sistemas o modelos, donde se maneja una gran cantidad de información, los datos personales de base pueden someterse a procesos de anonimización (eliminación de cualquier posibilidad de vinculación con el individuo al que se refieren) o seudonimización.

Los procesos de anonimización constituyen tratamientos de datos en sí. Al menos en su inicio, partimos de datos personales en relación a los cuales los interesados pueden ejercer sus derechos. El ejercicio de derechos en estos supuestos no resulta baladí, sobre todo cuando se solicita la oposición a tratamientos basados en el interés legítimo y facilitar tal oposición constituye una garantía esencial del afectado. Adicionalmente, la anonimización no siempre es efectiva, y podría existir la posibilidad de reidentificación (y, por tanto, tratamiento de datos personales) en un futuro, bien por errores no previstos o por la mera evolución técnica[10].

Por lo que se refiere a la seudonimización, resulta necesario destacar que la dificultad en la identificación de un afectado no implica que no se estén tratando datos personales y, consiguientemente, no excluye la atención del ejercicio de derechos. En este sentido, a veces

[9] A modo de ejemplo, señalaremos lo indicado por la Agencia Española de Protección de Datos (2020): "Puede haber tratamientos que incluyen componentes de IA que manejan datos de personas físicas, como en un modelo de perfilado de marketing o electoral, o puede haber tratamientos en los que no aparezcan datos de carácter personal, como podría suceder en un modelo de predicción meteorológico que recoge datos de estaciones geográficamente distribuidas. Un tratamiento que tome decisiones automatizadas usando la inteligencia artificial puede afectar a personas físicas, como por ejemplo un sistema de autenticación de usuarios, o puede no afectar a personas, como un sistema de control industrial. En el que caso de que se tomen decisiones que afectan a las personas, estas decisiones pueden ser relativas a la interacción de la persona en su contexto social, como el acceso a un contrato o servicio, o relativas a la personalización de dicho servicio, como podría ser la personalización en los mandos de un coche o la programación de un televisor".

[10] La Agencia Española de Protección de Datos (2016) y Personal Data Protection Commission Singapore (2022) han publicado en su página web distintos documentos orientativos sobre cómo realizar procesos de anonimización correctos, donde se resaltan los riesgos de reidentificación producidos por la evolución de las tecnologías.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

resulta de utilidad solicitar información adicional al afectado que ejerce un derecho a los efectos de obtener nuevos parámetros de búsqueda.

En otras ocasiones, tal y como pone de manifiesto la autoridad de protección de datos de Reino Unido, la *Information Commissioner's Office* (ICO) (s.f.), aunque el responsable debe atender la solicitud de todos los interesados, pueden darse supuestos en los que la petición resulte excesiva o desproporcionada. Por tanto, sería posible denegarla. La lógica nos dice que no podemos olvidar que la seudonimización es una garantía para el propio afectado, ya que reduce la información personal que se somete a tratamiento, y su aplicación no debería penalizar al responsable a la hora de cumplir con otras obligaciones como la atención del ejercicio de derechos haciéndola más complicada. Dado que siempre corresponderá la carga de la prueba al responsable, es aconsejable documentar y justificar los escenarios de denegación de peticiones.

3.2.2. Imposibilidad de eliminación o modificación de los datos personales

Algunas soluciones tecnológicas no permiten suprimir definitivamente los datos o ejecutar cambios en los mismos y, por tanto, imposibilitan en sí mismas la correcta atención de los derechos de los afectados.

El derecho de supresión resulta, por otro lado, especialmente complicado de atender por las dudas que, inevitablemente, surgen sobre (i) los plazos de conservación aplicables y (ii) la procedencia de aplicar la figura del bloqueo recogida en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Según este precepto, cuando un afectado ejerce el derecho de supresión, los datos no se deben eliminar sino conservarse aplicando medidas técnicas y organizativas que impidan cualquier tipo de utilización, incluyendo el mero acceso, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos.

El análisis de riesgos y la evaluación de impacto realizados en las primeras fases del tratamiento han de contemplar aspectos que luego simplificarán la atención del ejercicio de derechos como plazos de conservación, medidas de bloqueo de datos, revisión de mecanismos técnicos para garantizar la eliminación o cancelación de la información, o existencia de canales apropiados para el ejercicio de derechos.

También deberían reseñar si, en el momento del diseño de la infraestructura o sistema de tratamiento, se han incluido medidas que permitan suprimir o bloquear datos en caso de ser necesario.

Entendemos que, en última instancia, se trata de una obligación que corresponde al proveedor o fabricante, pero el responsable del tratamiento que actúe, por utilizar la terminología del RIA, como responsable del despliegue ha de aplicar medidas de diligencia en la selección del producto que utiliza.

3.2.3. Dependencia de terceros proveedores que actúan como encargados del tratamiento

En la misma línea expuesta en el punto anterior, cuando parte de los datos personales se alojan en los sistemas del encargado, siendo además éste quien trabaja sobre los mismos, se han de establecer mecanismos de comunicación que permitan al responsable verificar que los derechos se ejecutan correctamente.

En este sentido, la adopción de medidas previas a la contratación para verificar las garantías que ofrece el proveedor para una correcta atención del ejercicio de derechos podría resultar cada vez más relevante, así como la inclusión de cláusulas específicas en los contratos de encargo del tratamiento.

En todo caso, la utilización de encargados del tratamiento tampoco exime al responsable del cumplimiento de sus obligaciones de atención de los derechos del afectado. Recordemos que los proveedores de soluciones tecnológicas también quedan obligados por los principios de privacidad desde el diseño y por defecto y deberían desarrollar sus productos incluyendo garantías que permitan una correcta atención de los derechos.

3.2.4. Asignación de recursos a la gestión interna de los derechos

Como consecuencia de los puntos anteriores, es posible que en algunas organizaciones la atención de derechos requiera que se involucren perfiles distintos a los habituales, especialmente con un componente más técnico que permita comprender el funcionamiento de los sistemas y modelos de IA.

La formación y la comprensión del funcionamiento de los sistemas y modelos de IA resultará básica para poder dar una respuesta adecuada a las peticiones recibidas de los interesados.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

3.2.5. Ejercicios de derechos relacionados con el resultado de la aplicación de IA o información de salida

Siendo los anteriores puntos muy relevantes, el mayor impacto previsiblemente se producirá en el ejercicio de derechos en la fase de obtención de resultados. En esos casos, desde el punto de vista de protección de datos, cobra relevancia determinar si los elementos de IA sirven para obtener perfiles individualizados o tomar decisiones automatizadas. Ambas actividades se consideran generalmente intrusivas.

El art. 4.4 del RGPD determina que "elaboración de perfiles" consiste en

> 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.

Esta definición implica que se cumplan tres requisitos acumulativos:

— es un tratamiento automatizado;
— emplea datos personales; y
— el objetivo es realizar una evaluación o juicio aplicable a un individuo concreto con una finalidad de seguimiento o de tratamiento también individualizada. Conocer el perfil genérico o tipo de cliente (por ejemplo, que el comprador típico de un producto es mujer profesional de 30 años) tras un análisis de las características de los compradores de una tienda on-line no implica la elaboración de un perfil, aunque para ello se hayan partido del tratamiento de datos personales de un número relevante de compradores.

El RGPD introduce posteriormente en su articulado otro concepto que no define: decisión basada únicamente en el tratamiento automatizado. Las decisiones automatizadas parecen tener un ámbito de aplicación distinto a la elaboración de perfiles, aunque pueden solaparse. Suponen la utilización medios tecnológicos para suplantar la capacidad humana en actividades tales como asignar, seleccionar o eliminar candidatos a puestos de trabajo, predecir el nivel de riesgo de impago de un préstamo, aplicar unos determinados parámetros para asignar turnos o proponer compras, etc. El perfilado podría ser un tipo

de decisión automatizada, pero las decisiones automatizadas no implican necesariamente elaborar perfiles. Por otro lado, una vez perfilado un individuo, se podrían tomar decisiones que le afecten de forma automatizada o no.

Los conceptos anteriores no son fáciles de entender y diferenciar, aunque se intuyen potencialmente peligrosos para los derechos del afectado. El artículo 22 del RGPD reconoce un derecho específico relacionado con ambas operaciones, bajo el epígrafe "decisiones individuales automatizadas, incluyendo la elaboración de perfiles". A este derecho, no se le ha prestado demasiada atención hasta la fecha (raramente se menciona en los textos informativos de privacidad). Su contenido y utilidad práctica se irá concretando en el futuro como veremos a continuación.

4. **Decisiones automatizadas: el olvidado artículo 22 del RGPD**

4.1. *Contenido del derecho reconocido en el artículo 22 del RGPD*

El Capítulo III del RGPD se cierra con el reconocimiento de un derecho de los interesados que se formula en el artículo 22.1 como sigue:

> Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Si bien parece introducido específicamente para responder a las necesidades que presenta el momento actual, en el que la IA parece que se convertirá en la herramienta básica de trabajo de muchas organizaciones, el origen de este derecho se remonta a la primera ley de protección de datos francesa de 1970. También nuestra primera ley orgánica de protección de datos, Ley Orgánica 5/1992, de 29 de octubre, conocida como LORTAD, reconocía entre los derechos de las personas el derecho a la impugnación de valoraciones basadas exclusivamente en datos automatizados. Por su parte, la Directiva 95/46/CE reguló un derecho en términos similares a los del citado artículo 22 del RGPD: el derecho a no verse sometido a determinadas decisiones automatizadas, dando lugar a transposiciones que diferían sustancialmente en los distintos Estados miembros. En la transposición al derecho nacional, algunos como Bélgica establecieron una

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

prohibición, mientras que otros, como Suecia, garantizaron un sistema de *opt-out* u oposición.

En definitiva, no nos encontramos ante una facultad o derecho totalmente nuevo. Sin embargo, ha sido poco utilizado en la práctica y no ha dado lugar ni a la imposición de número elevado de sanciones por las autoridades de control nacionales ni a resoluciones o sentencias que interpreten su contenido.

En 2017, previendo la relevancia que podría tener por el auge en la utilización de IA, el desaparecido Grupo de Trabajo del Artículo 29 (GT 29) (2018) le dedicó un documento específico. En su introducción, se apuntan los problemas y riesgos derivados del uso masivo de datos y la irrupción de la IA:

> La elaboración de perfiles y las decisiones automatizadas se utilizan en un número creciente de sectores, tanto privados como públicos.
>
> El sector bancario y financiero, la asistencia sanitaria, la fiscalidad, los seguros, la mercadotecnia y la publicidad son solo algunos ejemplos de los ámbitos en los que se lleva a cabo con más regularidad la elaboración de perfiles para contribuir al proceso de toma de decisiones.
>
> Los progresos tecnológicos y las posibilidades del análisis de macrodatos, la inteligencia artificial y el aprendizaje automático han facilitado la creación de perfiles y han automatizado las decisiones, y tienen el potencial de afectar de forma significativa a los derechos y libertades de las personas. (…)
>
> No obstante, la elaboración de perfiles y las decisiones automatizadas pueden plantear riesgos importantes para los derechos y libertades de las personas que requieren unas garantías adecuadas.
>
> Estos procesos pueden ser opacos. Puede que las personas no sean conscientes de que se está creando un perfil sobre ellas o que no entiendan lo que implica.
>
> La elaboración de perfiles puede perpetuar los estereotipos existentes y la segregación social. Asimismo, puede encasillar a una persona en una categoría específica y limitarla a las preferencias que se le sugieren. Esto puede socavar su libertad a la hora de elegir, por ejemplo, ciertos productos o servicios como libros, música o noticias. En algunos casos, la elaboración de perfiles puede llevar a predicciones inexactas. En otros, puede llevar a la denegación de servicios y bienes, y a una discriminación injustificada.

La anterior descripción podría servir para ejemplificar los efectos negativos de los sesgos o *bias* que pueden darse en sistemas de IA.

Por ello, el documento del GT 29 constituye una herramienta que ha cobrado gran utilidad: las recomendaciones que se establecen en el mismo son en la práctica un listado de controles críticos de cumplimiento para sistemas y modelos de IA (entre otros, cumplimiento de principio de licitud y transparencia, minimización de datos y respeto al principio de finalidad).

Centrándonos en la interpretación del derecho reconocido en el artículo 22, el GT 29 aclara algo que había sido objeto de discusión hasta ese momento por las diferencias en las transposiciones nacionales de la Directiva 95/46/CE que se han mencionado: el apartado 1 de este precepto debe interpretarse como una prohibición genérica de decisiones automatizadas que produzcan efectos que podemos definir como trascendentes en los afectados. No requiere una actividad del afectado (una solicitud formal) para que el artículo despliegue sus efectos.

Como señala el GT 29 esta

> interpretación refuerza la idea de que sea el interesado quien tenga el control sobre sus datos personales, lo cual se corresponde con los principios fundamentales del RGPD. Interpretar el artículo 22 como una prohibición en vez de como un derecho que debe invocarse significa que las personas están protegidas automáticamente frente a las posibles consecuencias que pueda tener este tipo de tratamiento.

Además, el GT 29 pone el derecho en relación con el Considerando 71 del RGPD, que determina:

> Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros [...], o necesario para la conclusión o ejecución de un contrato [...], o en los casos en los que el interesado haya dado su consentimiento explícito.

La prohibición del artículo 22, en todo caso, no es absoluta, ya que tiene dos límites:

a) Por un lado, solo se aplica a decisiones totalmente automatizadas que, además, han de producir (i) efectos jurídicos, como la resolución de un contrato o la retirada de un beneficio social, o (ii) afectar significativamente de modo similar a las personas. En este último punto, deberíamos incluir

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

consecuencias relevantes para el afectado como su no selección para un puesto de trabajo e, incluso, determinadas acciones promocionales que tengan un carácter intrusivo. A modo de ejemplo, podemos señalar las campañas dirigidas a menores o colectivos vulnerables (personas susceptibles de contratar préstamos rápidos o jugar on-line).

A sensu contrario, si no existe una automatización total o los efectos de la decisión no son ni jurídico ni especialmente relevantes, podrá efectuarse el tratamiento.

b) Por otro lado, el apartado segundo del mismo artículo 22 señala tres excepciones que permiten llevar a cabo las decisiones automatizadas inicialmente prohibidas. Estas excepciones se dan en los siguientes supuestos:

— Cuando la decisión automatizada es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
— Cuando está autorizada por el Derecho de la Unión o de los Estados miembros, que además deberá establecer medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
— Cuando se basa en el consentimiento explícito de los interesados.

En definitiva, el legislador protege a los interesados con el reconocimiento de un derecho que se plasma en la existencia de una prohibición general, similar a la del artículo 9.1 del RGPD. Como en el caso de este último precepto, se han regulado excepciones que levantan dicha prohibición.

4.2. *La dificultad de determinar cuándo nos encontramos ante una decisión automatizada*

La principal tarea a la que se enfrentan los responsables del tratamiento a la hora de garantizar el derecho del artículo 22 es la de catalogar una decisión como completamente automatizada e identificar los efectos que puede producir en el afectado. El derecho no obliga a prever respuestas o a reaccionar cuando el afectado lo pide, sino más bien a justificar un tratamiento desde su origen, analizando si es lícito de acuerdo con el Reglamento General de Protección de Datos.

Como se ha explicado, no existe un amplio abanico de resoluciones que interpreten el artículo 22 que comentamos[11], que por otra parte es muy casuístico. En España, probablemente, la resolución más relevante de la AEPD que analiza el concepto de decisiones automatizadas se refiere a un asunto transfronterizo que se cerró con una multa de 550.000 euros a la entidad GLOVOAPP23, S.A. (en adelante, GLOVOAPP). En este caso, se investigó la utilización de una aplicación que asignaba turnos y pedidos a los denominados *riders* de forma automatizada y era empleada por las distintas filiales de la sociedad sancionada en varios Estados miembros[12]. De hecho, las actuaciones se inician en Italia, con una inspección Foodinho SRL. por parte del *Garante per la Protezione dei Dati Personali*.

Uno de los aspectos que se analiza en la resolución, no el único, es si la aplicación implica la toma de decisiones automatizadas. GLOVOAPP defiende que no se cumplen los requisitos para ello, en síntesis, porque los criterios de asignación de turnos estaban decididos o acordados con intervención humana, limitándose la aplicación a llevar a cabo un proceso automatizado consistente en tres fases: (i) Aplicar una tabla de franjas horarias acordada por las partes; (ii) ejecutar una decisión adoptada por las partes; (iii) dar acceso a franja horaria según un orden establecido previamente en función de las preferencias de las partes.

Sin embargo, en opinión de la AEPD, la decisión automatizada existe, ya

> que es el sistema el que adoptaba la decisión sobre en qué orden se permitía acceder a unos repartidores determinados para la reserva de una franja horaria concreta, independientemente de que era GLOVOAPP como responsable de tratamiento quien introducía los parámetros necesarios en el Sistema para que pudiera adoptar tal

[11] Una completa revisión de las resoluciones recientes de autoridades de control puede encontrase en Future of Privacy Forum (2022). Igualmente, resulta interesante la lectura de Privacy Internacional (2017).

[12] Nos referimos al procedimiento sancionador con referencia PS/00209/2022, disponible en https://www.aepd.es/documento/ps-00209-2022.pdf. Este procedimiento fue objeto de recurso de reposición, pudiéndose consultar su resolución en: https://www.aepd.es/documento/reposicion-ps-00209-2022.pdf

Se imputan a la entidad sancionada las siguientes infracciones:

— Infracción del artículo 13 del RGPD, por la que se le apercibe.
— Infracción de los artículos 25 (privacidad desde el diseño y por defecto) y 32 (aplicación de medidas de seguridad) del RGPD, por las que se le impone la multa de 550.000 €.

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

> decisión. La decisión sobre el orden en que se permitía acceder a los repartidores a las franjas horarias era adoptada por la aplicación, sin intervención humana de ningún tipo. Únicamente se producía una intervención humana en aquellos casos en que los repartidores reclamaban, pero si no había reclamación, no había intervención humana que modificara dicha decisión ni supervisión alguna de tal decisión.

Más recientemente, hemos conocido la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 7 de diciembre de 2023, que es la primera en abordar centralmente el artículo 22, con un enfoque amplio y garantista que extiende el concepto de decisión automatizada hasta la actividad de una empresa que facilita información de solvencia o probabilidad de impago a terceros que son los que toman realmente la decisión que afecta al individuo[13].

Previendo que se dará una interpretación amplia a los conceptos de decisión automatiza y decisión completamente automatizada, será importante demostrar que o bien los efectos en los interesados no tienen consecuencias relevantes, o bien que se cumplen las excepciones ya comentadas del artículo 22.2.

Por ello, las recomendaciones a la hora de revisar estos tratamientos son (i) documentar y justificar la licitud del tratamiento y (ii) aplicar garantías adicionales suficientes.

4.3. *Garantías que deben adoptarse si se supera la prohibición del artículo 22 del RGPD*

Cuando existan decisiones automatizadas excluidas de la prohibición del artículo 22 deberán tomarse determinadas garantías, que incluyen, además del cumplimiento del resto de las obligaciones del Reglamento General de Protección de Datos, las siguientes:

— No utilizar categorías especiales de datos, salvo que se cuente con el consentimiento explícito del afectado (artículo 9.2.a del RGPD) o el tratamiento sea necesario por razón de un interés público esencial (artículo 9.2.g del RGPD).

— Informar a los afectos de forma expresa y específica de la lógica aplicada para tomar la decisión, así como de las consecuencias

[13] Para un análisis detallado puede consultarse Cotino (2024).

previstas e importancia de la mismas (según se recoge en los artículos 13 y 14 del RGPD)[14].

— Atender los derechos activos y directamente ejercitables frente al responsable del tratamiento que se recogen en el apartado 3 del propio artículo 22: derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión. En principio, parecen tres facultades que pueden ejercerse de forma diferenciada y en cuya tramitación deberán aplicarse las normas generales ya citadas que se incluyen en el artículo 12 del RGPD. Se limita la posibilidad de utilizarlos a los supuestos en los que las decisiones automatizadas se hayan basado en la existencia de un contrato o en el consentimiento explícito del afectado. En este punto, conviene advertir que, si su solicitud se generaliza, significará que los responsables del tratamiento deberán arbitrar procedimientos de revisión de las decisiones adoptadas a petición de los titulares de los datos.
— La realización de una evaluación de impacto sobre la protección de datos, como en el caso de otros tratamientos que entrañen un riesgo sustancial para los derechos y libertades de los afectados.

Conclusiones

La utilización de sistemas y modelos de IA de forma generalizada en las organizaciones hará más complejo el cumplimiento de las obligaciones derivadas de la normativa de protección de datos. La atención del ejercicio de derechos, que ha adquirido relevancia en los últimos años por su carácter casuístico, se enfrenta a problemas nuevos como la dificultad de localizar los datos personales del afectado, la mayor dependencia de proveedores tecnológicos muy especializados, o el propio desconocimiento de si realmente se tratan datos personales en algunas fases como el entrenamiento de sistemas de IA.

El mayor reto para los profesionales de la privacidad a corto plazo consiste en recibir una formación adecuada que permita comprender los tratamientos que se están llevando a cabo y las funcionalidades de los componentes de IA que aparecen en los mismos. Aquellos que

[14] Por lo que se refiere al ámbito laboral, el Ministerio de Trabajo y Economía Social publicó en 2022 una guía en la que se explicaba el derecho de los afectados a la recibir lo que se denomina "información algorítmica" tomando como punto de partida el artículo 22 del RGPD (Ministerio de Trabajo y Economía Social 2022).

Deusto Journal of Human Rights
ISSN: 2530-4275 • ISSN-e: 2603-6002, No. 14/2024, 313-339
https://doi.org/10.18543/djhr.3198 • http://djhr.revistas.deusto.es/

desempeñen funciones de delegados de protección de datos tendrán que intervenir de forma activa en la evaluación de los riesgos asociados a la utilización de sistemas y modelos de IA, y quizás se coordinen sus funciones con responsables de IA.

Las autoridades de protección de datos están publicando diversos documentos y guías para ayudar a las organizaciones en el cumplimiento de sus obligaciones. Esperamos que también se aprueben documentos aclaratorios del RIA en los próximos meses. Probablemente, también en un corto plazo veremos resoluciones y sentencias que dan forma al concepto de decisión automatizada. En este sentido, resulta relevante entender qué significa "sin intervención humana", es decir cuál es el grado de participación o revisión de una persona física que se requiere para que una decisión no sea totalmente automatizada.

El artículo 22 del RGPD y las obligaciones de transparencia sobre la lógica aplicada para tomar una decisión que prevén los artículos 13 y 14 de la misma norma resultan claves para asegurar el control de los interesados sobre sus datos personales. También lo es la posibilidad de conocer los datos personales tratados durante un proceso en el que intervienen componentes de IA.

Desde el punto de vista del individuo, las garantías establecidas por el RGPD son un complemento necesario que refuerza la protección que les otorga el RIA frente a sistemas y modelos de inteligencia artificial con efectos discriminatorios o impactos negativos en otros derechos y libertades.

Bibliografía

Agencia Española de Protección de Datos. 2016. *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Acceso el 10 de octubre de 2024: https://www.aepd.es/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

Agencia Española de Protección de Datos. 2020. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción.* Acceso el 10 de octubre de 2024: https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf

Agencia Española de Protección de Datos. 2023. «Inteligencia Artificial: Sistema vs. tratamiento, medios vs. Finalidad» (post de 10 de abril). Acceso el 10 de octubre de 2024: https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-sistema-vs-tratamiento-medio-vs-finalidad

Comité Europeo de Protección de Datos-Supervisor Europeo de Protección de Datos. 2021. *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). Acceso el 10 de octubre de 2024: https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_es.pdf

Comité Europeo de Protección de Datos. 2023. *Directrices 01/2022 sobre los derechos de los interesados - Derecho de acceso*. Acceso el 10 de octubre de 2024: https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_es.pdf

Comisión Europea. 2017. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital. Un mercado único digital conectado para todos.* Acceso el 10 de octubre de 2024: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0228

Comisión Europea. 2018. *Comunicación de la Comisión: Inteligencia artificial para Europa*. Acceso el 10 de octubre de 2024 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0237

Cotino, Lorenzo. 2024. «La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial». *Diario LA LEY* 80, *Sección Ciberderecho*. Acceso el 10 de octubre de 2024: https://diariolaley.laleynext.es/dll/2024/01/17/la-primera-sentencia-del-tribunal-de-justicia-de-la-union-europea-sobre-decisiones-automatizadas-y-sus-implicaciones-para-la-proteccion-de-datos-y-el-reglamento-de-inteligencia-artificial

DOUE. 2024. *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858), (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)*, n. 1689, de 12 de julio. Acceso el 10 de octubre de 2024: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079

Future of Privacy Forum. 2022. *Automated decision-making under the GDPR: Practical cases from courts and data protection authorities*. Acceso el 10 de octubre de 2024: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf

Grupo de Trabajo del Artículo 29. 2017. *Directrices sobre el derecho a la portabilidad de los datos*. Acceso el 10 de octubre de 2024: https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf

Grupo de Trabajo del Artículo 29. 2018. *Directrices WP 251, sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. Acceso el 10 de octubre de 2024: https://www.aepd.es/documento/wp251rev01-es.pdf

Herrán, Isabel. 2002. *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales.* Madrid: Dickinson.

Information Commissioner's Office. s.f. *How do we ensure individual rights in our AI systems?* Acceso el 10 de octubre de 2024: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/

Ministerio de Trabajo y Economía Social. 2022. *Información algorítmica en el ámbito laboral. Guía Práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral*. Acceso el 10 de octubre de 2024: https://www.mites.gob.es/ficheros/ministerio/inicio_destacados/Guia_Algoritmos_ES.pdf

Murillo de la Cueva, Pablo Lucas. 2007. «Perspectivas del derecho a la autodeterminación informativa». *IDP: Revista de Internet, derecho y política* 5: 18-32. Acceso el 10 de octubre de 2024: https://raco.cat/index.php/IDP/issue/view/6978

Parlamento Europeo. 2024. La Eurocámara aprueba una ley histórica para regular la inteligencia artificial. Notas de prensa. 13 de marzo. Acceso el 10 de octubre de 2024: https://www.europarl.europa.eu/news/es/press-room/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial

Personal Data Protection Commission Singapore. 2022. *Guía básica de anonimización*. Acceso el 10 de octubre de 2024: https://www.aepd.es/documento/guia-basica-anonimizacion.pdf

Privacy Internacional. 2017. *Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR.* Acceso el 10 de octubre de 2024: https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf