Cuadernos de RES PUBLICA en derecho y criminología
Nº en prensa ISSN: 2990-0697 DOI: 10.46661/respublica.12596

Luces y sombras en la realidad práctica del RGPD

Lights and shadows in the practical reality of the GDPR

Nicolás Dabrio Díaz
Investigador independiente. Sevilla. (España)
nicolasdabrio03@gmail.com
ORCID: 0009-0009-9290-8844

Resumen

El objetivo de esta obra será analizar la influencia del RGPD en la nueva era de la información, caracterizada por la creciente preocupación por la privacidad y la mercantilización de datos personales como herramienta de análisis de mercados. Para ello se estudiarán los aspectos fundamentales de la regulación, al igual que se analizarán una serie de casos prácticos seleccionados según criterios de relevancia, actualidad y amplitud de matices, tratando así de profundizar en las dimensiones de esta normativa. Esta materia se aborda motivada por una paradoja central: pese a que el RGPD se ha erigido como la normativa de referencia para la protección de los datos de los usuarios, estableciendo un nuevo marco legal para Estado, empresas y ciudadano, su utopía teórica sigue lejos de su aplicación práctica.

Palabras clave: RGPD; protección de datos; privacidad; biometría.

Abstract

The objective of this work will be to analyze the influence of the GDPR in the new information age, characterized by growing concerns over privacy and the commodification of personal data as a tool for market analysis. To this end, the fundamental aspects of the regulation will be studied, and a series of practical cases will be analyzed, selected based on criteria of relevance, timeliness, and breadth of nuance, thereby seeking to delve into the dimensions of this legislation. This subject is approached motivated by a central paradox: despite the GDPR having been established as the benchmark regulation for the protection of user data, creating a new legal framework for the state, companies, and citizens, its theoretical utopia remains far from its practical application.

Key words: GDPR; data protection; privacy, biometrics.

Cómo citar este trabajo: Dabrio Díaz, Nicolás. *(2026).* Luces y sombras en la realidad práctica del RGPD. *Cuadernos de RES PUBLICA en derecho y criminología, (en prensa), 01–15.* https://doi.org/10.46661/respublica.12596

Recepción: 04.09.2025 **Aceptación:** 22.12.2025 **Publicación:** 15.01.2026

1. Introducción

1.1. Breve historia de la protección de datos

Todo comenzó con la creciente preocupación por la privacidad y la protección de la información personal en un mundo cada vez más interconectado. En Europa, el primer paso significativo fue la Directiva 95/46/CE de 1995, que estableció las bases para la protección de datos personales en los Estados miembros de la Unión Europea. Esta directiva fue revolucionaria para su época, pero con el paso del tiempo y el avance tecnológico, se hizo evidente que necesitaba una profunda actualización.

El verdadero cambio llegó con el desarrollo del Reglamento General de Protección de Datos (RGPD), que entró en vigor el 25 de mayo de 2018. Este reglamento no fue simplemente una actualización de la normativa anterior, sino una transformación completa en la manera de entender y proteger los datos personales. El RGPD introdujo conceptos fundamentales como, por ejemplo, el principio de responsabilidad proactiva, que obliga a las organizaciones a implementar medidas técnicas y organizativas apropiadas para garantizar y demostrar el cumplimiento de la normativa.

1.2. Importancia del RGPD en la era digital

Un aspecto crucial del RGPD es su enfoque en la transparencia y el control del individuo sobre sus datos personales. El reglamento reconoce explícitamente el derecho de las personas a saber cómo se utilizan sus datos, a acceder a ellos, a rectificarlos e incluso a solicitar su eliminación. Esto se refleja en el artículo 17 del RGPD, que representa el derecho a la supresión o al olvido. Además de este, se reconocen otros derechos, como pueden ser el de la portabilidad de datos, para hacer más sencilla la transmisión entre diferentes proveedores de servicios, y el derecho a conocer cuándo ha existido una violación en la seguridad de los datos personales.

El RGPD también ha introducido cambios significativos en la manera en que las organizaciones deben abordar la protección de datos. Esto significa que la privacidad debe considerarse desde el inicio de cualquier proyecto o actividad que implique el tratamiento de datos personales.

La normativa ha tenido un impacto global, influyendo en legislaciones de protección de datos en todo el mundo. Muchos países han tomado el RGPD como modelo para desarrollar sus propias leyes de protección de datos, reconociendo la importancia de establecer estándares elevados en esta materia. Además, en materia empresarial es esencial no solo para aquellas empresas con sede en la UE, sino también para las localizadas fuera de ella, pero que presten servicios dentro de la Unión Europea, ya que estas también deberán acogerse a la normativa del RGPD.

En España, la adaptación del RGPD se materializó con la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que no solo implementa el reglamento europeo, sino que también añade aspectos específicos para el contexto español, como se refleja en el artículo 31 de la LOPDGDD, que establece las obligaciones relativas al registro de actividades de tratamiento.

2. Marco Teórico Normativo

2.1. Concepto de tratamiento de datos personales

El tratamiento de datos personales bajo el RGPD constituye un concepto amplio que abarca cualquier operación realizada con datos personales, requiriendo un enfoque sistemático y documentado que garantice el cumplimiento de los principios fundamentales de protección de datos y los derechos de los interesados.

Esta normativa establece un marco de responsabilidad proactiva que obliga a las organizaciones a implementar medidas

técnicas y organizativas para garantizar que el tratamiento es conforme a la regulación.

2.2. Principios fundamentales del RGPD

Licitud, lealtad y transparencia

El principio de licitud garantiza que el tratamiento de datos se haga bajo el amparo de la legitimidad legal, que al mismo tiempo representa la soberanía nacional y la voluntad popular.

El principio de lealtad por su lado, se encuentra directamente relacionado con el de transparencia y es que con ellos se promueve que los datos no sean tratados de forma fraudulenta y que, al mismo tiempo, la organización que trate los datos, debe proporcionar al usuario la información necesaria al usuario para que este sea consciente de las consecuencias y riesgos que tiene dicho tratamiento de datos.

Limitación de la finalidad

Esta limitación supone una doble obligación para las organizaciones, debido a que, por un lado, la finalidad o finalidades que tenga el tratamiento de datos deben ser determinadas, explícitas y legítimas. Por otro lado, una vez los datos ya hayan sido recogidos, estos no podrán ser utilizados de una forma incompatible con los fines ya establecidos. Sin embargo, sí será posible tratarlos siempre que sea en pro del interés público o de la investigación científica, con el aval de que se seudonimice estos datos para evitar que se pueda identificar al usuario.

Minimización de datos

Este principio se encuentra directamente relacionado con el anterior y es que su fundamento se encuentra en que los datos que traten las empresas deben ser estrictamente los necesarios y deben encontrarse limitados a la finalidad por la cual son tratados.

Exactitud

Los datos deben ser exactos y si fuera necesario actualizados. Por ello, la empresa que trate los datos debe ser diligente y actuar de tal forma que se puedan suprimir o modificar aquellos datos incorrectos.

Limitación del plazo de conservación

Este principio garantiza que los datos sean destruidos una vez se haya alcanzado la finalidad para la que fueron recogidos. Sin embargo, una vez que se haya conseguido esa finalidad, existe la posibilidad de que esos datos se conserven durante un tiempo mayor. De forma prudencial, los datos se podrán mantener para posibles reclamaciones o si el tratamiento de datos se realiza con fines históricos, científicos o estadísticos.

Integridad y confidencialidad

Estos principios garantizan que el tratamiento de datos sea realizado de manera segura.

Por un lado, de acuerdo a la integridad, los datos deberán ser exactos, completos y actualizados. Además, implica que los datos no sean alterados, destruidos o accedidos de manera no autorizada, todo ello para no perjudicar a su precisión o utilidad.

Por otro lado, de acuerdo a la confidencialidad, los datos solo podrán ser accedidos por aquellas personas que tengan una necesidad legítima y estén autorizadas. Garantizando así que los datos personales no sean accesibles para terceros no autorizados.

Responsabilidad proactiva

El principio de responsabilidad proactiva establece que las organizaciones que tratan datos personales deben asumir la responsabilidad de cumplir con el RGPD y ser capaces de demostrar que lo hacen. Esto implica que las empresas no pueden limitarse a cumplir pasivamente con las normas, sino que deben adoptar un enfoque proactivo y transparente en la gestión de los datos personales.

2.3. Derechos de los interesados

Acceso

Art. 15 RGPD. El derecho al acceso garantiza que los interesados puedan acceder a sus datos personales y a cómo están siendo tratados. Por ejemplo, solicitando a la

empresa encargada del tratamiento una copia de todos los datos personales que haya recogido.

Rectificación

Art. 16 RGPD. El interesado podrá solicitar que se corrijan o que se completen aquellos datos personales que sean inexactos o incompletos, garantizando así la integridad de los mismos. Un ejemplo de ello sería solicitar la rectificación sobre su dirección de correo electrónico que se encontrase expuesta en una plataforma.

Supresión (Derecho al Olvido)

Art. 17 RGPD. El afectado podrá solicitar la eliminación de sus datos personales en los siguientes supuestos:

- Los datos ya no son necesarios para el fin para los que fueron recogidos.
- Se retiró el consentimiento y no existía otra base legal para el tratamiento. Por ejemplo, deseo que se elimine mi cuenta de una red social y todos los datos vinculados a ella.
- Los datos han sido tratados o recogidos de manera ilícita.
- Los datos deben suprimirse para el cumplimiento de una obligación legal.

Limitación del tratamiento

Art. 18 RGPD. Este derecho consiste en que se podrá solicitar que se restrinja el tratamiento de datos. Va dirigido principalmente a limitar el tratamiento de la información cuando esta se vea envuelta en un proceso de reclamaciones o de impugnación de exactitud de los datos. Por ejemplo, ante una disputa de exactitud de la información de un historial de datos, se podría solicitar que se limitase el tratamiento hasta que se resolviese la disputa.

Portabilidad de los datos

Art. 20 RGPD. El interesado tiene derecho a recibir sus datos personales en un formato estructurado, de uso común y legible por máquina, y a transmitirlos a otro responsable del tratamiento sin obstáculos. Se realiza sobre todo ante medios automatizados y en tratamientos de datos con base contractual. En el caso de que quisiera cambiar de banco, podría solicitar sus datos al banco actual para que así le proporcionase sus datos financieros y poder transferirlos a otra entidad bancaria.

Oposición

Art. 21 RGPD. Este derecho consiste principalmente en la posibilidad de oponerse al tratamiento de sus datos en casos de marketing directo, como podría ser en el caso de que una empresa enviase publicidad no solicitada usando sus datos personales.

Derecho a no ser objeto de decisiones individuales automatizadas

Art. 22 RGPD. Garantiza que el interesado no sea objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos o le afecte significativamente. Excepto si esa decisión es necesaria para la celebración o ejecución de un contrato o cuando la decisión esté autorizada por ley y se establezcan medidas para proteger los derechos del interesado. Un ejemplo de ello, sería reclamar la denegación de un préstamo cuya decisión negativa se basó únicamente en un algoritmo automatizado sin intervención humana.

3. Análisis del RGPD

3.1. Ámbito de aplicación y sujetos obligados.

Ámbito de aplicación territorial y sujetos obligados

Debido a su idiosincrasia como normativa europea, el RGPD se aplica en los siguientes casos; para las organizaciones y sujetos establecidos en la UE y para las organizaciones de fuera de la UE en caso de que ofrezcan bienes y servicios a europeos y monitoreen su comportamiento, ya sea a través de las famosas cookies o de seguimiento en línea.

Ámbito de aplicación material:

El RGPD se aplica al procesamiento de datos personales. Esto incluye cualquier operación realizada con datos personales, ya sea

automatizada o manual. Abarcando tareas como la recopilación, almacenamiento, modificación, consulta o eliminación de datos.

3.2. Tratamiento de datos especiales

¿Qué son los datos especiales? Los datos especiales son categorías de datos personales que revelan información íntima sobre una persona. Según el Artículo 9 del RGPD, estos incluyen; datos médicos, biométricos, orígenes raciales, opiniones políticas, orientación sexual o creencias religiosas. Con respecto a los antecedentes penales, el RGPD les ha dedicado un artículo específico, el 10, otorgándoles un régimen más estricto.

¿Cómo se encuentran regulados en el RGPD? Debido al contenido sensible de estos datos, en un principio su tratamiento está prohibido, salvo que se cumpla alguna de las condiciones excepcionales del 9.2. Estas condiciones se pueden englobar en que el interesado debe dar un paso más en su consentimiento o que el tratamiento de datos atienda a razones médicas, de investigación o de protección del interés público esencial.

3.3. Transferencias internacionales de datos

La transferencia internacional de datos es un aspecto clave del RGPD. Se refiere a la transmisión de datos personales fuera del Espacio Económico Europeo (EEE).

Dado que el RGPD tiene como objetivo proteger los datos personales de los ciudadanos de la UE, las transferencias internacionales están sujetas a normas estrictas para garantizar que el nivel de protección de los datos no se vea comprometido. Por ello, establece que los datos personales solo pueden transferirse a países fuera del EEE si se garantiza un nivel adecuado de protección o si se aplican garantías adecuadas.

Un caso relevante en este ámbito fue el Schrems II del TJUE en 2020. Este caso invalidó el Escudo de Privacidad UE-EE.UU., un marco legal que permitía transferencias de datos a empresas estadounidenses que se adherían a ciertos principios de privacidad. Finalmente, el TJUE determinó que las leyes de vigilancia en Estados Unidos no ofrecían un nivel de protección equivalente al del RGPD y por ello, en la actualidad, las transferencias a EE.UU. deben tener garantías adicionales.

3.4. Seguridad de los datos

Respecto a la cuestión de cómo se encuentran protegidos, la respuesta variará dependiendo del tipo de dato. Sin embargo, todos los tratamientos de datos comparten, en mayor o menor cuantía, medidas como; cifrado de datos, control de acceso, copias de seguridad para evitar pérdidas y la implementación de firewalls o antivirus que sirvan como protección contra ciberataques.

Además, parafraseando a Cumbreras Amaro (2020), el RGPD no solo obliga a garantizar la seguridad de los datos, sino que, además, en caso de brecha de seguridad de los datos personales, se habrá de notificar de la misma a las autoridades de control y a los interesados.

3.5. Responsables y encargados del tratamiento

Tanto unos como otros representan a dos figuras clave que intervienen en el procesamiento de datos personales.

Por un lado, el responsable del tratamiento es la persona física o jurídica, autoridad pública, agencia u otro organismo que, de manera individual o conjunta, determina los fines y los medios del tratamiento de datos personales. Es decir, responde a las preguntas de por qué y cómo se tratan los datos.

Por otro lado, el encargado del tratamiento es la persona física o jurídica, autoridad pública, agencia u otro organismo que trata datos personales en nombre del responsable del tratamiento. Es decir, actúa bajo las instrucciones del responsable y no tiene autonomía para decidir sobre los fines del tratamiento.

La primordial entre ambas figuras es que su relación viene formalizada en un contrato basado en el art. 28.3 del RGPD. Este acuerdo

debe especificar extremos tales como: información del tratamiento, tipología de los datos, derechos y obligaciones recíprocas o las medidas de seguridad a implementar, entre otros.

4. El RGPD y su nuevo esquema normativo para las empresas

4.1. Adaptación a las nuevas normativas

Desde la entrada en vigor del RGPD el 24 de mayo de 2016 y su plena aplicación, el 25 de mayo de 2018, las empresas tuvieron un período de 2 años para que aquellos responsables y encargados de tratamientos de datos adecuasen sus procesos de acuerdo con el RGPD, adoptando las medidas necesarias para seguir así los principios, derechos y obligaciones de carácter novedoso que preveía esta normativa.

Siguiendo a Gadea Soler (2020), podemos afirmar que la nueva normativa formada por el RGPD y su desarrollo español, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), supuso para todas las empresas la obligación de realizar un análisis de riesgo de los tratamientos de datos previos al 25 de mayo de 2018. En caso de que los resultados de este análisis hicieran saltar las alarmas del riesgo, debía realizarse una Evaluación de Impacto en la Protección de Datos Personales o EIPD y adoptar las medidas que fuesen necesarias para cumplir con la normativa de protección de datos. Sin embargo, a pesar de que pareciera que esta evaluación podría perjudicar a los intereses de la empresa con sobrecostes inesperados, la doctrina opina totalmente lo contrario.

Autores como López Calvo (2017) y Puyol (2018) afirman que la EIPD representa una oportunidad para la empresa con el fin de reducir el riesgo del tratamiento de datos y ayudarle en la toma de decisiones relacionadas con el cumplimiento del RGPD, evitando así tanto costosos rediseños de los sistemas una vez han sido desarrollados, como posibles daños a la reputación y la imagen por un tratamiento inadecuado de los datos personales.

Por último, esta "herramienta" no es ajena a los tratamientos posteriores a la plena aplicación del RGPD, ya que hoy en día sigue indicada en casos donde, siguiendo el dictado del RGPD, sea probable que un tipo de 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. Por ello, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales que analice el riesgo.

4.2. El delegado de protección de datos

La figura del delegado de protección de datos, en adelante DPO por sus siglas en inglés (Data Protection Officer), resulta especialmente novedosa para España, pero no para su entorno europeo. Como ejemplifica Suárez Blavia, A., Maestre Salcedo, A. (2018) la regulación del DPO ya se encontraba en la Propuesta de Directiva del Parlamento Europeo y del Consejo 2012/0010 (COD), en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 e incluso en la normativa interna de EEMM como Alemania, con su "Comisionado Federal para la Protección de Datos", en alemán "Bundesbeauftragten für den Datenschutz", ya en 1977. Siendo en la Directiva 95/46/CE, la primera vez que se incluía en la normativa comunitaria, gracias en gran medida a la influencia alemana.

Para explicar esta figura es necesario desgranar el Considerando 97 del RGPD, en el que se explica que el responsable del tratamiento de datos, siguiendo esta normativa, requerirá de la ayuda de una persona con conocimientos especializados en Derecho y con práctica en materia de protección de datos si el tratamiento se realiza con las particularidades de los siguientes supuestos; los datos son tratados por una autoridad pública, a excepción de los

tribunales u otras autoridades judiciales en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consistan en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. Por todo ello, podemos definir al DPO como un profesional del Derecho y de la protección de datos, cuya función será supervisar y asesorar en estas materias y que será imprescindible para una organización si se dan las circunstancias anteriormente descritas.

Respecto a su regulación actual, esta se encuentra enmarcada en el art. 37 y ss. del RGPD y en el art. 34 de nuestra Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, teniendo en ambas una redacción prácticamente idéntica que recoge lo anteriormente explicado. Sin embargo, en nuestra normativa nacional se añaden, además, especificaciones para las Instituciones y entidades de nuestro ordenamiento jurídico.

5. Desafíos y tendencias

5.1. Inteligencia artificial y protección de datos

El reto que supone la inteligencia artificial para la protección de datos es más que evidente. Según la Comisión Europea, la inteligencia artificial ocupará la cúspide de su política de investigación en la próxima década, por ello es necesario prestar especial atención a la protección de datos de carácter personal. Como explica Herrera de las Heras (2022), "como cualquier revolución científica, los avances en esta materia comportan mejoras, pero también riesgos e incertidumbres que han de ser tenidos en cuenta de cara a evitar mayores problemas".

La base del desarrollo y el avance de la inteligencia artificial se encuentra en el machine learning, esto es, curiosamente el aprendizaje más humano posible, el famoso prueba y error. Gracias a las interacciones que vaya teniendo con los usuarios, las respuestas serán cada vez más humanas y precisas. Como afirma Fernández Hernández (2020), "la disponibilidad de datos es esencial para el desarrollo de unos sistemas de inteligencia artificial que están evolucionando rápidamente de la capacidad de reconocimiento de patrones y la generación de conocimientos al desarrollo de técnicas sofisticadas de predicción". Por ello, cabe afirmar que el avance de la inteligencia artificial gracias a estas técnicas representa un riesgo para la protección de datos, debido al uso de los mismos para el desarrollo de esta tecnología.

Ante esta situación, la Unión Europea y su legislación aspiran a defender los derechos fundamentales, no desde una perspectiva que frene el avance, sino desde una en la que la protección de datos represente uno de los objetivos del desarrollo de la tecnología.

Concretamente, nuestra materia central de estudio, el RGPD, no se pronuncia sobre la IA, aunque sí alude de forma garantista de la protección de datos a una de sus principales funciones, las decisiones individuales automatizadas, en sus artículos 21 y 22. Frente a estas circunstancias, el Parlamento Europeo también se pronunció en su Recomendación a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas. Manifestando que "el uso de datos, incluidos los datos personales como los datos biométricos, resultantes del desarrollo, despliegue y utilización de la inteligencia artificial, la robótica y las tecnologías conexas están aumentando rápidamente, lo que pone de relieve la necesidad de respetar y hacer cumplir los derechos de los ciudadanos a la intimidad y la protección de los datos personales de conformidad con el derecho de la Unión".

En definitiva, y siguiendo la normativa europea, la inteligencia artificial deberá,

desde el diseño, ser garante de que su aplicación es compatible con la protección de datos.

5.2. Big data y privacidad

El Big Data es un término que describe el gran volumen de datos, tanto estructurados como no estructurados, que inundan los procesamientos de datos cada día.

Las características de sus datos se encuentran en sus 5 V (volumen, velocidad, variedad, veracidad y valor).

- Volumen: Cantidad masiva de datos generados (ej: redes sociales, transacciones).
- Velocidad: Los datos se generan y deben procesarse en tiempo real o casi real (ej: transacciones bancarias).
- Variedad: Diversidad de formatos (estructurados, no estructurados como imágenes, videos, textos).
- Veracidad: Calidad y confiabilidad de los datos.
- Valor: Contienen información útil para la toma de decisiones.

La principal cuestión con el Big Data se encuentra en que este se puede analizar para obtener ideas que conduzcan a mejores decisiones empresariales. Sin embargo, la relación entre Big Data y el RGPD es crucial, ya que el procesamiento de grandes volúmenes de datos personales debe cumplir con estrictas normas de privacidad y seguridad. Algunas de estas normas son las explicadas anteriormente, como pueden ser la limitación de la finalidad, la transparencia, o la limitación temporal de conservación de datos.

Siguiendo a Martínez Devia (2019) y vinculándolo con el punto anterior, "dentro del gran conjunto de datos que se recogen mediante la técnica del big data o macrodatos se están recolectando datos de carácter personal. Lo anterior crea un riesgo para el titular si no se hace un tratamiento responsable, ético y transparente que proteja sus derechos y libertades".

Sin embargo, aunque, el RGPD no se ha quedado impasible ante el Big Data, podría criticarse la tendencia de establecer marcos conductuales y declaraciones de intenciones más que medidas concretas ante esta materia, recalcándose en definitiva la necesidad de reforzar la seguridad jurídica para que las personas tengan el control sobre sus propios datos personales.

5.3. El papel de las autoridades de control

En el contexto del RGPD, las autoridades de control representan los organismos públicos independientes encargados de supervisar el cumplimiento de la normativa de protección de datos, asesorar a empresas y ciudadanos, investigar infracciones y, en su caso, imponer sanciones. Cada país de la Unión Europea (UE) tiene su propia autoridad, y trabajan de forma coordinada a través del Comité Europeo de Protección de Datos (CEPD), creado tras el RGPD, actuando conjuntamente con el Supervisor Europeo de Protección de datos (SEPD), de creación anterior.

En España, la autoridad de control más representativa es la Agencia Española de Protección de Datos (AEPD), y cada país tiene su propia autoridad de control, con algunas particularidades. Así ocurre en el caso de Alemania, en el que, al ser un Estado federal, cada Länder tiene su propia autoridad, denominado BfDi por sus siglas en alemán.

Esta posibilidad de multiplicidad de autoridades de control se encuentra explicada por Rodríguez Ayuso (2020); "el considerando 117 RGPD establece que los Estados miembros deberán contar con la opción de disponer de más de una autoridad de control, con el objetivo de plasmar su estructura constitucional, organizativa y administrativa. De este modo, se procura respetar la configuración constitucional de cada país, configuración que podrá atender a un modelo de Estado más o menos centralizado, dando lugar, en su caso, al surgimiento de entidades territoriales subordinadas o de Comunidades Autónomas que asuman tales competencias.

En el supuesto de que exista más de una autoridad de control en un mismo país (en España, la AEPD y las AAPD), será este el que deberá establecer cuál de dichas autoridades habrá de representar a todas ellas ante el CEPD (en nuestro país, esta función se encomienda a la AEPD en virtud del artículo 44.2 LOPDGDD), debiendo cumplir todas las autoridades subnacionales la normativa relativa al mecanismo de coherencia, garantizando una cooperación rápida y fluida con otras autoridades de control, el CEPD y la Comisión (artículo 51.3 y considerando 119, ambos del RGPD)."

El mayor reto se encuentra en que en nuestro mundo globalizado, los datos no son asunto de un solo país, por lo que surgen conflictos con respecto a qué autoridad concreta debe liderar cada investigación y respecto a los criterios de interpretación del RGPD. Ante esta problemática sí existe una solución mucho más clara que para los desafíos anteriores y es que, gracias al CEPD, existe un órgano que, por un lado, resuelve los conflictos entre las distintas Autoridades de Protección de Datos y por otro emite directrices interpretativas.

Poniendo un ejemplo práctico. Si Facebook procesa datos de usuarios españoles de forma ilegítima, la AEPD podría investigar y sancionar, pero coordinaría con la autoridad irlandesa (DPC, Data Protection Commission), ya que la sede europea de Meta está en Irlanda y todas estas acciones se harían bajo el amparo de la supervisión de la CEPD y de sus directrices.

6. Análisis de casos reales

6.1. Uniqlo y la responsabilidad ante brechas de seguridad

En el pasado año 2022, una trabajadora de Uniqlo, al terminar su contrato laboral, solicitó su nómina y recibió como respuesta, por parte de la empresa, un documento en el que se incluía su nómina y la de 446 trabajadores más. Este error humano supuso que datos personales de especial sensibilidad, como son el número de la Seguridad Social, el DNI o el número de la cuenta bancaria, de un gran número de trabajadores fueran desvelados.

Esta brecha de seguridad, respecto a la confidencialidad de la información, violó el Reglamento General de Protección de Datos (RGPD), al no garantizar medidas adecuadas para proteger los datos personales. Aunque fue fruto de un error humano, la empresa no tuvo conocimiento de esta filtración de datos hasta que fue comunicada por la propia AEPD, ya que la responsable de recursos humanos no lo puso en conocimiento de la empresa

Por todo ello, la responsabilidad era compartida tanto por la persona que cometió el error como por la empresa, debido a que esta falla de seguridad evidenció que las medidas de seguridad tomadas por la empresa respecto al tratamiento de datos no eran las adecuadas para garantizar la seguridad y confidencialidad de los datos personales en el momento de producirse la quiebra, como explicaba la AEPD.

La sanción inicial impuesta era de 450.000 euros, por infracción de la necesaria seguridad de los datos, del artículo 5.1 y 32 del RGPD, pero se redujo un 20 % al reconocer la empresa parte de la responsabilidad en la brecha de seguridad y otro 20 % debido al pago voluntario de la sanción.

En conclusión, este caso demuestra la ineludible obligación de las empresas de implantar estrictos protocolos de seguridad y de capacitar correctamente al personal que tiene que tratar con estos datos sensibles, ya que brechas de seguridad como la de este caso no solo dañan la privacidad de los trabajadores, sino que además pueden acarrear duras sanciones y un detrimento en la imagen corporativa.

6.2. CaixaBank y los principios de transparencia y licitud

Por otro lado, a CaixaBank se le impuso una sanción de 6 millones de euros al evidenciar el incumplimiento del principio de transparencia establecido en los artículos 13 y 14 del RGPD, así como el principio de licitud del tratamiento regulado en el artículo 6 del RGPD, con

respecto al contrato marco de CaixaBank que debían firmar los clientes de la entidad.

En este caso, se detectaron incumplimientos en dos aspectos clave del RGPD; en primer lugar, se infringió el principio de transparencia, artículos 13 y 14. Y en segundo lugar, se incumplió con la licitud del tratamiento de datos, artículo 6.

Respecto al principio de transparencia, la AEPD consideró que esta empresa no informaba de manera clara y sistemática sobre los tratamientos de datos personales ni las finalidades para las que eran utilizados. Por ello, los clientes no recibían con claridad las finalidades por las que sus datos iban a ser tratados, al usar expresiones como: "personalizar su experiencia comercial en nuestros canales", "estudiar productos o servicios que puedan ser ajustados a su perfil y situación comercial o crediticia", "definir o mejorar las experiencias de los usuarios"... Además, para un mismo tratamiento, en ciertas ocasiones se legitimaba su uso en el interés legítimo y en otras en el consentimiento expreso, resultando en una zona gris que permitiría que un tratamiento no consentido se terminase realizando justificándose en el interés legítimo.

En relación con el principio de licitud, CaixaBank recababa en un único consentimiento el envío de comunicaciones comerciales y la cesión de datos a esta entidad y a cualquiera de las empresas de su grupo. El resultante de esto es un consentimiento que no es específico, incumpliendo, de esta forma, los requisitos de legalidad del consentimiento. El RGPD, por su parte, exige consentimiento separado por cada finalidad y entidad, no uno genérico que imposibilite conocer cuáles son las empresas a las cuales se ceden los datos.

Por último, estas cláusulas, al encontrarse en un contrato de adhesión, eran impuestas obligatoriamente al interesado, sin tener éste posibilidad de negociar los términos y condiciones. Al imponerse obligatoriamente la cesión de datos personales a CaixaBank y a las entidades de su grupo, se vulneraba el consentimiento, que el RGPD exige que sea libre, es decir, que el cliente pueda aceptar o rechazar sin perjuicio.

En este caso, una vez más se demuestra la preocupación de los legisladores europeos por proteger al consumidor frente a las grandes empresas, que aprovechándose de su posición y de la ignorancia y la heteronomía de sus usuarios, son capaces de exponer a sus redes empresariales los datos personales de sus clientes.

6.3. WorldCoin y los escaneos de iris

Cualquier español se sorprendió el pasado año 2023, cuando al pasear por un centro comercial se encontraba largas colas ante puestos que parecían de lo más inofensivos, en los que al hacerte una foto al ojo, se te entregaba una cantidad de dinero en forma de criptomoneda. Lo que muchos incautos no tenían en cuenta es que de esta forma estaban cediendo los datos biométricos de su iris de forma totalmente ingenua.

Esta situación no pasó desapercibida para las distintas autoridades de control, desde la AEPD española a la BayLDA de Baviera, Alemania. Las circunstancias no eran para menos, ya que esta recogida de datos extremadamente sensibles, como son los biométricos, y su recogida masiva estaban infringiendo en gran medida el RGPD.

En este caso, se detectaron numerosos incumplimientos de la normativa del RGPD, conclusión a la que llegaron tanto la AEPD como la BayLDA, en un pronunciamiento posterior.

En primer lugar, se vulneró el artículo 5 (Principios de licitud, transparencia y minimización de datos). Por un lado, WorldCoin no informó claramente a los usuarios sobre el uso real de sus datos del iris de una forma clara y accesible. Todo ello ocurría mientras el consentimiento se encontraba incentivado, al estar vinculado a una recompensa económica, incitando a personas vulnerables y de escasos recursos económicos a aceptar sin pensar en las consecuencias. Por otro lado, la finalidad, artículo 5.1.b, era de forma explícita "verificar

la humanidad". Siendo la recogida masiva de iris un profundo exceso de los fines establecidos.

Respecto a la licitud del tratamiento, artículo 6, también se encuentra infringido. Esto se debe a que el consentimiento se encontraría viciado, de acuerdo con el artículo 7.3 y es que era imposible revocarlo una vez otorgado.

Además, la información que trataba, como es la del iris de un ojo, pertenece a la categoría de los datos biométricos, los cuales son inmutables. Como se explicaba anteriormente, estos necesitan de circunstancias excepcionales para tratarlos y WorldCoin no demostró una base legal para hacerlo, artículo 9.

También se incumplía con el principio de transparencia de la información, del artículo 12. Una total opacidad de la información provocó que los usuarios no recibieran detalles claros sobre cómo, dónde y por cuánto tiempo se almacenarían sus datos.

Y por último, hubo una total inobservancia del artículo 25, la protección de datos desde el diseño y por defecto. La empresa no implementó medidas técnicas ni organizativas que garantizasen la seguridad de los datos, el seguimiento del RGPD y los derechos de los usuarios.

Ante esta retahíla de incumplimientos y las múltiples denuncias, la AEPD actuó de urgencia, basándose en el artículo 66 del RGPD y los poderes que le confería el artículo 58, para así ordenar cautelarmente el cese en la recogida y el tratamiento de datos personales que la compañía estaba llevando a cabo en España, así como el bloqueo de los que ya se habían recopilado.

Posteriormente, el 19 de diciembre de 2024, la BayLDA, autoridad de protección de datos del país donde la empresa tiene su establecimiento principal en Europa, adoptó una resolución que declaraba la infracción por parte de la empresa responsable del proyecto Worldcoin de varios artículos del RGPD y le instaba a implantar medidas correctivas, ratificando así la medida cautelar de la AEPD.

En esta última resolución, la BayLDA ordenó la eliminación de todos los códigos de iris almacenados desde el inicio del proyecto y la adopción de medidas para futuros tratamientos de iris, como un consentimiento explícito del interesado o el derecho a la supresión de los datos. Además, se constató que la empresa no implantó las medidas adecuadas para impedir el tratamiento de datos de menores.

Este caso representa todo un precedente, por el cual la AEPD y la BayLDA han establecido que la biometría masiva con fines comerciales, más aún en estas circunstancias, no es compatible con el RGPD.

7. Conclusiones

Tras la sociedad industrial, podría afirmarse que hoy en día nos encontramos en la sociedad de la información, en la que el conocimiento se usa como moneda de cambio en todos los ámbitos. Por ello, las grandes corporaciones se han ido adaptando a estas nuevas circunstancias, invirtiendo cada vez más para conseguir esta información, llegando al punto de aprovecharse de su situación de superioridad para conseguir estos datos de sus usuarios. Esto ha derivado en una compleja coyuntura socioeconómica en el plano de la protección de datos, donde los conflictos entre los derechos digitales de los usuarios, la veloz evolución de la tecnología y los intereses económicos de las corporaciones se encuentran entrelazados. Ante esta relación de desigualdad y de permanente mutación, la propia UE decidió crear un marco normativo, en el que se encuadra el RGPD, en el que se otorgasen unos derechos a sus ciudadanos con respecto a sus datos y privacidad, para así equilibrar la balanza.

Gracias a este estudio, me gustaría destacar varias conclusiones:

1. Ya sea desde una postura proactiva, con normativa que asegure la protección de los datos desde el diseño o desde una reactiva, con derechos como al olvido, el RGPD trata de proteger la seguridad de la información de sus ciudadanos, con más ahínco aún si

esta se denomina especialmente sensible, diferenciándose así como una normativa preventiva y no una punitiva.

2. A pesar de ser una de las normativas más alabadas, sirviendo como referencia para países ajenos a la UE, el RGPD no está exento de críticas. Una de las más importantes es que, al igual que otras normativas europeas, genera una desigualdad entre grandes corporaciones y PYME, sobre todo en los países con menor poder adquisitivo en la UE. Desde mi punto de vista, esto es debido a que los legisladores europeos pecan en exceso de ser influenciados por las potencias económicas centroeuropeas como Alemania, donde la coyuntura económica es mucho más favorecedora que por ejemplo en Italia, Portugal o España. Por un lado, existen dificultades técnicas y económicas, lo que dejaría a estas pequeñas y medianas empresas desprotegidas frente a incumplimientos o a la implementación de soluciones inadecuadas.

   Por otro lado, aunque es cierto que el desconocimiento no exime de su cumplimiento, tanto el RGPD como la LOPDGDD, siguen siendo un nuevo mundo para muchas de estas empresas, ya sea por falta de formación específica o por la constante actualización de la normativa. Sin embargo, también hay que destacar los intentos de la AEPD de solucionar esta problemática, publicando guías interpretativas y poniendo a disposición herramientas informáticas para PYME y autónomos con perfiles de bajo riesgo, con el fin de facilitarles el cumplimiento de sus obligaciones en materia de protección de datos.

3. A propósito del anterior párrafo, es necesario destacar la importancia de una educación que ayude a concienciar tanto a la población como a las empresas. Sigue habiendo una gran desinformación al respecto, clara muestra de ello fue el caso de Worldcoin, explicado anteriormente, donde los usuarios, en su gran mayoría, tomaron decisiones sumamente importantes de forma imprudente debido al desconocimiento. Por lo tanto, es fundamental que todos los actores sociales cooperen en tratar de educar a la población respecto a sus derechos sociales y a cómo gestionar sus datos personales.

4. Si bien, tanto el RGPD como la LOPDGDD, ofrecen un marco normativo amplio y acertado, siguen existiendo dificultades respecto a su aplicación práctica. Como afirma Garay Velasco (2024), estos desafíos derivan de la falta de claridad de determinadas disposiciones, la dificultad para adaptarse a tecnologías nuevas y la variabilidad de aplicación por parte de diferentes autoridades nacionales.

5. Por último, pero no por ello menos importante, me gustaría destacar un hecho, el cual puede simbolizar un peligroso precedente para la población. Se trata del consentimiento a ceder información biométrica a cambio de una recompensa económica. No poner un cordón sanitario a actuaciones así y dejarlas pasar bajo el radar, implica una aceptación tácita de la mercantilización del cuerpo humano. La proliferación de la prostitución, de la gestación subrogada o de la venta de órganos ya representan, de por sí, una amenaza contra la integridad física y moral de la población. Aunque puedan obtenerse por medios menos invasivos, los datos biométricos son irrepetibles e inalterables y conforman la identidad única de la persona. Por lo que el Estado debe intervenir y no permitir que haya quienes se aprovechen más aún de situaciones de vulnerabilidad para comercializar con el cuerpo humano.

Referencias

Fuentes académicas o doctrinales.

AEPD. (2024, 19 diciembre). “Worldcoin tendrá que eliminar todos los códigos de iris almacenados desde el inicio del proyecto”. AEPD. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/worldcoin-

tendra-que-eliminar-todos-los-codigos-de-iris.

Adaptalia. (2022, 9 junio). "Principios de la protección de datos". Grupo Adaptalia Empresa de Protección de Datos. https://grupoadaptalia.es/blog/principios-de-la-proteccion-de-datos/

Adminrevista. (2019, 7 junio). "Principios de protección de datos en el RGPD". EnRed@2.0. https://ws168.juntadeandalucia.es/iaap/revista/2019/06/07/principios-de-proteccion-de-datos-en-el-rgpd/

ADSUARA VARELA, Francisco de Borja. (2019). "El ciudadano ante el RGPD y la nueva LOPDGDD", Dialnet.

BALLESTEROS MOFFA, Luis Ángel. (2020). "Las fronteras de la privacidad: el conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica", Comares.

BOLÍVAR OÑORO, María del Val. (2019). "Protección de Datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)", en *Revista de Derecho UNED*, 26, págs. 621–626. https://doi.org/10.5944/rduned.26.2020.29207

CAZURRO BARAHONA, Víctor. (2020). "Antecedentes y fundamentos del derecho a la protección de datos", JM Bosch Editor. https://doi.org/10.2307/j.ctv14t46sm

Comisión Europea (2018), Coordinated Plan on the development and use of Artificial Intelligence Made in Europe.

CUMBRERAS AMARO, Maria. (2020). "La seguridad de los datos personales y la obligación de notificar las brechas de seguridad", en *Revista de Derecho, Empresa Y Sociedad. (REDS)*, ISSN 2340-4647, nº 16, 2020, págs. 151-162.

DELGADO MORÁN, Juan. José,. y GINER ALEGRÍA, Cesar. Augusto. (2017). La protección de datos de carácter personal en el ordenamiento jurídico español. Sociedad, empresas e instituciones: una aproximación desde la economía y la historia". Ed. Sotezca. Pp. 347-365

DOÑATE MAZCUÑAN, Félix (2024, 25 febrero). "Escanearte el iris a cambio de criptomonedas: Worldcoin, el nuevo y cuestionado negocio del creador de ChatGPT". RTVE.es. https://www.rtve.es/noticias/20240225/asi-es-worldcoin-escaneo-iris-criptomonedas-negocio-chatgpt/15982136.shtml

FERNÁNDEZ HERNÁNDEZ, Carlos. (2020). "La nueva estrategia europea sobre el dato y la inteligencia artificial. Foto fija de un diseño en evolución", en *Derecho digital e innovación*, nº 5, 2020.

GADEA SOLER, Enrique. (2020). "Análisis de riesgos y evaluación de impacto relativa a la protección de datos: su aplicación a las sociedades cooperativas", en *Boletín de La Asociación Internacional de Derecho Cooperativo,* pág. 56. https://doi.org/10.18543/baidc-56-2020pp47-72

GAREA, Eva. (2024, 10 abril). "El caso de Worldcoin y los escaneos de iris". Blog Protección Datos I Conversia. https://protecciondatos.conversia.es/escaneo-iris-worldcoin/

GAREA, Eva. (2024, 12 noviembre). "Multa a Uniqlo por enviar por error un PDF con las nóminas de 447 empleados". Blog Protección Datos I Conversia. https://protecciondatos.conversia.es/multa-a-uniqlo-por-enviar-por-error-un-pdf-con-las-nominas-de-447-empleados/

GONZÁLEZ PASCUAL, Manuel. (2024, 19 diciembre). "Worldcoin deberá eliminar todos los registros de iris almacenados en España". El País. https://doi.org/10.53766/PROHIS/2023.44.02

Grupo Atico34. (2025, 28 enero). "Delegado de Protección de Datos (DPO) definición, funciones y requisitos". Grupo Atico34. https://protecciondatos-lopd.com/empresas/delegado-proteccion-datos-dpo/.

GUASP MARTÍNEZ, Virginia, LÓPEZ CALVO, José, LESMES SERRANO,

Carlos. (2019). "La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD", Wolters Kluwer España: Bosch.

HERRERA DE LAS HERAS, Ramón. (2022). "Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil", Dykinson. https://doi.org/10.2307/j.ctv2gz3t4t

TAWALBEH, Lo'ai A, & SALDAMLI, Gokay. (2021). "Reconsidering big data security and privacy in cloud and mobile cloud systems", en *Journal of King Saud University: Computer and Information Sciences,* 33(7),págs. 810–819. https://doi.org/10.1016/j.jksuci.2019.05.007

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE-A-2018-16673. https://boe.es/buscar/act.php?id=BOE-A-2018-16673a1-3.

LÓPEZ CALVO, José. (2017). "Comentarios al Reglamento Europeo de protección de Datos", Editorial Sepín

LÓPEZ CALVO, José. (2018). "La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD", Wolters Kluwer.

LÓPEZ-VIDRIERO TEJEDOR, y Iciar, SANTOS PASCUAL, Efrén. (2018). "RGPD y su afectación práctica: nuevo escenario-nuevas prácticas", Fundación Confemetal.

MARTÍNEZ MARTÍNEZ, Ricard. "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", en *Revista Catalana de Dret Públic,* nº 58, 2019, pág. 73.

MARTÍNEZ, Laura. (2023, 20 diciembre). "Sanciones RGPD recientes: Comentarios y ejemplos". GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/sanciones-rgpd-recientes/.

MATURO SERNA, Amedeo. (2019). "Inteligencia artificial y privacidad: un encaje problemático", en *La Ley*, nº 2, 2019, págs. 2 y 3.

MAYER-SCHONBERGER, Viktor, CUKIER, Kenneth. (2013). "Big data: la revolución de los datos masivos", Turner.

NIETO MARTÍN, Adán. (2015). "El cumplimiento normativo", en *Manual de cumplimiento penal en la empresa*, págs. 25-48, Editorial Tirant Lo Blanch. https://doi.org/10.36151/TLB_9788490863268

ORTEGO RUIZ, Miguel. (2018). "Sin miedo a la protección de datos: el Reglamento General de Protección de Datos fácil", Siglo XXII legal.

Parlamento Europeo. (2017). Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica.

Parlamento Europeo (2020). Recomendación del Parlamento Europeo a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 20 de octubre de 2020, recomendación núm. 63.

PÉREZ RODRÍGUEZ, María Dolores. (2018). "Nuevo Reglamento Europeo de Proteccion de Datos (RGPD)", ICB Editores.

PUYOL MONTERO, Javier. (2018). "El modelo de evaluación de riesgos en la protección de datos EIPD /PIA's", Tirant lo Blanch.

RAMÍREZ DE MATOS, Emilio, COBOS TUBILLA, Jesús. (2018). protección de datos: aplicación del RGPD, Ediciones Francis Lefebvre.

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 ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *Diario Oficial de las Comunidades Europeas,* 4.

RODRÍGUEZ AYUSO, Juan Francisco. (2020). "Control externo de los obligados por el tratamiento de datos personales",

Bosch Editor. https://doi.org/10.2307/j.ctv14t46qk

RODRÍGUEZ AYUSO, Juan Francisco. (2019). "Figuras y responsabilidades en el tratamiento de datos personales", Siglo del Hombre Editores. https://doi.org/10.2307/j.ctvwcjghh

RODRÍGUEZ, Gladys Stella. (2020). "Privacidad y seguridad en la nube: algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo", en *Revista de La Facultad de Derecho Y Ciencia Política de La Universidad Alas Peruanas*, ISSN 1991-1734, Vol. 18, Nº. 25, 2020, Págs.. 329-358. https://doi.org/10.21503/lex.v18i25.2109

SIMÓN CASTELLANO, Pere, BACARIA MARTRUS, Jordi. (2020). "Las funciones del delegado de protección de datos en los distintos sectores de actividad", Bosch.

SUÁREZ BLAVIA, Ana, MAESTRE SALCEDO, Andrés. (2018). "El delegado de protección de datos", Editorial La Jurídica.

SUN, Pan Jun. (2020). "Research on the Optimization Management of Cloud Privacy Strategy Based on Evolution Game", en *Security and Communication Networks*. https://doi.org/10.1155/2020/6515328

VÁZQUEZ, Sonia. (2017). "Las brechas de seguridad en el RGPD": Actualidad jurídica Aranzadi, Nº 936, 2017, págs. 11-11.

VIGURI CORDERO, Jorge Agustín. (2023). "La implementación del reglamento general de Protección de Datos en España y el impacto de sus cláusulas abiertas", Tirant lo Blanch.

VILLALBA CANO, Laura., TRONCOSO REIGADA, Antonio. (2024). "El contenido esencial del derecho fundamental a la protección de datos personales en Europa: análisis en perspectiva multinivel", Aranzadi.