Universidad Internacional de La Rioja
Facultad de Derecho

Grado en Derecho

Protección de Datos en España: Análisis del Marco Regulatorio y sus implicaciones prácticas

Trabajo fin de estudio presentado por:	Katalina Hernández Delgado
Tipo de trabajo:	TFG Individual
Director/a:	Alberto Campos Jiménez
Fecha:	19 de febrero de 2024

Resumen

Este Trabajo de Fin de Grado analiza de manera exhaustiva el marco legal y regulatorio de la protección de datos en España, abarcando desde la Ley Orgánica de Protección de Datos Personales hasta normativas específicas como la Ley Orgánica 13/2015 y la Ley 07/2021. Se destaca la complejidad del entorno regulatorio, enfatizando la armonización de principios como la licitud, proporcionalidad y minimización de datos. El estudio revela una disparidad en la aplicación de estas leyes entre los sectores público y privado, con una mayor rigurosidad y sanciones en el ámbito privado. Se examina la actuación de la Agencia Española de Protección de Datos (AEPD), resaltando los desafíos de equilibrar seguridad y privacidad. El análisis concluye con la necesidad de una regulación más equitativa y coherente para fortalecer la protección de datos en la era digital.

Palabras clave: (De 3 a 5 palabras)

1. RGPD
2. Seguridad
3. Videovigilancia
4. Privacidad
5. AEPD

Índice de contenidos

1. Introducción

1.1. Justificación del tema elegido

La era digital intensifica la necesidad de proteger la privacidad y los datos personales en España, donde el Estado y las empresas recopilan y analizan datos masivos, equilibrando la seguridad pública con los derechos individuales.

1.2. Problema y finalidad del trabajo

Este Trabajo de Fin de Grado investiga cómo el marco legal español equilibra la privacidad individual con las demandas de seguridad y vigilancia del Estado y el tratamiento de datos personales por las empresas, cuestionando el alcance del acceso a los datos personales sin legitimación: tanto en el ámbito público como en el privado.

1.3. Objetivos

Se analizará la legislación sobre la protección de datos y la privacidad, sentando los principios de la LOPDGDD y el RGPD como pilares fundamentales. Se examinará el entramado legal-regulatorio con énfasis en la protección de datos para la seguridad ciudadana y sobre la videovigilancia. Se comparará la aplicación práctica de los principios legales examinados en el ámbito laboral con la gubernamental, utilizando para ello resoluciones de la Agencia Española de Protección de datos en los ámbitos público y privado. Finalmente, se destacarán las mejores prácticas regulatorias y futuras tendencias en la regulación de la protección de datos a nivel nacional y europeo.

2. Marco legal-regulatorio y desarrollo

En el contexto español de 2023, la cuestión de la protección de datos en el dominio tecnológico ha trascendido de ser una mera noción técnica para convertirse en un tópico de urgente relevancia sociopolítica. La temática ha impregnado los debates públicos y se ha arraigado en la conciencia colectiva, extendiendo su inquietud desde los hogares, como ilustra el caso de Almendralejo[1] donde datos personales de menores se utilizaron de manera deshonrosa para su dignidad (VIGARIO 2023), hasta el ámbito corporativo donde empresas ven una ventaja competitiva en garantizar la privacidad de datos (DÍEZ ESTELLA 2022). La persona común, ahora más que nunca, dedica atención a elementos antes obviados, tales como banners de cookies o términos y condiciones de uso. Es notable que incluso plataformas de entretenimiento, como Netflix, utilizan sus narrativas para alertarnos de la importancia de estos 'tediosos' documentos, como se reflejó recientemente en la serie *Black Mirror* en 'Joan es horrible'[2]. Si bien es cierto que el discurso predominante en medios y literatura tiende a centrarse en el aprovechamiento comercial de los datos personales y en los riesgos asociados a la inteligencia artificial mal regulada, persiste un vacío informativo sobre los procedimientos requeridos para que una entidad, ya sea pública o privada, procese datos personales de forma lícita. Por ello, es esencial desentrañar y analizar minuciosamente el marco regulador existente en España relacionado con la protección de datos y la seguridad ciudadana.

2.1. Las bases la Protección de Datos en España

En el marco jurídico español, el derecho a la privacidad se consagra como una prerrogativa fundamental en el artículo 18 de la Constitución[3], el cual protege el derecho al honor, a la intimidad personal y familiar, y a la propia imagen. No obstante, como se ha visto anteriormente, la salvaguarda efectiva de este derecho se encuentra con numerosos desafíos en una sociedad en constante evolución tecnológica y digital. Ante esta realidad, se ha tejido

[1] VIGARIO, D. "Más de 30 afectadas, una familia con una niña víctima y otro hijo administrador del chat, 11 denuncias... el caso de fotos falsas que alarma Almendralejo". *El Mundo.* 22 de septiembre 2023. Disponible en: https://www.elmundo.es/espana/2023/09/19/6509d01be85eceaa5a8b457b.html
[2] Pankiw, Ally (2023). En *Black Mirror* (Temporada 6, Episodio 1). Netflix Inc. Netflix. Reino Unido.
[3] Constitución Española. *Boletín Oficial del Estado*, núm. 311, de 29/12/1978.

un complejo entramado legislativo que se analizará a continuación, abarcando ámbitos nacional, europeo e internacional: con el propósito de garantizar la privacidad a través de la protección de datos. El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) son los dos pilares fundamentales en la regulación de la protección de datos personales y la privacidad en España y la Unión Europea. Aunque ambas leyes tienen objetivos similares, existen importantes diferencias entre ellas que son críticas para entender el panorama legal de la protección de datos en España.

2.1.1. El Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos representa una directriz fundamental dentro de la Unión Europea, aplicable a todos sus estados miembros, cuyo propósito esencial es la tutela de los datos personales y la privacidad ciudadana. Este marco normativo se enfoca en asegurar que el tratamiento de los datos personales se realice de manera justa, precisa y transparente, conforme a los estándares establecidos por la Comisión Europea en 2018 (COMISIÓN EUROPEA, "Reglamento General de Protección de Datos"). Dentro de este reglamento se consolidan principios clave que definen las bases legales para un tratamiento adecuado de los datos personales, principios que se reflejan en el conjunto de leyes que configuran el sistema regulatorio de la privacidad en España. Entre estos principios[4] se encuentran la limitación de la finalidad del tratamiento (art. 5.1.b RGPD), que estipula que los datos deben ser recopilados con fines específicos, explícitos y legítimos; el principio de licitud, integridad y confidencialidad (art. 5.1.f RGPD), que demanda que los datos sean tratados de manera segura, protegiendo contra el tratamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental; y el derecho de los interesados a ejercer sus derechos (arts. 12-22 RGPD), que incluye solicitudes de acceso, rectificación, supresión y oposición al tratamiento de sus datos personales. El RGPD, además de consolidar derechos ya existentes

[4] El Artículo 5 del RGPD, enumera los siguientes principios relativos al tratamiento: Licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud, limitación del plazo de conservación; integridad y confidencialidad, y responsabilidad proactiva. Estos principios constituyen el núcleo del RGPD, orientando cómo deben gestionarse los datos personales en cualquier contexto, asegurando la protección de los derechos fundamentales de las personas.

en la legislación previa española, introdujo principios novedosos que no habían sido contemplados en marcos legales anteriores en España, como la Ley Orgánica de Protección de Datos DE 1999[5]. Entre estas novedades, destaca el principio de "privacidad desde el diseño y por defecto", que exige que las organizaciones incorporen medidas de protección de datos en las primeras fases de cualquier proyecto que implique el tratamiento de datos personales. También, el RGPD refuerza el principio de responsabilidad proactiva, obligando a las entidades a demostrar, en todo momento, que están cumpliendo con el reglamento. Además, el RGPD introdujo derechos como el "derecho de supresión" y la "portabilidad de datos", que ayudan a la ciudadanía a retener cierto control sobre el tratamiento de sus datos. Estos principios propulsan una evolución en la protección de datos, poniendo énfasis en la prevención y en garantizar una gestión más responsable y transparente de la información personal en el entorno digital contemporáneo.

2.1.2. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Una de las diferencias más significativas entre el RGPD y la LOPDGDD es que mientras el primero es una regulación que se aplica de forma uniforme en toda la Unión Europea, la LOPDGDD tiene especificidades propias del ordenamiento jurídico español. No solo aborda la protección de datos personales, sino que también añade garantías en el ámbito de los derechos digitales, como el derecho al acceso universal a Internet y la protección de menores en el entorno digital.

Por ejemplo, la LOPDGDD introduce el concepto de "derechos digitales", que no está contemplado en el RGPD. La LOPDGDD no solo adapta el RGPD, sino que también lo amplía en ciertos aspectos, incorporando protecciones adicionales y especificando los mecanismos por los cuales la ciudadanía española puede ejercer sus derechos en materia de protección de datos, como el derecho de acceso, rectificación, supresión, entre otros. A su vez, obliga a las entidades a adoptar medidas proactivas para garantizar la transparencia y la responsabilidad en el tratamiento de datos, estableciendo mecanismos de notificación y respuesta ante

[5] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

posibles brechas de seguridad. Este complemento subraya la bidireccionalidad del marco legal: no sólo confiere derechos a los individuos, sino que también impone obligaciones a las entidades que manejan datos personales (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para el cumplimiento del deber de informar*. 2017).

2.2. Protección de datos aplicada a la Seguridad Ciudadana

Al abordar la temática de la protección de datos, es común que la atención se centre primordialmente en el Reglamento General de Protección de Datos y en la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, debido a su reconocimiento como los pilares que establecen los principios legales del tratamiento de datos personales. Sin embargo, considerar el marco regulatorio de la privacidad y la protección de datos en España exclusivamente a través de estas dos legislaciones constituiría un enfoque limitado. Dada la extensa red de normativas, este estudio se enfocará específicamente en los dominios de la seguridad ciudadana y la videovigilancia, analizando su interrelación con la protección de datos y su implementación tanto en el sector público como en el privado. A través de este análisis, se pretende destacar sectores clave de la legislación española que fundamentan su aplicación en el procesamiento de datos personales con el objetivo de preservar la seguridad de los ciudadanos, examinando cómo se integran las consideraciones sobre la protección de datos en estas áreas.

2.2.1. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos para fines penales

La Ley Orgánica 7/2021, de 26 de mayo, representa un esfuerzo normativo destinado a proporcionar un marco jurídico específico para el tratamiento de datos personales en el ámbito penal[6]. La ley se inserta en el marco legal español alineándose con la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 («Directiva de Protección de Datos de la Policía»). Esta legislación fue orientada a la adaptación y

[6] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. *Boletín Oficial del Estado,* núm. 126, de 27 de mayo de 2021, páginas 64103 a 64152.

modernización de la normativa española con la estructura jurídica europea, en respuesta a los desafíos digitales y las amenazas emergentes en ciberseguridad.

La Ley Orgánica 7/2021 tuvo como objetivo principal establecer un marco regulador para el tratamiento de datos personales por autoridades competentes en contextos penales, garantizando el respeto a los derechos fundamentales y la proporcionalidad en dicho tratamiento, y promoviendo un intercambio seguro y sin restricciones de dichos datos a nivel nacional y europeo, todo ello respaldado por un régimen sancionador específico (VILLAR FUENTES 2019). Esta ley se destaca por introducir garantías específicas para el afectado, como el derecho de acceso, el derecho de rectificación y el derecho a la supresión de los datos personales, siempre y cuando no se ponga en peligro las finalidades de la investigación o se ponga en peligro a un tercero que tenga relación con dicha investigación[7]. Se establecen también obligaciones claras para las autoridades competentes, como la necesidad de mantener registros de tratamiento y realizar evaluaciones de impacto en determinados casos (COLOMER 2018).

La Ley Orgánica 7/2021 reconoce la especial sensibilidad de los datos tratados en este ámbito y establece en su artículo nueve un sistema de categorías de datos, distinguiendo, por ejemplo, entre datos personales de diferentes categorías de personas, como víctimas, testigos y sospechosos. Además, prohíbe expresamente el tratamiento de datos personales que revele el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, salvo en circunstancias excepcionales según su artículo trece.

Uno de los aspectos más aplaudidos por la comunidad jurídica es la inclusión de medidas específicas de protección para los grupos más vulnerables, como menores o víctimas de delitos de violencia de género en línea (RODRÍGUEZ FERNÁNDEZ 2022). No obstante, es importante subrayar que, pese a sus avances, uno de los mayores retos para la aplicación efectiva de la Ley Orgánica 7/2021 es que se requiere de una estrecha colaboración entre las autoridades judiciales y las fuerzas de seguridad, así como de una formación continua de estos profesionales para garantizar que la protección de datos se integre plenamente en las

[7] Artículo 16 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

investigaciones penales. Expertos como VOGUEL (2007, p.158) instan a la adaptación de una "cultura penal común" que permitan una mayor cooperación para abordar casos de ciberdelincuencia transfronterizos, pero protegiendo efectivamente las libertades civiles (ÁLVAREZ GARCÍA, 2008).

2.2.2. Ley Orgánica 13/2015, de modificación de la LECrim y regulación de medidas de investigación tecnológica

La Ley Orgánica 13/2015[8] introdujo modificaciones sustanciales en la Ley de Enjuiciamiento Criminal (LECrim)[9] para adaptarse a la era digital y para afrontar los retos que supone la investigación de delitos cometidos mediante el uso de tecnologías de la información. Esta adaptación no solo buscó dotar a las autoridades de herramientas adecuadas para combatir el *cibercrimen*, sino que también se enfocó en garantizar los derechos fundamentales de la ciudadanía, especialmente la protección de sus datos personales. De esta forma, la legislación armonizó de manera más efectiva las facultades de las fuerzas de seguridad del Estado con los derechos de protección de datos. Tal equilibrio, como se ha observado en análisis previos, no había sido adecuadamente establecido en normativas complementarias, como la Ley de Seguridad Ciudadana (SANCHIS CRESPO 2017).

La reforma introducida por la Ley Orgánica 13/2015 estableció un marco normativo que buscaba asegurar que las intervenciones en comunicaciones electrónicas y la obtención de datos digitales se llevaran a cabo respetando íntegramente los derechos fundamentales. Según el artículo 588 bis a de la citada reforma, estas intervenciones debían ser proporcionadas, fundamentadas y sujetas a la supervisión de una autoridad judicial, lo que representó un progreso notable en la tarea de asegurar un equilibrio entre la protección de la seguridad pública y la salvaguarda de los derechos individuales. Adicionalmente, el artículo 588 ter g establecía que, tras concluir la fase de investigación y previamente a la

[8] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado*, núm. 239, de 6 de octubre de 2015, páginas 90192 a 90219

[9] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *Boletín Oficial del Estado*, núm. 260, de 17 de septiembre de 1882, páginas 803 a 806.

celebración del juicio oral o la decisión de sobreseimiento, el juez instructor debía determinar la notificación a los individuos sometidos a intervenciones de comunicaciones, así como a terceros afectados, respecto a dichas medidas, a menos que dicha notificación pudiera comprometer seriamente la protección de derechos fundamentales o la seguridad nacional. Este precepto consolidó el derecho de las partes a estar informadas, fortaleciendo las garantías procesales y ofreciendo la posibilidad de impugnar intervenciones que se consideraran impropias. Con estas disposiciones, la reforma procuró armonizar las exigencias propias de la investigación judicial con el respeto inalienable a los derechos fundamentales de los sujetos involucrados (BUENO DE MATA 2015).

La reforma efectuada por la Ley Orgánica 13/2015 incorporó también herramientas novedosas como la autorización del uso de software intrusivo para fines investigativos, luego de esto más conocidos como "troyanos judiciales" o "virus espía" (JORGE SANMARTÍN 2016). De acuerdo con su artículo 588 bis b, la aplicación de estos dispositivos quedaba reservada únicamente para la indagación de delitos de especial gravedad, y siempre estaba supeditada a una previa autorización judicial. Para delimitar la injerencia en los derechos fundamentales, se estipulan en el artículo 588 bis parámetros concretos respecto a la duración y el alcance de estas intervenciones, asegurando que solo se actuara en la medida en que resultase estrictamente necesario. Por otro lado, el artículo 588 bis d de la LECrim, tras su modificación, enfatizó la premisa de que solo debían recolectarse los datos imperativos para la elucidación de un hecho delictivo, reflejando así la esencia del principio de minimización de datos en el ámbito penal. Dicho principio es trascendental en la protección de datos en el ámbito penal, puesto que tiene como finalidad evitar la exposición o manejo inapropiado de información personal que no guarde relación directa con el objeto investigativo (MARCOS AYJÓN 2017).

Adicionalmente, al reconocer la imperatividad de garantizar la inviolabilidad de la información recabada, el artículo 588 bis *e* estableció protocolos rigurosos que buscaban proteger los datos de cualquier riesgo de acceso no autorizado, extravío o destrucción. En este contexto, la norma previó la implementación de medidas de carácter técnico y organizativo con el propósito de asegurar la integridad y seguridad de la información a lo largo de la investigación. Esta conciencia creciente sobre la importancia de la ciberseguridad ha llevado también a la colaboración más estrecha con entidades como el Instituto Nacional de Ciberseguridad (INCIBE), que hoy en día actúa como referente nacional en materia de ciberseguridad,

asesorando y ofreciendo las salvaguardas tecnológicas indispensables para garantizar una adecuada protección de los datos en el ámbito judicial (BARRIO ANDRÉS 2018).

2.2.3. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

La Ley 25/2007 fue creada en respuesta a la Directiva 2006/24/EC de la Unión Europea, con el fin de regular la retención de datos generados durante la prestación de servicios de comunicaciones electrónicas y redes públicas. El principal objetivo de esta ley era el de asegurar que estos datos estuviesen disponibles para investigar y perseguir delitos serios en España, siempre respetando las normativas europeas.

Según su artículo 3, se requería la conservación de ciertos datos específicos relacionados con las comunicaciones electrónicas, tales como la identidad de los comunicantes, las fechas y duración de las comunicaciones, excluyendo de manera explícita el contenido de las mismas. Estos datos, conocidos comúnmente como "datos de tráfico", se convertían en herramientas indispensables para la investigación, facilitando la geolocalización y el seguimiento del uso de internet. A principios del siglo XXI, prevalecía la tendencia entre los proveedores de servicios de retener datos únicamente con fines de facturación, eliminándolos posteriormente para optimizar el almacenamiento en sus bases de datos. Esta legislación, sin embargo, instauró la obligación de conservar dichos datos por un período de entre seis meses a dos años desde la fecha de la comunicación, según se recoge en su artículo 5. Resulta esencial subrayar que la entrega de datos conservados a las autoridades solo es permisible en el contexto de una investigación de delitos graves y siempre que se cuente con una orden judicial, alineándose con los criterios establecidos en la Ley de Enjuiciamiento Criminal (LECrim)[10], y evitando la cesión de datos que resultasen innecesarios para la finalidad perseguida por la investigación judicial. Esto no solo buscaba salvaguardar los derechos y libertades individuales, sino también asegurar que el principio de proporcionalidad fuese mantenido, aunque de manera limitada, pese a la naturaleza intrusiva de esta ley (RODRÍGUEZ LAINZ 2008). Sin embargo, la insuficiencia de estas garantías para con la privacidad de la ciudadanía resultó aparente

[10] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *Boletín Oficial del Estado*, núm. 260, de 17 de septiembre de 1882, páginas 803 a 806.

cuando el Tribunal de Justicia de la Unión Europea, en la Sentencia de 8 abril de 2014, declaró la nulidad de la Directiva 2006/24, considerando que era demasiado intrusiva en la vida privada (MARZO COSCULLUELA 2014).

A pesar de este pronunciamiento, en España la ley se mantuvo, si bien se realizaron ajustes menores en mayo de 2014 publicados en el Boletín Oficial del Estado. En la práctica, estos cambios no tienen efectos sobre la exigencia significativa que supone el cumplimiento de esta norma para los proveedores de telecomunicaciones. Estos enfrentan el reto de equilibrar la obligación normativa de retener datos con el deber de garantizar transparencia y permitir el ejercicio de derechos como el de supresión por parte de sus clientes y otros interesados, en consonancia con el Reglamento General de Protección de Datos. La problemática radica en discernir entre retener datos en aras de la prevención y atender solicitudes de supresión, evitando sanciones, pero también resguardándose de posibles reclamaciones ante la Agencia Española de Protección de Datos.

2.3. Protección de datos aplicada a la videovigilancia

2.3.1. Ley 5/2014, de 4 de abril, de Seguridad Privada

La Ley 5/2014, de 4 de abril[11], se erige como la normativa esencial que regula las actividades y servicios relacionados con la seguridad privada en España. Esta ley, a través de sus artículos, establece un marco legal que guía la actuación de la seguridad privada y su interacción y complementación con las instancias de seguridad pública. Esta ley propuso reformas con el objetivo de garantizar que las operaciones de seguridad privada en España se realizaran respetando tanto las libertades y derechos fundamentales de los interesados como los parámetros del cumplimiento normativo en el ámbito de investigaciones privadas, y la cooperación eficiente con las entidades de seguridad pública, sin sobrepasar sus atribuciones (DE MADRID DÁVILA 2021). En cuanto al objeto y ámbito de aplicación, en sus artículos primero a tercero, se define el propósito y alcance de esta normativa, sentando las bases que supervisan la actuación de las empresas, el personal de seguridad privada y actividades

[11] Ley 5/2014, de 4 de abril, de Seguridad Privada. *Boletín Oficial de Estado,* núm. 83, de 5 de abril de 2014, páginas 28975 a 29024.

llevadas a cabo por detectives privados, garantizando que no desempeñen roles exclusivos de las Fuerzas y Cuerpos de Seguridad del Estado, respaldando el principio de la preeminencia de la seguridad pública sobre la seguridad privada (MARTOS 2018).

El primer capítulo de la Ley 5/2014 delinea las actividades y servicios subsumidos bajo el ámbito de la seguridad privada. Estas actividades abarcan desde la vigilancia y protección de bienes, emplazamientos, establecimientos y eventos, hasta las investigaciones privadas relacionadas con asuntos particulares. La normativa se destaca como uno de los cimientos legales primordiales para el ejercicio de la videovigilancia en el marco del RGPD, especialmente en lo que concierne a las empresas y las operaciones desempeñadas por su personal de seguridad privada. Con el artículo 30 (h) de la Ley 5/2014, se instaura una obligación legal para las empresas de seguridad privada de cooperar activamente con las Fuerzas y Cuerpos de Seguridad del Estado. En este contexto, la videovigilancia se consolida como un recurso esencial, no solo para dar cumplimiento a un mandato jurídico, sino también para contribuir al interés público de mantener la seguridad y el orden.

En palabras de PARDO MARQUINA (2021), «*El interés público inherente al tratamiento de imágenes se centra en garantizar la protección o seguridad de las personas y bienes localizados en el respectivo establecimiento o empresa*». Para enfatizar la relevancia de este concepto en el marco del tratamiento de datos personales, de acuerdo con el Reglamento General de Protección de Datos de 2018, específicamente en su artículo 5, se establece que los datos recopilados para un propósito específico no deben ser utilizados para fines diferentes. Por lo tanto, las empresas que instalan sistemas de videovigilancia, atendiendo a este interés público, deben ser cautelosas para asegurarse de no emplear las grabaciones con fines distintos a la seguridad y protección de personas y bienes (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía sobre el uso de videocámaras para seguridad y otras finalidades.* 2017).

Cabe destacar también la clara delimitación del alcance de actuación de la seguridad privada que establece el artículo 42.2 de la Ley 5/2014. Dicho artículo veta de manera expresa la captación de imágenes y sonidos en vías y espacios públicos, o aquellos de acceso público, sin el debido aval del órgano público competente. Esta disposición impone una responsabilidad incrementada sobre las empresas de vigilancia privada contratadas por entidades, instándolas a ser particularmente meticulosas al evitar la ubicación de cámaras en áreas públicas. Por otra

parte, el artículo 42.4 armoniza esta legislación con el RGPD y la LOPGDD, conviniendo que las imágenes obtenidas sólo deben emplearse con el objetivo primordial de garantizar la seguridad de las personas y bienes en las instalaciones de la entidad y resaltando el mandato de que las empresas y profesionales de seguridad privada observen las normativas actuales en materia de protección de datos [12]. Esto implica que, cuando se utilice este interés público como base legitimadora para el uso de cámaras de videovigilancia en una empresa, las imágenes captadas por dichas cámaras no podrán ser usadas también para monitorear el rendimiento de los trabajadores, siendo necesario para este propósito que se utilice un método alternativo de monitoreo (ya sean cámaras diferentes a las que la empresa de seguridad privada no tenga acceso si no existiera un método menos intrusivo para esta finalidad) y que se lleve a cabo un estudio de impacto de la privacidad totalmente al margen de las actividades de la seguridad privada por parte del personal de seguridad[13].

Respecto al uso de cámaras de videovigilancia en el marco de esta la Ley 5/2014, el ámbito privado encuentra sus mayores desafíos respecto al uso de cámaras con respecto a las obligaciones específicas que el RGPD impone a las empresas como encargados del tratamiento de los datos personales de sus empleados. Entre estas obligaciones, destaca la prohibición de procesar datos de carácter especial (artículo 9 del RGPD), que incluye categorías de datos que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o la afiliación sindical, entre otros.

En lo que respecta a los datos biométricos, como el reconocimiento facial, el RGPD los cataloga como datos de carácter especial. Su uso está sujeto a un escrutinio y regulación más estrictos, ya que implica el procesamiento de información única y personal que puede identificar a un individuo con precisión. Por ello, cualquier sistema de videovigilancia que utilice reconocimiento facial debe contar con una base jurídica sólida para su tratamiento, y las empresas deben garantizar medidas de protección adicionales. Según expertos como PARDO MARQUINA (2021), esto no supone ningún problema en el estricto contexto del cumplimiento

[12] Lo cual atiende al "principio de limitación de la finalidad," del artículo 5 del Reglamento General de Protección de Datos.

[13] Siguiendo las recomendaciones de la Agencia Española de Protección de datos, en su guía "La protección de datos en las relaciones laborales" 2021, páginas 52 y 53.

de las obligaciones establecidas por la Ley 5/2014, por parte del personal privado de seguridad siempre y cuando el uso de datos biométricos sea rigurosamente necesario, ya que: *"el hecho de recabarlos con motivo del cumplimiento de una misión realizada en interés público permite no solamente tal tratamiento, sino también que el mismo se efectúe sin el consentimiento previo del interesado, ex artículo 9.2.g) RGPD, junto con su considerando 45. Ello legitima el tratamiento de los datos captados por las videocámaras".* Es imperativo abordar con prudencia la excepción estipulada en el artículo 9.2(g)[14] del RGPD, ya que cualquier limitación al tratamiento de datos impuesta por el RGPD debe ser evaluada detenidamente. Este proceso implica una compleja tarea, generalmente asignada al delegado de protección de datos, consistente en demostrar que los beneficios en términos de interés público derivados de la actividad de vigilancia prevalecen sobre las posibles repercusiones negativas en la privacidad de las personas registradas. Aun así, es crucial destacar que, incluso apelando a la excepción del artículo 9.2(g) del RGPD, los interesados mantienen íntegramente su derecho a ejercer las facultades de información, acceso o supresión. En este sentido, se plantea un escenario desafiante para la empresa, que debe encontrar el justo equilibrio para justificar adecuadamente el tratamiento de los datos y, simultáneamente, satisfacer las demandas de los interesados cuando estos decidan ejercer sus derechos.

Por el contrario, expertos como MAGRO SERVET (2022) defienden que esta postura no es correcta, ya que, para emplear el reconocimiento facial, se hace uso de tecnologías que son altamente intrusivas para la privacidad de los interesados y, por lo tanto, a falta de un interés público por parte de las Fuerzas y Cuerpos de seguridad del Estado, su uso para meros propósitos de seguridad privada es desproporcionado. Este autor considera la regulación *actual "insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada, al no cumplir los requisitos anteriormente señalados, siendo necesario que se aprobara una norma con rango de ley que justificara específicamente* ***en qué medida y en qué supuestos****, la utilización de dichos sistemas respondería a un interés público esencial".* En ausencia de una normativa de tal

[14] *"El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado"*

índole, se hace imprescindible que las empresas que deseen implementar tecnologías de reconocimiento facial, potencialmente lesivas para los derechos y libertades individuales, realicen una consulta previa ante la Agencia Española de Protección de Datos. Este organismo, a su vez, tiene el deber de evaluar los riesgos asociados y, en consecuencia, proponer ajustes tecnológicos para minimizar los impactos adversos, o incluso, en casos extremos, podría llegar a restringir la implementación y comercialización de dichas tecnologías (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. 2021).

2.3.2. Ley Orgánica 4/1997 sobre la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos

La Ley Orgánica 4/1997[15] constituye un hito jurídico en la regulación del uso de videocámaras por parte de las Fuerzas y Cuerpos de Seguridad en espacios públicos en España. Teniendo en cuenta su promulgación anterior a la entrada en vigor de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[16], esta norma surge en un contexto donde se busca armonizar dos derechos fundamentales con especial sensibilidad: por un lado, el derecho a la seguridad ciudadana que resulta del artículo 104 de la Constitución y, por otro, el derecho a la intimidad y protección de datos personales de la ciudadanía.

El principal objetivo de esta Ley es regular el empleo de videocámaras como herramienta de prevención frente a delitos y actos antisociales, así como facilitar la labor investigadora posterior a la comisión de ilícitos. No obstante, su ámbito de aplicación se circunscribe de manera exclusiva a las zonas de uso público, entendiendo por estas aquellas vías públicas o espacios donde la ciudadanía tiene un libre acceso. Adhiriéndose a los principios de proporcionalidad, idoneidad y necesidad, la ley postulaba que cualquier intervención que implicase la instalación y uso de estas cámaras debería ser adecuada y congruente respecto a

[15] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. *Boletín Oficial del Estado*, núm. 186, de 5 de agosto de 1997, páginas 23824 a 23828.

[16] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial de Estado*, núm. 298, de 14/12/1999. Norma derogada, con efectos de 7 de diciembre de 2018, sin perjuicio de lo previsto en la disposición adicional 14 de la Ley Orgánica 3/2018, de 5 de diciembre,

la finalidad perseguida. En este sentido, la instalación de dispositivos de videovigilancia en espacios públicos requeriría de una autorización expresa por parte de la Delegación del Gobierno competente. Esta autorización, lejos de ser arbitraria, debía de estar justificada en razones de prevención de actividades delictivas o para la investigación de actos delictivos ya perpetrados (GARCÍA MIGUEL 2020).

Uno de los aspectos más relevantes es la temporalidad de las grabaciones, pues la ley exigía en su artículo 8 que las mismas debían ser eliminadas al cabo de un mes desde su registro, a menos que fuesen requeridas por instancias judiciales o se utilicen en procedimientos sancionadores administrativos. Paralelamente, y en consonancia con los derechos de los interesados contemplados por el RGPD sobre protección de datos, su artículo 9 reconoce el derecho de la ciudadanía a acceder a las grabaciones donde figuren, pudiendo solicitar su rectificación o supresión. Por último, cabe mencionar que la norma contemplaba límites claros a la videovigilancia, prohibiendo expresamente la captación de imágenes y sonidos en espacios donde razonablemente se espera privacidad, como el ámbito doméstico, en su artículo 6.5. Pese a estas provisiones que, hasta cierto punto, eran novedosa para la época de la entrada en vigor de la Ley Orgánica 4/1997, la falta de una provisión expresa que instase a la transparencia en esta regulación fue especialmente criticada, sobre todo respecto a la falta de delimitación del alcance de los poderes atribuidos por esta ley a las Fuerzas y Cuerpos de Seguridad del Estado (GONZÁLEZ GUTIÉRREZ y GONZÁLEZ URDINGUIO 2003).

Según BARCELONA LLOP (2001), la Ley Orgánica 4/1997 presentaba una falta de balance preocupante en relación con la separación de poderes, principalmente al permitir que jueces y magistrados activos participasen en órganos administrativos que posteriormente podrían revisar judicialmente, lo cual generaba un conflicto de interés evidente. Según el citado experto, ciertas incoherencias hacían que esta ley pareciese haberse promulgado de manera prematura, apuntando por ejemplo que, a pesar de contemplar el principio de proporcionalidad en su artículo 4, el artículo 3 no dejaba claro si dicho principio sería aplicable sólo para decidir sobre la instalación de cámaras fijas, o también para decidir si su utilización era necesaria. Sobre esto, BARCELONA LLOP reitera al final su análisis que «*si las videocámaras fijas se instalan es para ser utilizadas*».

Pese a la crítica inmediata a su entrada en vigor en agosto de 1997, y pese a la crítica que se le ha seguido dando durante los últimos veintiséis años en múltiples contextos respecto a su

aplicabilidad, la ley sigue en vigor y sin modificaciones en su texto hoy en día (FRÍAS MARTÍNEZ 2010, SEMPERE SAMANIEGO 2020, CARDONA RUBERT 2016). Sin embargo, algunos de estos preceptos han sido abordados por la reciente ley Orgánica 07/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales[17].

3. Aplicación y cumplimento del marco legal-regulatorio

El marco legal-regulatorio de la protección de datos en España se articula a través de un conjunto de organismos e instituciones que tienen la misión de velar por el cumplimiento de la legislación en materia de privacidad y protección de datos personales. Este análisis se concentra principalmente en el trabajo de la Agencia Española de Protección de Datos (AEPD), entidad autónoma encargada de garantizar y supervisar la aplicación de las normativas de protección de datos a nivel nacional. La AEPD ejerce un papel fundamental en la tutela de derechos relacionados con la protección de datos personales, actuando como una entidad independiente de supervisión y control (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Funciones y Poderes*. 2017).

En el ámbito judicial, los juzgados de primera instancia atienden las cuestiones relacionadas con reclamaciones individuales y conflictos en materia de protección de datos, proporcionando resoluciones que sientan precedentes y clarifican la aplicación de la ley en casos concretos (BLANCO ANTÓN 2019). Por otro lado, la Audiencia Nacional se ocupa de las apelaciones en contra de las resoluciones de la AEPD, mientras que el Tribunal Supremo, como máximo órgano jurisdiccional en España, tiene la última palabra en la interpretación del derecho español, incluyendo el régimen de protección de datos (DÍEZ SASTRE, S. MARTÍNEZ SÁNCHEZ, C. EGEA DE HARO, A. et al. 2019). Las sentencias de este tribunal no solo resuelven los litigios, sino que también consolidan la jurisprudencia y dirigen la interpretación de las

[17] La reciente legislación modificó significativamente la gestión de datos personales y el uso de videocámaras por las fuerzas de seguridad, promoviendo un enfoque conforme al RGPD. Esta normativa recalca la necesidad de un tratamiento de datos y vigilancia equitativos, proporcionales y transparentes, salvaguardando los derechos fundamentales y estableciendo un marco legal claro para el uso de tecnologías de vigilancia en el ámbito público. Se subraya la expectativa de directrices futuras que refuercen estas prácticas dentro del respeto a la privacidad.

normas de protección de datos, teniendo un impacto directo en la política de privacidad de las entidades públicas y privadas. Asimismo, el Tribunal Constitucional desempeña un papel preeminente en la protección de los derechos fundamentales, incluido el derecho a la protección de datos personales, considerado como tal por la jurisprudencia constitucional (RODRÍGUEZ ROCA 2022). Este tribunal tiene la facultad de enjuiciar la constitucionalidad de las leyes, pudiendo declarar nulos aquellos preceptos que vulneren derechos fundamentales. Finalmente, cabe mencionar el papel de los tribunales europeos, como el Tribunal de Justicia de la Unión Europea (TJUE), que, a través de sus sentencias, determinan la interpretación uniforme de la legislación europea en materia de protección de datos, asegurando su correcta aplicación y efectividad en todos los estados miembros[18].

3.1. Aplicación práctica en el sector público: Administraciones Públicas y las Fuerzas de Seguridad del Estado

La Agencia Española de Protección de Datos tiene atribuidas una serie de facultades específicas en relación con las administraciones públicas y las fuerzas y cuerpos de seguridad del Estado y las agencias de inteligencia, aunque con ciertas limitaciones en su ámbito de actuación. Con respecto a las administraciones públicas y las fuerzas de seguridad, la AEPD tiene la capacidad de supervisar y controlar el cumplimiento de la normativa en materia de protección de datos. Puede recibir denuncias, realizar investigaciones y, en caso de detectar incumplimientos, está facultada para emitir resoluciones que pueden incluir medidas correctivas y, si es necesario, apercibimientos (DELGADO MARTÍN 2019). Sin embargo, a diferencia de lo que ocurre con las entidades privadas, la AEPD no puede imponerles sanciones económicas.

A pesar de que el Reglamento General de Protección de Datos ofrece a los Estados miembros la facultad de sancionar económicamente a tales entidades, la LOPDGDD opta por excluir las sanciones financieras a administraciones públicas y otros órganos estatales en su artículo 77. Esta elección legislativa se ha justificado como un método regulador que busca inducir a la

[18] Web oficial de la Unión Europea: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_es

corrección y al cumplimiento normativo a través de la presión social y la responsabilidad institucional, más que por la vía económica. Además, se considera que las sanciones pecuniarias entre entidades del sector público no supondrían una transferencia efectiva de recursos, sino una redistribución interna dentro del sector público (SÁNCHEZ-JARA 2021). En lugar de multas, se prefieren medidas como el apercibimiento y la amonestación, acompañadas de la posibilidad de hacer pública la infracción (ORTEGO RUIZ 2020). Recientemente, se ha observado un incremento notable en la actividad sancionadora de la AEPD. En el año 2020, por ejemplo, las sanciones impuestas a administraciones públicas aumentaron en un sustancial 160%, evidenciando una tendencia creciente hacia la fiscalización más estricta de la privacidad y la protección de datos (GARCÍA 2021).

Finalmente, es importante señalar que la situación del Centro Nacional de Inteligencia (CNI), encargado de investigar amenazas contra la Seguridad Nacional, es más compleja por su función y actividades. La AEPD no interviene en la supervisión de esta agencia de inteligencia, ya que sus operaciones están sujetas a un régimen legal específico que reconoce la necesidad de proteger la seguridad nacional y manejar información clasificada. La regulación establece mecanismos alternativos de control, como el Defensor del Pueblo o la Comisión Delegada del Gobierno para Asuntos de Inteligencia, para garantizar la legalidad de sus operaciones sin comprometer la confidencialidad requerida en inteligencia. Aunque las actividades del CNI están excluidas de la aplicación directa de las normas de protección de datos personales y privacidad por el RGPD (Considerando 16) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (artículo 2(c)), se espera que respete principios de protección de datos acordes a su marco legal, reconociendo las dificultades de armonizar completamente las regulaciones de seguridad nacional con las de protección de datos.

Este apartado presenta un examen detallado de resoluciones notables de la AEPD dentro de los ámbitos de más común incumplimiento por parte de las administraciones públicas y las fuerzas de seguridad del Estado.

3.1.1. Videovigilancia y captación de audio y limitación de la finalidad de tratamiento

a) Resolución PS/00377/2021: Ayuntamiento de Villargordo

En la esfera de la videovigilancia y su regulación conforme al Reglamento General de Protección de Datos es pertinente examinar la resolución PS/00377/2021 emitida por la Agencia Española de Protección de Datos (AEPD). Este caso involucra al Ayuntamiento de Villargordo Del Cabriel en Valencia, sancionado por la implementación de un sistema de videovigilancia que no solo capturaba imágenes sino también grabaciones sonoras, sin obtener el consentimiento necesario ni informar adecuadamente a los empleados municipales. Esta práctica fue considerada una transgresión al artículo 5(1)(c) del RGPD que prescribe la adecuación, pertinencia y limitación de los datos al mínimo necesario en relación con los fines para los que son tratados.

La AEPD respondió con una medida disciplinaria en forma de advertencia al municipio, acompañada de la instrucción de instalar señalización apropiada y la obligación de informar a los trabajadores sobre la recopilación y procesamiento de sus datos personales. Sin embargo, la decisión fue objeto de un recurso de reposición. Un mes más tarde, la Agencia concluyó la falta de evidencias concluyentes que demostrasen el procesamiento efectivo de las conversaciones del empleado denunciante, y se tuvo en cuenta la aseveración del ayuntamiento de que las cámaras nunca estuvieron operativas.

No obstante, la situación del denunciante, quien alegó que estas acciones contribuyeron a su despido, no fue examinada con profundidad. La AEPD no extendió sus investigaciones para confrontar las asimetrías de poder inherentes en la relación empleado-empleador, las cuales podrían constituir un obstáculo considerable para el empleado a la hora de proporcionar pruebas del funcionamiento de las cámaras y de un uso indebido de grabaciones en su contra.

b) Resolución PS/00027/2019: Cuerpo Nacional de Policía

Siguiendo un análisis comparativo del tratamiento de infracciones al Reglamento General de Protección de Datos (RGPD) entre el sector público y el privado, es ilustrativo examinar la resolución PS/00027/2019 emitida por la Agencia Española de Protección de Datos. Esta resolución atañe a una denuncia presentada por el Inspector A.A.A. del Cuerpo Nacional de Policía (CNP), quien se vio afectado por el uso indebido de material videográfico recabado por sistemas de vigilancia. El Inspector del CNP se encontraba cerca de las dependencias de la Comisaría, preparándose para salir a cenar, y fue captado vistiendo con un forro polar negro sobre su uniforme reglamentario debido a que era de noche y había una baja temperatura. Días después, sus superiores usaron estas imágenes, captadas por el sistema

de vigilancia de detenidos de la Comisaría, para instruirle un procedimiento disciplinario por no llevar bien puesto el uniforme. El Inspector del CNP interpuso reclamación por este motivo ante la AEPD, alegando que el uso de las cámaras de seguridad era el de vigilar a los detenidos y no el de monitorear a los empleados. Esta aplicación habría transgredido el principio de limitación de finalidad, tal como lo estipula el artículo 5.1.b) del RGPD. Este principio sostiene que los datos personales deben ser recogidos con fines específicos, explícitos y legítimos, y no ser tratados de manera incompatible con dichos fines. En especial, para el uso de cámaras de vigilancia, se requiere que las imágenes capturadas para un fin específico (seguridad de las dependencias) no sean usadas para otro fin totalmente distinto, como para amonestar a un empleado. La gravedad de la infracción fue reconocida por la AEPD, la cual optó por imponer un apercibimiento a la Dirección General de la Policía, entidad del Ministerio del Interior. Esta decisión no incluyó sanciones de índole económica, pese a que el uso indebido de la grabación para sancionar al Inspector por la vestimenta desviaba claramente el propósito original del sistema de videovigilancia.

La ausencia de penalización económica en este caso resalta una discrepancia potencial en la severidad con la que se abordan casos similares en el ámbito público versus el privado. En escenarios análogos dentro del sector privado, donde las relaciones laborales empleador-empleado están igualmente sujetas al escrutinio del RGPD, la utilización de videovigilancia para sancionar a empleados sin la debida base legal podría haber acarreado consecuencias monetarias significativas. La discreción administrativa ejercida al imponer únicamente un apercibimiento, y no una sanción económica, en un organismo estatal como la Dirección General de la Policía, podría ser interpretada como una manifestación de una dualidad de criterios que amerita una evaluación más profunda en pos de garantizar la equidad en la aplicación de la ley de protección de datos personales, independientemente de la naturaleza jurídica del ente infractor.

c) Resolución EXP202102430: Secretaría General de Instituciones Penitenciarias

Por último, en el contexto de la videovigilancia con fines de investigación penal, cabe destacar la resolución de procedimiento sancionador EXP202102430. La Agencia Española de Protección de Datos atendió a una serie de reclamaciones formuladas por distintas asociaciones de funcionarios penitenciarios contra la Secretaría General de Instituciones Penitenciarias (SGIP). Estas asociaciones denunciaban la filtración y difusión de imágenes de

videovigilancia del centro penitenciario de Villena, en Alicante, las cuales captaron un acto de agresión a un interno por parte de funcionarios. El caso, que fue objeto de una investigación interna y recibió atención mediática[19], planteaba serias preocupaciones acerca del manejo y confidencialidad de datos personales sensibles. Las mayores deficiencias encontradas por la AEPD respecto a la gestión de la seguridad de la información fueron la falta de perfiles de acceso adecuados y la ausencia de trazabilidad en el sistema de videovigilancia. Estas deficiencias indicaban que cualquier inspector podía acceder a las imágenes sin autorización clara, y no existían registros de acceso que permitieran rastrear quiénes habían consultado las imágenes. Tras la notificación de las reclamaciones y la ausencia inicial de respuesta por parte de la SGIP, la AEPD procedió a admitir las reclamaciones a trámite y a realizar las investigaciones preliminares pertinentes. Se constató que las imágenes se habían compartido no solo dentro de la administración penitenciaria sino también con órganos judiciales, lo que llevó a la apertura de procedimientos judiciales correspondientes. No obstante, la autoría de la filtración no pudo ser determinada, ni cómo se había producido la brecha de confidencialidad en el tratamiento de las imágenes. La SGIP justificaba el tratamiento de las imágenes basándose en las provisiones de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos para fines penales, pero reconocía la ausencia de registros de acceso a los datos personales y la concesión de perfiles de acceso amplios entre los funcionarios, lo cual impedía identificar a los responsables de la divulgación pública.

En respuesta a las alegaciones de la SGIP, la Agencia subrayó que el procedimiento sancionador respetaba el principio de presunción de inocencia y que la falta de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad del tratamiento de datos personales constituía una infracción de acuerdo con el artículo 32 del RGPD. La AEPD resolvió imponer un apercibimiento a la SGIP por la infracción del artículo 32 del RGPD y ordenó la adopción de medidas para asegurar registros adecuados de acceso a datos personales y la restricción de perfiles de acceso. La SGIP debía acreditar dicha adopción en un plazo de seis meses. Este caso resalta la necesidad imperativa de proteger la integridad de los sistemas de videovigilancia y la confidencialidad de los datos personales en el contexto de

[19] REDACCIÓN, “Todos contra Tu Abandono Me Puede Matar” El Periódico de Villena, 22 de noviembre 2021. Disponible en: https://elperiodicodevillena.com/todos-contra-tu-abandono-me-puede-matar/

penal. A pesar de la clara utilidad que la filtración de las imágenes tuvo en futuras investigaciones, la resolución de la AEPD subraya su rol de supervisión y refuerza la necesidad de cumplimiento estricto de las normativas de protección de datos para fines penales, ya que se debe garantizar los derechos y libertades fundamentales de todas las personas implicadas.

3.1.2. Licitud del tratamiento, integridad y confidencialidad

a) Procedimiento Nº AP/00055/2017: Policía Local y Ayuntamiento de Haro

En un procedimiento de Declaración de Infracción de Administraciones Públicas, la Agencia Española de Protección de Datos recibió denuncias anónimas en las cuales se acusaba a un miembro de la Policía Local de una localidad de la Rioja de conductas impropias en el manejo de datos personales. El policía local y otro colega del mismo Ayuntamiento fueron denunciados por el supuesto uso comercial de datos personales contenidos en las fichas policiales custodiadas por la institución, comercializándolos o facilitándolos a terceros sin autorización.

Pese a la gravedad de la denuncia respecto a las actuaciones de dicho policía local, la atención de la AEPD se centró en la conformidad de las medidas de seguridad del Ayuntamiento con el Reglamento General de Protección de Datos (RGPD). Se identificó que la infraestructura de seguridad de datos del Ayuntamiento era deficiente, permitiendo el acceso indebido a ficheros de datos personales a personal no autorizado, lo que facilitó la supuesta conducta delictiva del policía. Como resultado, se instó al Ayuntamiento a implementar ajustes correctivos para fortalecer sus sistemas de seguridad de datos y evitar futuras infracciones. En agosto de 2018, el Ayuntamiento de Haro remitió a la AEPD un informe sobre medidas correctivas que fueron implementadas para mejorar la seguridad de la información de sus ficheros digitales, y para rastrear los accesos a los archivos policiales en papel. La AEPD aceptó las medidas presentadas por el Ayuntamiento de Haro, y procedió al archivo de actuaciones del expediente.

Aunque la denuncia fue contra el presunto tratamiento de datos ilícito por parte de dicho agente de policía, la resolución se centró en la responsabilidad institucional del Ayuntamiento, destacando deficiencias en el cumplimiento de los estándares de protección de datos. No obstante, en la documentación de la AEPD no se detallan sanciones específicas contra el

agente acusado ni contra el funcionario del Ayuntamiento. Esta omisión resalta una falta de transparencia en la comunicación de los resultados de las acciones disciplinarias y correctivas, dejando un vacío informativo sobre la eficacia y el seguimiento de las resoluciones en términos de responsabilidad individual y mejora de los protocolos de seguridad de datos. La ausencia de estos detalles pone de relieve la necesidad de una mayor claridad en la rendición de cuentas por parte de las instituciones públicas.

b) Resolución PS/00123/2020: Ayuntamiento de Tobar

La Agencia Española de Protección de Datos sancionó al Ayuntamiento de Tobar tras una reclamación presentada contra éste, debido a la exposición pública de un censo con datos personales en el tablón de anuncios del ayuntamiento. Fotografías adjuntas demostraron la presencia de datos de vecinos fallecidos y vivos. Ante la falta de respuesta del Ayuntamiento a las solicitudes de la Agencia, se inició un procedimiento sancionador por la posible violación del artículo 5 del RGPD respecto a la falta de garantías sobre la confidencialidad e integridad del tratamiento de datos personales.

La Subdirección General de Inspección de Datos requirió al Ayuntamiento de Tobar que atendiera la reclamación y proporcionara información sobre las medidas tomadas para prevenir incidentes similares; sin embargo, esta solicitud no fue atendida. Posteriormente, se admitió a trámite la reclamación y se inició un procedimiento sancionador, en virtud de la presunta transgresión del artículo 5 del RGPD. La falta de respuesta del Ayuntamiento persistió aun después de una propuesta de resolución que establecía un apercibimiento y un requerimiento para que retirara el listado y expusiera los procedimientos de manejo de anuncios con datos personales. La resolución final de la directora de la AEPD impuso un apercibimiento al Ayuntamiento de Tobar, conforme al artículo 5.1.f del RGPD y el artículo 5 de la LOPDGDD, lo cual fue debidamente notificado al ente local.

El mantenimiento prolongado e innecesario de datos personales en un espacio público contradice directamente el principio de limitación de la finalidad de tratamiento, lo cual fue adecuadamente sancionado, reafirmando la importancia de la adecuada gestión y protección de datos conforme a las disposiciones normativas vigentes. Sin embargo, se puede observar que el Ayuntamiento fue apercibido con anterioridad a esta resolución, persistiendo en su falta de respuesta y cumplimiento hacia las instrucciones de la AEPD. Pese a ello, el único recurso disponible para la Agencia fue el de apercibir al reclamado una vez más. En la página

5 de la resolución, la AEPD indica *"El ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas",* pudiéndose percibir como un intento de reiterar que la falta de respuesta por parte del Ayuntamiento no se trata de una infracción leve y que, si no fuera por su condición de entidad pública, sin duda hubiese conllevado una multa.

c) Resolución PS/00388/2019: Grupo Municipal del Partido Popular de Vélez-Málaga

Finalmente, respecto a la limitación y licitud de tratamiento de datos especialmente sensibles y confidenciales, destaca procedimiento sancionador PS/00388/2019. La Agencia Española de Protección de Datos resolvió una reclamación contra el Grupo Municipal del Partido Popular de Vélez-Málaga, donde se alegaba una infracción de la normativa de protección de datos. El reclamante, identificado como A.A.A., denunció que un concejal del Partido Popular publicó en Facebook un decreto del Ayuntamiento que incluía su nombre y DNI con fines de crítica política, considerando esto una violación de sus derechos de protección de datos personales.

El Grupo Municipal del Partido Popular respondió que la publicación fue realizada en una cuenta personal de Facebook, no asociada directamente al partido. A pesar de esto, la AEPD inició un procedimiento sancionador por la presunta infracción del artículo 6.1.a del RGPD, considerando que la publicación de los datos personales del reclamante era excesiva y no necesaria para la crítica política expresada. La AEPD determinó que el Grupo Municipal del Partido Popular había infringido el principio de minimización de datos del artículo 5 del RGPD. La publicación del nombre y DNI del reclamante en Facebook fue considerada desproporcionada para los fines de crítica política perseguidos. La AEPD concluyó que esta práctica violaba el deber de confidencialidad y la obligación de limitar el tratamiento de datos personales a lo estrictamente necesario.

La AEPD sancionó al Grupo Municipal del Partido Popular en Vélez-Málaga con un apercibimiento por violar el artículo 5.1.c del RGPD, relacionado con la minimización de datos, y exigió la implementación de medidas preventivas para evitar reincidencias, asegurando así el cumplimiento de la legislación de protección de datos. Se requirió la comprobación de la adopción de estas medidas correctivas en un plazo de un mes. Aunque la AEPD enfatizó la inadecuación de utilizar el DNI del reclamante para objetivos políticos, no se abordó la gravedad inherente a la divulgación del DNI per se. La Agencia ha impuesto sanciones más severas a entidades privadas por compartir el DNI de un interesado con terceros, incluso en

contextos más alineados con la finalidad de tratamiento de datos que el presente caso. Conforme a las directrices del Comité Europeo de Protección de Datos sobre el cálculo de multas administrativas bajo el RGPD[20], la gestión indebida de categorías de datos que demandan una protección intensificada, como aquellos cuya exposición podría generar daños o molestias directas a la persona afectada (incluyendo datos de localización, información sobre comunicaciones privadas o números de identificación nacionales), requiere una aplicación más estricta de sanciones. En este caso, la AEPD podría haber también apercibido al Grupo Municipal del Partido Popular en Vélez-Málaga por una posible infracción de los artículos 9 y 10 del RGPD, que abordan categorías especiales de datos, siguiendo las recomendaciones del Comité Europeo. No obstante, a pesar de la relevancia de este aspecto en un entorno político, no se hizo mención específica al respecto.

3.1.3. Ejercicio de derechos de los interesados

a) Resolución EXP202303720: Dirección General de la Policía

En la resolución del expediente número EXP202303720, la Agencia Española de Protección de Datos se ocupó de una reclamación presentada por un ciudadano en relación con el ejercicio de su derecho de acceso a datos personales. La reclamación se dirigía contra la Dirección General de la Policía por no haber recibido respuesta a una solicitud de acceso a grabaciones de videovigilancia de unas dependencias policiales en Sevilla.

El ciudadano, identificado como A.A.A., había solicitado acceso a las grabaciones el 3 de agosto de 2022 y, aunque inicialmente se le indicó que su petición había sido transferida al departamento correspondiente, no recibió más información dentro del plazo legal establecido. La Dirección General de la Policía, por su parte, justificó su falta de respuesta argumentando que las grabaciones solicitadas estaban vinculadas a diligencias policiales y judiciales en curso, y que por tanto no podían proporcionarse directamente al solicitante, sino que estarían a disposición de la autoridad judicial competente en caso de ser requeridas.

[20] Directrices 04/2022, del Comité Europeo de Protección de Datos, sobre el cálculo de multas administrativas bajo el RGPD. Última actualización: Versión 2.1 del 24 de mayo 2023.

La AEPD, tras examinar el escrito de la Dirección General de la Policía y no haber recibido alegaciones por parte del reclamante, determinó que la respuesta proporcionada no se justificaba adecuadamente conforme a los supuestos legales que permiten denegar el derecho de acceso. La Agencia instó a la Dirección General de la Policía a que, dentro de un plazo de diez días hábiles tras la notificación de la resolución, atendiera el derecho de acceso solicitado o que lo denegara de forma motivada, indicando las causas por las cuales no procede atender la petición, según lo dispuesto en el artículo 24 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos para fines penales.

La resolución de la AEPD destaca la importancia de que las solicitudes de acceso a datos personales sean atendidas de manera oportuna y adecuada por los responsables de tratamiento. También enfatizó que cualquier restricción a este derecho debe comunicarse de manera adecuada al interesado, incluyendo las razones de la restricción y las posibilidades de presentar una reclamación ante la autoridad competente, según lo estipulado por el mismo artículo 22 y el artículo 24 de la Ley Orgánica 7/2021.

El incumplimiento de plazos límite o falta de respuesta respecto a solicitudes de derecho de acceso de los interesados es una de las causas más comunes de apercibimientos por parte de la AEPD a ayuntamientos (junto con la falta de designación de un delegado de Protección de Datos), según la Memoria 2022 de la AEPD.[21]

3.2. Aplicación práctica en el sector privado: Empresas y personas físicas

El ámbito de la protección de datos en España, especialmente en el sector privado, refleja un panorama contrastante y desafiante. España se destaca en la Unión Europea por ser el país que más sanciones impone a los negocios por incumplimientos del Reglamento General de Protección de Datos (CASAL TAVASCI 2023). Estas sanciones, que en su mayoría corresponden a faltas leves cometidas por autónomos y pequeños negocios, evidencian un escenario donde las medidas de control y penalización son rigurosas y frecuentes. En el año 2022, se impusieron sanciones por un total de 23 millones de euros, con una significativa proporción relacionada

[21] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Memoria 2022”. Disponible en: https://www.aepd.es/documento/memoria-aepd-2022.pdf

con la instalación de cámaras de videovigilancia en establecimientos comerciales (SÁNCHEZ ADELANTADO 2023). En la presente sección, se realizará un análisis detallado de algunas resoluciones destacadas emitidas por la AEPD, que ilustran de manera contundente esta postura. Estas resoluciones no solo involucran a autónomos y empresas, sino que también abarcan multas impuestas a personas físicas, demostrando que la ley de protección de datos se aplica con igual rigor tanto a entidades comerciales como a particulares.

3.2.1. Videovigilancia y captación de audio y limitación de la finalidad de tratamiento

En el ámbito de la protección de datos personales, la videovigilancia y la captación de audio constituyen áreas de particular atención y regulación. Resulta notable que, en el contexto de las intervenciones de la Agencia Española de Protección de Datos (AEPD), una proporción significativa de las multas y sanciones impuestas están vinculadas precisamente a la videovigilancia. Este hecho subraya la complejidad y la sensibilidad de este tema, en el que la seguridad y la vigilancia se cruzan constantemente con el derecho a la privacidad y la protección de datos personales. Esto es relevante no sólo para las empresas, que representan una parte considerable de las sanciones impuestas, sino también para personas físicas. A continuación, se explorarán detalladamente resoluciones clave de la AEPD que ilustran la aplicación de estos principios fundamentales.

a) Resolución PS/00314/2021: Grupo Transaher S.L.

En la resolución de Procedimiento Sancionador PS/00314/2021, la AEPD abordó una reclamación interpuesta contra el GRUPO TRANSAHER S.L. por uno de sus trabajadores, debido a la colocación de cámaras en el área del comedor, destinada al descanso de los trabajadores, y la inadecuada señalización informativa sobre la videovigilancia. El Grupo TRANSAHER, tras ser notificado, presentó un análisis detallado justificando la necesidad de las cámaras por motivos de seguridad: dada la naturaleza de su negocio de transporte y logística y la alta afluencia de personas en sus instalaciones. Afirmó que la instalación era proporcionada y que se había informado debidamente tanto al Comité de Empresa como a los trabajadores sobre la existencia del sistema de videovigilancia. Pese a no poseer carteles que informasen adecuadamente la base legitimadora del tratamiento, el GRUPO TRANSAHER defendió que sí poseían de señalización genérica indicando la existencia de cámaras de

vigilancia. La AEPD, al resolver el caso, impuso una sanción económica al GRUPO TRANSAHER por infracción del artículo 6 del RGPD, categorizada como muy grave según el artículo 72.1.b) de la LOPDGDD, y determinó una multa de 50.000 euros. Además, ordenó a la entidad que en un plazo de un mes adoptara las medidas necesarias para adecuar su actuación a la normativa de protección de datos, debiendo informar a la Agencia sobre el cumplimiento de las medidas impuestas.

La empresa GRUPO TRANSAHER defendió la instalación de cámaras de videovigilancia en el área de comedor argumentando que no se trataba de un espacio exclusivo para el descanso y esparcimiento de los trabajadores, sino de una zona de alto tráfico que incluía a personas no pertenecientes al personal interno, como autónomos. Además, la empresa justificaba esta medida de seguridad en respuesta a robos significativos ocurridos anteriormente en esa área, especialmente de máquinas expendedoras, situación que era de conocimiento general entre los empleados. Sin embargo, la Agencia Española de Protección de Datos (AEPD) sostuvo que, independientemente de que el comedor no fuera de uso exclusivo de los empleados y a pesar de los robos previos, la captura de imágenes excedía los límites establecidos por el artículo 20.3 del Estatuto de los Trabajadores. La AEPD enfatizó que el uso compartido del comedor por terceros no disminuye la protección legal de los trabajadores en cuanto a su derecho a la intimidad en zonas de descanso.

Esta decisión de la AEPD subraya el compromiso con la protección de los datos personales de los trabajadores, aunque la prohibición de videovigilar áreas comunes podría verse como excesiva, salvo en espacios privados como baños y vestuarios, para preservar la dignidad de las personas. Mientras que GRUPO TRANSAHER intentaba proteger sus bienes, debió haber sido más explícito sobre los detalles y límites de la videovigilancia. La necesidad de supervisar espacios comunes, ante el riesgo de robos, requiere una reflexión para conciliar las necesidades de seguridad de las empresas con los derechos de los empleados, enfatizando la proporcionalidad y la claridad en tales medidas para minimizar su impacto en la privacidad y dignidad de los trabajadores.

b) Resolución EXP202202563: SUPERCOR S.A.

La AEPD tomó un enfoque similar en la resolución del procedimiento sancionador del expediente EXP202202563.La Agencia Española de Protección de Datos resolvió un caso en el que dos ex empleadas de la empresa reclamada, identificadas como A.A.A. y B.B.B.,

presentaron reclamaciones contra SUPERCOR, S.A. debido al uso indebido de sistemas de videovigilancia. Las reclamantes alegaron que fueron despedidas basándose en imágenes captadas por cámaras de seguridad en áreas no informadas, específicamente en un "cuarto de descanso", lo que consideraban una violación del artículo 20.3 del Estatuto de los Trabajadores y de la doctrina del Tribunal Constitucional, en relación con los derechos fundamentales de los trabajadores. SUPERCOR argumentó que había informado adecuadamente sobre la videovigilancia y que las cámaras estaban destinadas a garantizar la seguridad y controlar la actividad laboral. La empresa también destacó que las medidas técnicas y organizativas aseguraban la seguridad de las imágenes captadas y que las imágenes se conservaban por un periodo menor al máximo legal. Asimismo, SUPERCOR aclaró que el espacio en cuestión era una "Sala de Mermas" y no un cuarto de descanso, utilizado unilateralmente por los trabajadores para ese fin. La AEPD, tras analizar la documentación y los argumentos presentados, concluyó que SUPERCOR cometió una infracción del artículo 6 del RGPD, al carecer de base jurídica legítima para el tratamiento de los datos personales captados (imágenes de las empleadas) en un espacio destinado al descanso. La Agencia determinó que la instalación de la cámara en dicha sala no cumplía con los requisitos de proporcionalidad y necesidad, infringiendo así la normativa de protección de datos y el Estatuto de los Trabajadores. En su resolución, la AEPD impuso a SUPERCOR, S.A. una sanción de 70.000 euros, basándose en la tipificación de la infracción como muy grave.

Esta resolución subraya la necesidad de adherirse estrictamente a las normativas de protección de datos, especialmente en contextos laborales con videovigilancia que incide en los derechos de los empleados. Se critica a una empresa por no definir claramente el uso de espacios comunes, donde se vigilaba un área de descanso también usada para almacenar productos, bajo la sospecha de sustracción indebida por parte de empleados. La AEPD sugiere que las empresas deben designar áreas específicas para el descanso de los trabajadores para evitar conflictos con la vigilancia de sus bienes. Esto apunta a la necesidad de que las empresas revisen sus prácticas de monitoreo para cumplir con la legislación y las directrices de la AEPD, especialmente en lo que respecta a la videovigilancia en lugares de trabajo, promoviendo un equilibrio entre las necesidades de seguridad de la empresa y la privacidad de los trabajadores.

c) Resolución PS/00120/2021: Mercadona S.A.

En otra resolución reciente, la Agencia Española de Protección de Datos (AEPD) impuso una sanción a Mercadona, S.A por diversas infracciones relacionadas con la implementación de un sistema de reconocimiento facial en varias de sus tiendas, según el procedimiento PS/00120/2021. La multa inicial de 3,15 millones de euros se redujo a 2,52 millones tras aplicar un descuento por pago voluntario. El contexto del caso revela que Mercadona, una empresa con una significativa presencia en España (1.636 tiendas y unos 95.000 trabajadores), había desplegado un sistema de reconocimiento facial para identificar y prevenir el acceso de personas condenadas con órdenes de alejamiento de sus instalaciones. Este sistema, altamente sofisticado, capturaba datos biométricos de todas las personas que ingresaban a sus tiendas y los comparaba con una base de datos para detectar a individuos sujetos a restricciones judiciales.

La AEPD determinó que Mercadona infringió varios artículos del Reglamento General de Protección de Datos (RGPD), incluyendo el tratamiento de categorías especiales de datos personales (art. 9), la licitud del tratamiento (art. 6), el principio de minimización de datos (art. 5.1.c), la transparencia (art. 12 y 13), la protección de datos desde el diseño (art. 25), y la evaluación de impacto relativa a la protección de datos (art. 35). El análisis de la AEPD se centró en dos aspectos clave: la naturaleza de los datos biométricos como categoría especial de datos personales y la legitimación del tratamiento de estos datos. Se concluyó que el sistema de reconocimiento facial de Mercadona no solo capturaba información de las personas condenadas, sino también de clientes y empleados inocentes, lo que no se justificaba bajo la excepción del art. 9.2.f del RGPD. Además, la AEPD argumentó que la finalidad del sistema no protegía un interés público esencial como defendía la parte reclamada, sino intereses privados de Mercadona, lo que invalidaba la legitimación del tratamiento basada en el interés público según el art. 6.1.e del RGPD. La decisión de la AEPD no solo impuso una multa económica significativa, sino que también ordenó a Mercadona prohibir todo tratamiento de datos personales relacionado con el reconocimiento facial en sus establecimientos. Este caso destaca la importancia de garantizar que los sistemas de vigilancia y seguridad implementados por las empresas cumplan estrictamente con las normas de protección de datos, especialmente cuando involucran tecnologías avanzadas como el reconocimiento facial.

Esta resolución se ha convertido en un referente importante para futuras deliberaciones y posibles reformas legislativas, marcando un precedente en el balance entre la implementación de medidas de seguridad y la protección de la privacidad individual (JORGE GARCÍA HERRERO 2023). Este caso subraya el desafío inherente a justificar el uso de datos biométricos bajo la premisa de "interés público" cuando, en realidad, se persiguen intereses corporativos privados. La decisión de la AEPD refleja una postura firme: el uso de reconocimiento facial por una empresa privada, en este contexto, no responde a un interés público esencial, sino que sirve a propósitos corporativos. Esta situación contrasta con la perspectiva de que las empresas podrían, en teoría, justificar el uso de reconocimiento facial si este se alinea con un interés público significativo. Sin embargo, el caso de Mercadona demuestra que es sumamente difícil para una entidad privada probar que su uso de tecnologías invasivas responde a un interés público, especialmente cuando estos sistemas capturan datos de individuos que no están directamente implicados en las actividades de interés público, como es el caso de los clientes y empleados comunes. La Ley 5/2014 de Seguridad Privada y la Ley Orgánica 4/1997 sobre el uso de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado, proporcionan cierto marco normativo, pero no abordan de manera específica la utilización de tecnologías de reconocimiento facial por parte de la seguridad privada. Esto deja un vacío legal que las empresas podrían intentar aprovechar, pero como muestra la resolución de la AEPD, cualquier intento de este tipo es sujeto a un escrutinio riguroso y una evaluación basada en los principios del RGPD. Por lo tanto, se pone de manifiesto la necesidad de una legislación más clara y detallada que aborde específicamente el uso de tecnologías de reconocimiento facial por parte de empresas privadas.

d) Resolución EXP202208166: Persona física

En contraste, en la resolución de procedimiento sancionador del expediente EXP202208166, la AEPD resolvió sobre una reclamación por parte de una persona física (el reclamante, identificado como A.A.A.) hacia otra persona física, un vecino (el reclamado, identificado como B.B.B.), por la instalación de un sistema de videovigilancia que aparentemente infringía el principio de minimización de datos del artículo 5.1.c del RGPD. La reclamación se basó en que la cámara, instalada en un mástil en la propiedad de B.B.B., podía captar imágenes de la finca contigua perteneciente a A.A.A. sin su beneplácito. A.A.A. proporcionó un reportaje

fotográfico como prueba. La AEPD realizó varios intentos de notificación a B.B.B. a diferentes direcciones, incluyendo la dirección del padrón y la Agencia Española de Administración Tributaria, todos sin éxito. Tras no recibir respuesta de B.B.B., la AEPD admitió a trámite la reclamación. En febrero de 2023, la AEPD inició un procedimiento sancionador contra B.B.B. por la presunta infracción del Artículo 5.1.c del RGPD, considerando que el uso de la cámara de videovigilancia podría no cumplir con los principios de minimización de datos, dado que las imágenes captadas podrían incluir espacios privativos del reclamante. Este principio exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario para los fines para los que son tratados. Dado que B.B.B. no presentó alegaciones, el acuerdo de inicio del procedimiento sancionador fue considerado como propuesta de resolución. La AEPD resolvió imponer a B.B.B. una multa de 300 euros por la infracción. Además, ordenó a B.B.B. reorientar o retirar el sistema de videovigilancia para asegurar que no se captaran imágenes de la propiedad de A.A.A., zonas comunes de la vivienda o la vía pública. La AEPD subrayó que la inobservancia de estos requerimientos podría conllevar procedimientos sancionadores adicionales conforme al RGPD.

Esta reciente resolución de la AEPD resalta un aspecto crucial del RGPD: la responsabilidad de los individuos en el tratamiento de datos personales de terceros, evidenciando que las obligaciones del RGPD no se limitan solo a entidades o empresas, sino que también aplican a personas físicas. Según el artículo 2.c del RGPD, el tratamiento de datos personales se escapa de la esfera del "uso doméstico" cuando su finalidad se extiende más allá del ámbito personal o familiar. Aunque la instalación de cámaras de vigilancia puede considerarse inicialmente como una medida de seguridad doméstica, la captación de imágenes que exceden los límites de la propiedad propia desencadena una responsabilidad bajo el RGPD. Esto se debe a que dicha práctica implica el tratamiento de datos personales (en este caso, imágenes) de individuos externos sin su consentimiento. La AEPD, al aplicar esta interpretación, subraya que la frontera entre el uso doméstico y la responsabilidad bajo el RGPD puede cruzarse incluso en actividades cotidianas como la instalación de sistemas de seguridad, siempre que dichas actividades impliquen un tratamiento de datos personales que afecte a terceros.

e) Resolución EXP202211675: Persona física

La resolución de procedimiento sancionador del expediente EXP202211675 presentó una situación similar. La Agencia Española de Protección de Datos abordó una reclamación

presentada por el reclamante identificado como A.A.A., contra el reclamado identificado como B.B.B., quien fue sancionado por la instalación inapropiada de una cámara de videovigilancia. La queja se centró en que dicha cámara, instalada en la fachada de un inmueble de B.B.B., estaba orientada hacia la vía pública, sin contar con la autorización administrativa necesaria. A pesar de los esfuerzos de la AEPD por obtener una justificación de B.B.B., este no proporcionó respuesta alguna. La resolución de la AEPD se fundamentó en la infracción del principio de minimización de datos del contemplado en el artículo 5.1.c del RGPD. Este principio implica que cualquier tratamiento de datos debe limitarse a lo estrictamente necesario para cumplir con sus objetivos. En este caso, la cámara de B.B.B. excedió el ámbito necesario al captar imágenes de la vía pública, lo cual no solo es innecesario para la seguridad del inmueble sino también una intrusión en la privacidad de terceros.

El caso también invocó la Ley Orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Dicha ley establece que la vigilancia de espacios públicos a través de cámaras es una competencia exclusiva de las autoridades estatales, por lo que cualquier instalación por parte de particulares que capture imágenes de estos espacios resulta no solo inadecuada sino también ilegal. La AEPD determinó que la cámara de B.B.B. estaba incorrectamente orientada, captando zonas no permitidas y, por lo tanto, ordenó su reorientación o retirada. Este ajuste debía asegurar que solo se captaran imágenes del espacio privativo de B.B.B., evitando la intimidación a vecinos colindantes y la captación de imágenes del espacio público.

La sanción impuesta fue de 300 euros, considerada en el extremo inferior del espectro de sanciones para este tipo de conductas. Esta cifra refleja tanto la gravedad de la infracción como la falta de respuesta de B.B.B. a los requerimientos de la Agencia. Adicionalmente, la AEPD dictó una orden para que B.B.B. demostrara, en un plazo de 10 días hábiles, haber reorientado o retirado la cámara, proporcionando documentación fotográfica que evidenciara dicha acción. Este expediente destaca la importancia de que los sistemas de videovigilancia instalados por particulares se adhieran estrictamente a la normativa de protección de datos y legislación específica sobre videovigilancia, subrayando la responsabilidad de los particulares en el tratamiento de datos personales y en el respeto a la privacidad de terceros y al espacio público.

3.2.2. Licitud del tratamiento, integridad y confidencialidad

a) Resolución PS/00340/2021: Vodafone España S.A.U.

En su resolución PS/00340/2021, la Agencia Española de Protección de Datos La Agencia Española de Protección de Datos (AEPD) multó a VODAFONE con 100.000 euros por tratar los datos personales de una cliente, A.A.A., sin base legal, tras asociarla erróneamente a una línea telefónica usada en estafas online. A pesar de que VODAFONE alegó haber cumplido con las obligaciones legales de identificación del comprador de la tarjeta prepago, según la Ley 25/2007, la AEPD determinó que la verificación de la identidad del comprador no fue adecuada, resultando en un tratamiento ilícito de datos. La ley exige la verificación de identidad para prevenir el uso delictivo de servicios telefónicos, lo cual VODAFONE no respetó al no confirmar correctamente la identidad del comprador. La acción de la Guardia Civil, basada en una investigación penal, no fue considerada infracción por la AEPD, enfatizando la importancia de medidas técnicas y organizativas apropiadas por parte de las empresas para asegurar una gestión adecuada de los datos personales.

Esta resolución de la AEPD enfatiza la responsabilidad de las empresas de telecomunicaciones de gestionar adecuadamente los datos personales y asegurarse de que las medidas de verificación de identidad sean eficaces para prevenir el uso indebido de datos en la contratación de servicios. La interpretación que la AEPD hace de la disposición Adicional Única de la Ley 25/2007 es fundamental, pues establece con claridad lo que constituye una identificación inequívoca en el marco de las responsabilidades de cooperación policial dictadas por dicha ley, y cómo esto se interrelaciona con los requisitos del RGPD. La sanción impuesta a VODAFONE por las deficiencias en sus medidas de verificación de identidad resalta la significativa responsabilidad que recae sobre las empresas de telecomunicaciones. Aunque la investigación policial reveló un uso fraudulento de los datos asociados a una tarjeta SIM, es la empresa operadora la que tuvo el deber principal de asegurar una verificación rigurosa de la identidad al ofrecer sus servicios. En el sector privado, es menos común encontrar empresas sujetas a tan extensivas obligaciones de cooperación con las autoridades. La mayoría de los servicios privados no están intrínsecamente ligados a responsabilidades de colaboración tan amplias y rigurosas. Este caso subraya la expectativa de que las teleoperadoras implementen mecanismos robustos para prevenir el mal uso de datos personales y resalta la importancia

de una colaboración efectiva con las autoridades sin comprometer la protección de datos de los individuos.

b) Resolución EXP202201254: Pelayo Mutua de Seguros y Reaseguros S.L.

Otra resolución relevante respecto al principio de confidencialidad del tratamiento fue la resolución del expediente EXP202201254. La Agencia Española de Protección de Datos inició un procedimiento sancionador contra Pelayo Mutua de Seguros y Reaseguros a Prima Fija, tras una reclamación presentada por una ciudadana, identificada como A.A.A. La reclamante acusó a la aseguradora de divulgar sin su consentimiento datos personales y de su póliza de seguro a un tercero, identificado en documentos como "B.B.B. comprador". Este incidente ocurrió en una oficina de la aseguradora, donde se entregó al tercero un documento que contenía información detallada sobre la reclamante y su póliza de seguro.

Pelayo argumentó que los datos fueron compartidos basándose en el interés legítimo del tercero, quien poseía un contrato de arras con la reclamante para la compra de su vehículo asegurado. Además, la aseguradora destacó que la información fue proporcionada por un empleado de un agente, y no directamente por ella. La AEPD, tras realizar investigaciones preliminares, determinó que Pelayo era responsable del tratamiento de datos en este caso. Se consideró que la aseguradora no ejerció la debida diligencia para asegurar que el tratamiento de datos estaba justificado y cumplía con los requisitos legales del RGPD. En particular, se identificó una infracción del principio de confidencialidad del artículo 5.1.f del RGPD. El procedimiento sancionador contempló dos presuntas infracciones: una del artículo 5.1.f del RGPD, relacionada con el principio de confidencialidad, y otra del artículo 32 del RGPD, relacionada con la seguridad del tratamiento. Se propusieron sanciones de 50.000 euros y 20.000 euros respectivamente, sumando un total de 70.000 euros.

La sanción impuesta por la AEPD a Pelayo Mutua de Seguros y Reaseguros a Prima Fija fue particularmente severa, ya que la AEPD enfatizó la sensibilidad del DNI como un tipo de dato que requiere protección especial bajo el RGPD. Según el artículo 10 del RGPD, y reflejado en las Directrices 4/2022[22] , los datos como el DNI merecen una consideración y protección más rigurosas, justificando así respuestas más estrictas, incluyendo multas más elevadas en casos

[22] Directrices 04/2022, del Comité Europeo de Protección de Datos, sobre el cálculo de multas administrativas bajo el RGPD.

de su tratamiento indebido. Esta categorización se basa en el potencial de estos datos para causar daños o inconvenientes significativos al interesado en caso de divulgación. Además, la AEPD subrayó que la gravedad de una infracción aumenta con el volumen de datos sensibles involucrados. En este caso, la divulgación por parte de Pelayo de un documento con múltiples datos personales del reclamante, incluyendo su DNI, nombre, apellidos, domicilio, teléfono, y detalles de la póliza de seguro y siniestros, representó una violación significativa del principio de protección de datos, lo que llevó a una penalización acorde con la sensibilidad y cantidad de los datos comprometidos.

c) Resolución PS/00116/2021: Avalos Consultores S.L.

Finalmente, considerando el principio de licitud del tratamiento, se analiza a continuación la resolución de procedimiento sancionador PS/00116/2021. La Agencia Española de Protección de Datos abordó una reclamación presentada por la reclamante, identificada como. A.A.A. contra Avalos Consultores, S.L. La reclamante denunció que Avalos Consultores había compartido sus datos personales con Torrent Asesores Nga, S.L. sin su consentimiento. Este hecho se verificó a través de documentación que incluía facturas de 2017 y 2020, y un correo electrónico donde la reclamante expresaba su desconocimiento y desaprobación de dicho traspaso de información. La AEPD determinó que Avalos Consultores era el responsable del tratamiento de datos en cuestión. A pesar de varios intentos de notificación y requerimientos de información a Avalos Consultores, la empresa no respondió ni colaboró con la AEPD. Se constató que Avalos Consultores había transferido los datos personales de la reclamante a un tercero sin una base legal para dicho tratamiento, violando así el artículo 6 del RGPD, que establece las condiciones de licitud del tratamiento de datos. Considerando la falta de cooperación de la empresa y la naturaleza de los datos personales afectados, la AEPD impuso una multa de 4.000 euros a Avalos Consultores por infringir el artículo 6 del RGPD.

Los hechos iniciales indicaban a pensar que el tratamiento en cuestión se había tratado de un traslado del expediente de la reclamante por parte del reclamado a otra gestoría. Pese a que esta práctica podría haber estado totalmente motivada por un propósito genuino de negocio, la falta de notificación de este tanto a la reclamante como al la AEPD agravó las circunstancias. Esta resolución es un ejemplo de cuán crucial es para las empresas responder a la AEPD con la mayor brevedad posible. Al tratarse de una empresa pequeña unipersonal, la multa correspondiente, pese a la falta de cooperación, se trató de una cantidad pequeña. En el

ámbito de las PYMES, la AEPD opta en la medida de lo posible, por medidas correctivas y educativas[23]. Aun así, también supone un buen ejemplo de cómo este tipo de errores en la gestión del fichero de los clientes por parte de pequeñas empresas puede tener impacto en su economía.

3.2.3. Ejercicio de derechos de los interesados

A pesar de que la omisión en responder a las solicitudes de ejercicio de derechos del interesado es una falta frecuentemente observada en el ámbito empresarial, la Agencia Española de Protección de Datos (AEPD) no acostumbra a imponer multas directas por estas omisiones. En su lugar, la AEPD opta mayoritariamente por iniciar procedimientos de tutela, exhortando a las empresas implicadas a dar respuesta adecuada a las peticiones de los interesados, siempre que estas sean pertinentes y legítimas (GONZÁLEZ TAPIA 2023). Esta práctica subraya un enfoque más orientado a la corrección y al cumplimiento que a la penalización. No obstante, es notable mencionar que la rigurosidad en el tratamiento de estas reclamaciones tiende a intensificarse en casos de reclamaciones transfronterizas, donde la dimensión internacional y la cooperación entre distintas autoridades de protección de datos de la UE añaden una capa adicional de complejidad y gravedad al asunto.

a) Resolución PS/00003/2021: Page Group Europe S.L.

Esto se vio evidenciado en la resolución del expediente PS/00003/2021. La Agencia Española de Protección de Datos (AEPD) resolvió sobre una reclamación iniciada por la reclamante, identificada como A.A.A. ante la Autoridad de Protección de Datos de los Países Bajos contra Michael Page International, una empresa con sede en Reino Unido. Este caso fue transferido a la AEPD debido a que el equipo de Cumplimiento Legal responsable de gestionar las solicitudes de acceso en Europa continental está ubicado en España, en la filial PAGE GROUP EUROPE, S.L. La reclamante, una ciudadana holandesa, había enviado su CV a través del portal web de la empresa en los Países Bajos. Posteriormente, solicitó acceso a sus datos personales, pero Michael Page International solicitó inicialmente documentación adicional para confirmar

[23] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Orientación a Pequeñas y Medianas Empresas (PYMES)”. 12 de julio 2021. Disponible en: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/pymes

su identidad, lo cual la reclamante consideró excesivo. Aunque la empresa rectificó su solicitud de documentación, la reclamante ya había iniciado un proceso de reclamación ante la autoridad holandesa. La AEPD, tras examinar el caso y tomar en cuenta las objeciones planteadas por las autoridades de protección de datos de otros países con sedes de la misma empresa, decidió admitir la reclamación para tramitación. Se identificó una presunta infracción de los artículos 5.1.c (minimización de datos) y 12 (transparencia de la comunicación) del RGPD por parte de PAGE GROUP EUROPE, por lo que la AEPD propuso sancionar a la empresa con 250.000 euros y con 50.000 euros por la infracción de cada artículo respectivamente, totalizando una multa propuesta de 300.000 euros. PAGE GROUP EUROPE presentó alegaciones solicitando el archivo del procedimiento o una reconsideración de la multa. Argumentaron que su proceso de verificación de identidad tenía como objetivo proteger los datos personales y evitar su cesión a terceros no autorizados. La empresa también destacó su buena fe y su intención de cumplir con la normativa. La AEPD emitió una propuesta de resolución sancionando a PAGE GROUP EUROPE con una multa total de 300.000 euros, dividida en 250.000 euros por el incumplimiento del artículo 5.1. y 50.000 euros por el artículo 12, del RGPD. La entidad aprovechó la reducción por pronto pago, abonando un total de 240.000 euros.

La sanción impuesta por la AEPD a la empresa por su inadecuada gestión en la verificación de identidad, en contraposición a los principios de minimización de datos y transparencia, subraya la imperiosa necesidad de una guía más clara para las multinacionales con operaciones en España. Este caso ilustra cómo la identificación de un individuo, basada únicamente en medidas técnicas y organizativas como el registro de comunicaciones, correo electrónico o teléfono, puede variar significativamente dependiendo del contexto y de las jurisdicciones involucradas.

4. Conclusiones

El presente Trabajo de Fin de Grado ha abordado un exhaustivo análisis del marco regulatorio español en materia de protección de datos, tanto en el ámbito público como en el privado. A lo largo de esta investigación, se ha evidenciado la complejidad y la amplitud de las leyes que rigen este sector, destacando que, más allá del Reglamento General de Protección de Datos

(RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), existen múltiples normativas que inciden específicamente en contextos como el penal o la seguridad ciudadana.

Una conclusión clave de este estudio es la constatación de una tendencia hacia la armonización en el entramado legislativo español en materia de protección de datos. Esta homogeneización se manifiesta en la adopción de principios comunes como la licitud, la proporcionalidad, la minimización y la limitación del tratamiento de datos personales por la mayoría de las leyes aquí analizadas. Esta cohesión normativa refleja el principio constitucional de supremacía de la ley, en el que nadie, incluidas las instituciones estatales, está por encima del derecho a la privacidad de los datos personales.

4.1. Tendencias y recomendaciones sobre el cumplimiento en el ámbito público

Sin embargo, se observa una disparidad notable en el nivel de exigencia y rendición de cuentas entre el sector público y el privado. Mientras que el sector privado enfrenta un escrutinio y sanciones económicas significativas, las Fuerzas y Cuerpos de Seguridad del Estado y las Administraciones Públicas se benefician de la inexistencia de sanciones económicas. Esto se debe a la LOPDGDD, que, a diferencia del RGPD, no contempla multas para el sector público.

Cuando se trata de organismos públicos que no atienden a las recomendaciones o apercibimientos de la AEPD, es preciso que se empiecen a adoptar medidas más drásticas. Esta práctica reiterativa de falta de respuesta ante las instrucciones de la AEPD no solo transmite un mensaje de tolerancia hacia la inobservancia, sino que también debilita potencialmente el efecto disuasorio de las resoluciones emitidas. La ausencia de sanciones más contundentes podría inducir a un cumplimiento normativo menos riguroso por parte de otras administraciones, minimizando así la eficacia y el alcance de la labor que la AEPD desempeña en cada uno de sus veredictos. La aparente inmunidad del sector público frente a las sanciones económicas contrasta significativamente con la rigurosidad aplicada en el sector privado, sugiriendo una dualidad en la aplicación de la ley que plantea interrogantes sobre la coherencia y equidad en la aplicación de las normativas en todos los sectores.

La efectividad del marco regulatorio de protección de datos se fortalece a través de la implementación y el respeto de sus disposiciones por parte de todas las instituciones, lo que

incluye la imposición de medidas correctivas proporcionales que refuercen el compromiso con la privacidad y protección de datos personales. Esta situación contrasta con prácticas en otros países, como el Reino Unido, donde, según un enfoque revisado por la Oficina del Comisionado de Información (ICO), se estaban imponiendo demasiadas sanciones económicas en el sector público (JOHN EDWARDS 2022[24]). Por ello, habría surgido una necesidad de menguar las instancias en las cuales sería aplicable la sanción monetaria, complementándolas con medidas centradas en educar a dichos organismos en mejores prácticas cuando se tratase de órganos no reincidentes, adoptando así un enfoque más colaborativo y efectivo en el cumplimiento del sector público. Todo ello parece indicar que es crucial encontrar un equilibrio entre la postura tradicional y una posible sobrecarga regulatoria en el ámbito público. Evocando a ADJUARA VARELA (2019), la ejemplaridad pública es crucial en materia de protección de datos debido a la naturaleza sensible de los datos que manejan y el potencial de perjuicio mayor para la ciudadanía por posibles infracciones. Siempre que se haga de manera proporcional, la imposición de sanciones económicas a las administraciones públicas no perjudicaría al contribuyente (ya que lo recaudado por estas multas se destinarían al Tesoro, reduciendo el déficit público), sino que sólo obligarían a las administraciones a ser más responsables y eficientes en la gestión de sus recursos.

En la actualidad, no existen iniciativas para modificar el límite impuesto por el artículo 77 de la LOPDGDD. Sin embargo, el pasado 5 de septiembre del 2023 la Agencia Española de Protección de datos incluyó una actualización significativa en su página web, sobre las sanciones impuestas a distintas Administraciones Públicas[25]. Se trata de un nuevo apartado de su sitio web donde se hacen visibles las Administraciones Públicas sancionadas de manera repetitiva por no atender órdenes o por incumplir medidas correctivas impuestas. Esta actualización supone un avance significativo hacia una mayor transparencia y responsabilidad en el sector público, y refleja un intento de equilibrar la disparidad en la rendición de cuentas entre los sectores público y privado. Al hacer públicas estas infracciones, la AEPD no solo

[24] INFORMATION COMMISSIONER'S OFFICE, "Open letter from UK Information Commissioner John Edwards to public authorities". 30 de Junio 2022. Disponible en: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/

[25] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas". 5 septiembre de 2023. Disponible en: https://www.aepd.es/areas-de-actuacion/administraciones-publicas/administraciones-publicas-sancionadas

aumenta la presión sobre las Administraciones Públicas para que mejoren su gestión de datos, sino que también informa a los ciudadanos sobre cómo se manejan sus datos personales.

4.2. Tendencias y recomendaciones sobre el cumplimiento en el ámbito privado

En el sector privado, aunque aún hay margen de mejora, se percibe un creciente reconocimiento de la importancia de la privacidad desde el diseño. La Agencia Española de Protección de Datos (AEPD) ha jugado un papel crucial en este cambio, siendo una de las autoridades más activas en Europa en materia de amonestaciones y creación de precedentes.

Una reciente modificación de la Ley Orgánica 3/2018, publicada en el Boletín Oficial del Estado, introdujo cambios sustanciales para las actuaciones de la AEPD. Esta actualización aborda principalmente dos aspectos: la redefinición del apercibimiento como una medida correctiva no sancionadora, en concordancia con el Reglamento General de Protección de Datos (RGPD), y la adaptación de los procedimientos de investigación y reclamación a la era digital. Entre los cambios más relevantes se incluyen la creación del procedimiento de apercibimiento específico, con una duración máxima de seis meses, y la implementación de sistemas digitales para las investigaciones y presentaciones de reclamaciones, facilitando así procesos más rápidos y accesibles.

Esta reforma legislativa tiene implicaciones particulares para las pequeñas y medianas empresas (PYMES), que históricamente han enfrentado desafíos significativos en el cumplimiento de las normativas de protección de datos, a menudo resultando en sanciones económicas por parte de la AEPD. La modificación de la ley, al redefinir el apercibimiento como una medida no sancionadora, podría aliviar la carga económica sobre las PYMES. Este cambio sugiere un enfoque más orientado hacia la educación y la corrección, en lugar de la penalización, lo cual es especialmente relevante para las PYMES que, debido a sus recursos limitados, pueden encontrar mayores dificultades para cumplir plenamente con las regulaciones de protección de datos. Además, la introducción de sistemas digitales para la gestión de investigaciones y reclamaciones puede resultar en un proceso más eficiente y menos oneroso para estas empresas. Esto no solo agiliza la resolución de los casos, sino que también facilita a las PYMES el cumplimiento de sus obligaciones, al proporcionarles herramientas más accesibles y claras.

Pese a que el marco regulatorio español en protección de datos personales avanza hacia una mayor coherencia y eficacia, persisten desafíos significativos. Por un lado, España se destaca como uno de los más severos en Europa en la imposición de multas en el sector privado, aplicando sanciones rigurosas a una amplia gama de actores, desde grandes corporaciones hasta personas físicas. Por otro lado, existe una marcada indulgencia hacia el sector público, donde las administraciones públicas parecen gozar de una especie de inmunidad frente a sanciones económicas por infracciones en materia de protección de datos. Esto señala una tendencia preocupante: existe la posibilidad de que nuestros datos personales estén, eventualmente, más seguros en manos de entidades privadas, impulsadas por imperativos económicos y sometidas a una regulación estricta, que bajo la custodia de organismos públicos. Paradójicamente, se esperaría que estas últimas entidades, dada su responsabilidad en la protección del bien común y los derechos individuales, aplicaran un tratamiento de datos con mayor rigor y responsabilidad.

Esta perspectiva, aunque pueda parecer inesperada, se ve respaldada por el análisis de casos como el Procedimiento Nº AP/00055/2017, en la que se efectuó un seguimiento mínimo para la gravedad de los hechos denunciados, como la venta de datos personales por parte de un policía y un funcionario municipal. Este caso evidencia que la preocupación por un trato desigual en la protección de datos entre sectores no es infundada.

No obstante, a lo largo de este estudio se destaca una evolución constante del marco jurídico en España, marcada por la actuación proactiva de la Agencia Española de Protección de Datos (AEPD) y la creación de la Agencia Española de Supervisión de Inteligencia Artificial (AESIA)[26] reflejando la adaptación del país a las nuevas tecnologías y desafíos digitales. La transformación digital, impulsada por leyes europeas como la Ley de Mercados Digitales 2022[27] y la Ley de Servicios Digitales 2022[28], busca establecer un entorno digital ético y

[26] Orden PCM/1203/2022, de 5 de diciembre, por la que se publica el Acuerdo del Consejo de Ministros de 5 de diciembre de 2022, por el que se determina la sede física de la futura Agencia Española de Supervisión de Inteligencia Artificial. *Boletín Oficial del Estado,* núm. 292, de 6 de diciembre de 2022, páginas 167580 a 167615.
[27] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).
[28] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

sostenible. España, con una infraestructura digital avanzada, se posiciona como líder en conectividad en Europa (RODRÍGUEZ CANFRANC 2023), lo que facilita su transformación digital. La tendencia hacia la privacidad por diseño indica un cambio hacia la innovación responsable, sugiriendo un futuro en el que la regulación equilibre innovación tecnológica y protección de derechos digitales.

Aunque el cumplimiento a menudo se impulsa por el temor a las fuertes multas de la AEPD, existe un cambio prometedor en el horizonte. Cada vez más, la adopción de la privacidad por diseño se reconoce no solo como un medio para eludir multas, sino como la estrategia más sostenible para fomentar la innovación. Las empresas se enfrentan a la necesidad de adaptarse a un entorno digital en constante evolución, donde la gestión de la privacidad y la protección de datos se convierten en aspectos cruciales de su operatividad y reputación. Las tendencias actuales sugieren que el futuro de la regulación en el ámbito privado estará marcado por un equilibrio entre la promoción de la innovación tecnológica y la protección eficaz de los derechos digitales.

Referencias bibliográficas

Bibliografía básica

Libros

ÁLVAREZ GARCÍA, F. *et al. La adecuación del derecho penal español al ordenamiento de la Unión Europea.* 1ª ed. Valencia: Tirant Lo Blanch. 2009.

DÍEZ SASTRE, S. MARTÍNEZ SÁNCHEZ, C. EGEA DE HARO, A. et al. *Informe sobre la Justicia Administrativa 2019: Tributos, Contratos Públicos, Responsabilidad Patrimonial, Derechos Fundamentales, Personal de la Administración, Protección de Datos, Transparencia y Responsabilidad Contable*. 1ª ed. Madrid: Centro de Investigación sobre Justicia Administrativa de la Universidad Autónoma de Madrid (CIJA-UAM). 2019.

RODRÍGUEZ CANFRANC, P. VILLAR GARCÍA, J. TARÍN QUIRÓS, C. y BLÁZQUEZ SORIA, J. *Sociedad Digital en España 2023*. 1ª ed. Barcelona: Penguin Random House Grupo Editorial, S. A. U., 2023.

RODRÍGUEZ ROCA, A. *La protección de datos personales en los juzgados y tribunales: Un enfoque desde la perspectiva laboral*. 1ª ed. Madrid: La Ley. 2022.

Estudios académicos

BARCELONA LLOP, J. <<A propósito de la Ley Orgánica 4/1997, de 4 de agosto, llamada de videovigilancia>>. Actualidad Administrativa, Sección Doctrina, 1998, Ref. XVI, pág. 205, tomo 1, LA LEY 2162/2001, Editorial LA LEY.

BARRIO ANDRÉS, M. <<Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos>>. Wolters Kluwer, Colección Temas - La Ley, septiembre 2018.

BUENO DE MATA, F. <<Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica>>. Diario La Ley, Nº 8627, Sección Doctrina, 19 de octubre de 2015. Ref. D-382. LA LEY 5958/2015.

CARDONA RUBERT M.B. <<La privacidad del teletrabajador>>. Trabajo y Derecho, LA LEY 8903/2016, Nº 24, Sección Estudios, diciembre 2016, Wolters Kluwer.

COLOMER HERNÁNDEZ, I. <<A Propósito de la compleja trasposición de la Directiva 2016/680 relativa al tratamiento de datos personales para fines penales>>. Diario La Ley, Nº 9179, Sección Doctrina. Wolters Kluwer, 17 de abril de 2018. LA LEY 2787/2018.

DE MADRID DÁVILA, E. <<Investigación privada en el marco del compliance>>. LA LEY compliance penal. 2021, vol. 7, Sección Otras áreas de cumplimiento normativo, Cuarto trimestre.

DÍEZ ESTELLA, F. << ¿Es la privacidad un parámetro de la competencia?». Estudios de la Red Académica de Defensa de la Competencia (RADC): El derecho de la competencia y los mercados digitales>>. 1ª ed. Madrid. Diciembre 2022.

FRÍAS MARTÍNEZ, E. << Protección y tratamiento de datos personales por el Ministerio Fiscal>>. La Ley Penal, LA LEY 2859/2010, Nº 71, Sección Estudios, mayo 2010, Wolters Kluwer.

GARCÍA MIGUEL, S. <<El uso de las nuevas tecnologías en la lucha contra la delincuencia especializada>>La Ley Penal, LA LEY 2371/2020, Nº 142, Sección Derecho Procesal Penal, Enero-Febrero 2020, Wolters Kluwer.

GONZÁLEZ GUTIÉRREZ DE LEÓN, M. A.; GONZÁLEZ URDINGUIO, A. <<La videovigilancia en el sistema democrático español: Análisis y crítica de la ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos>>. Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, 1997-1998, vol. 89, pp. 105-124. LA LEY 55067/2003, Editorial LA LEY.

GONZÁLEZ TAPIA, M. L. << ¿Por qué la falta de atención de un derecho del afectado tiene consecuencias más graves cuando la reclamación se presenta fuera de España?>> LINKEDIN ARTICLES, 16 de Marzo 2023. Disponible en: https://www.linkedin.com/pulse/por-qu%C3%A9-la-falta-de-atenci%C3%B3n-un-derecho-del-afectado-gonz%C3%A1lez-tapia/?originalSubdomain=es

JORGE SANMARTÍN, S. <<El Uso De Virus Espía Como Diligencia De Investigación: Análisis Crítico Y Propuestas>>. Trabajo fin de título, Máster en Acceso a la Abogacía. 1 de diciembre 2016. Escuela de Práctica Jurídica de Salamanca.

MAGRO SERVET, V. <<Las técnicas de identificación facial por la seguridad privada y su necesidad de cobertura legal según la AEPD>> Diario La Ley, LA LEY 3898/2022, Nº 10053, Sección Doctrina, 21 de abril de 2022, Wolters Kluwer.

MARCOS AYJÓN, M. <<Las múltiples implicaciones de la protección de datos en la justicia penal>>. La Ley Penal, Nº 132, mayo-junio 2018. Wolters Kluwer. LA LEY 2894/2018.

MARTOS, F. << Consideraciones de LEY 5/2014, de 4 de abril de SEGURIDAD PRIVADA>> LINKEDIN ARTICLES, 15 marzo 2018. Disponible en: https://www.linkedin.com/pulse/consideraciones-de-ley-52014-4-abril-seguridad-martos-tello/?originalSubdomain=es.

PARDO MARQUINA, V. <<Cámaras de videovigilancia: ¿mecanismo de seguridad o intromisión en el Derecho Fundamental a la protección de datos personales?>> Diario La Ley, LA LEY 5138/2021, Nº 9855, Sección Tribuna, 21 de mayo de 2021, Wolters Kluwer.

RODRÍGUEZ FERNÁNDEZ, R. <<Protección de datos personales: normativa europea y nacional (especial referencia a la normativa de protección de datos en la prevención, detección,

investigación y enjuiciamiento de infracciones penales)>>. La Ley Penal, Nº 157, Sección Legislación aplicada a la práctica. Wolters Kluwer, julio-agosto 2022. LA LEY 7704/2022.

RODRÍGUEZ LAINZ, J.L. <<El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones>> Diario La Ley, Nº 6859, Sección Doctrina. Wolters Kluwer, 11 de enero de 2008, LA LEY 7062/2007.

SANCHIS CRESPO, C. <<Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas>>. La Ley Penal, Nº 125, Sección Estudios, marzo-abril 2017. Wolters Kluwer. LA LEY 3914/2017.

SEMPERE SAMANIEGO, J. <<Tecnología contra una pandemia: la segunda oleada>>. Derecho Digital e Innovación, LA LEY 12232/2020, Nº 6, Sección Doctrina, Tercer trimestre de 2020, Wolters Kluwer.

VILLAR FUENTES, I. <<Datos personales al servicio de la investigación y detección de infracciones penales>> Revista General de Derecho *Procesal,* ISSN-e 1696-9642, N.º. 48, 2019.

Bibliografía complementaria

Periódicos y Revistas Digitales

ADSUARA VARELA, B. "¿Por qué no se multa a las AAPP en materia de Protección de Datos?" La Información, 11 de noviembre 2019. Disponible en: https://www.lainformacion.com/opinion/borja-adsuara/por-que-no-se-multa-a-las-aapp-en-materia-de-proteccion-de-datos/6512294/

CASAL TAVASCI, J. "Estadísticas de Sanciones en el año 2022" PROTECCIÓN DATA BLOG, 02 enero 2023. Disponible en: https://protecciondata.es/estadisticas-sanciones-2022/#:~:text=Las%20estad%C3%ADsticas%20sit%C3%BAan%20a%20Espa%C3%B1a,importe%20de%2036.734.810%20%E2%82%AC.&text=A%20pesar%20de%20ser%20el,somos%20el%20que%20m%C3%A1s%20recauda.

GARCÍA, L. "Menos quejas pero más sanciones: las infracciones de la Administración pública por protección de datos" NEWTRAL, 17 de junio 2021. Disponible en: https://www.newtral.es/sanciones-administracion-proteccion-datos/20210617/

MARZO COSCULLUELA, J. "El Tribunal de Justicia de la UE anula la Directiva 2006/24/EC de conservación de datos al ser intrusiva en la vida privada" *Garrigues*, 10 de abril 2014.

Disponible en https://www.garrigues.com/es_ES/noticia/el-tribunal-de-justicia-de-la-ue-anula-la-directiva-200624ec-de-conservacion-de-datos-al-ser

GARCÍA HERRERO J. "Indemnización al trabajador por «maltrato biométrico laboral»" Jorgegarciaherrero.com, 26 de septiembre 2023. Disponible en: https://jorgegarciaherrero.com/indemnizacion-al-trabajador-por-maltrato-biometrico-laboral/

ORTEGO RUIZ M. "¿Por qué la AEPD no multa a las Administraciones Públicas?" Miguelortego.com, 29 de septiembre 2020. Disponible en: https://miguelortego.com/por-que-la-aepd-no-multa-a-las-administraciones-publicas/

SANCHEZ ADELANTADO, D. "España es el país que más sanciona a los negocios por incumplir la protección de datos: éstos son los motivos" Autónomos y Emprendedor, 1 de mayo 2023. Disponible en: https://www.autonomosyemprendedor.es/articulo/actualidad/espana-es-pais-que-mas-sanciona-negocios-incumplir-proteccion-datos-son-motivos/20230428164015030308.html

SÁNCHEZ-JARA G. "Consecuencias de imponer solo apercibimientos a las administraciones públicas por la infracción del RGPD" RGPD BLOG, 14 de octubre 2021. Disponible en: https://rgpdblog.com/consecuencias-de-imponer-solo-apercibimientos-a-las-administraciones-publicas-por-la-infraccion-del-rgpd/

VIGARIO, D. "Más de 30 afectadas, una familia con una niña víctima y otro hijo administrador del chat, 11 denuncias... el caso de fotos falsas que alarma Almendralejo". *El Mundo.* 22 de septiembre 2023. Disponible en: https://www.elmundo.es/espana/2023/09/19/6509d01be85eceaa5a8b457b.html

Otros

Pankiw, Ally (2023). En *Black Mirror* (Temporada 6, Episodio 1). Netflix Inc. Netflix. Reino Unido.

Legislación citada

Constitución Española. *Boletín Oficial del Estado*, núm. 311, de 29/12/1978.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos para fines penales

Ley Orgánica 13/2015, de modificación de la LECrim y regulación de medidas de investigación tecnológica.

Ley Orgánica 4/1997 sobre la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 07/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

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 (Reglamento general de protección de datos).

Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

Orden PCM/1203/2022, de 5 de diciembre, por la que se publica el Acuerdo del Consejo de ministros de 5 de diciembre de 2022, por el que se determina la sede física de la futura Agencia Española de Supervisión de Inteligencia Artificial. *Boletín Oficial del Estado,* núm. 292, de 6 de diciembre de 2022, páginas 167580 a 167615

Jurisprudencia referenciada

Resolución de la Agencia Española de Protección de Datos PS/00377/2021

Resolución de la Agencia Española de Protección de Datos PS/00027/2019

Resolución de la Agencia Española de Protección de Datos EXP202102430

Resolución de la Agencia Española de Protección de Datos R/00443/2018

Resolución de la Agencia Española de Protección de Datos PS/00376/2019

Resolución de la Agencia Española de Protección de Datos PS/00123/2020

Resolución de la Agencia Española de Protección de Datos PS/00388/2019

Resolución de la Agencia Española de Protección de Datos EXP202303720

Resolución de la Agencia Española de Protección de Datos PS/00040/2020

Resolución de la Agencia Española de Protección de Datos PS/00314/2021

Resolución de la Agencia Española de Protección de Datos EXP202202563

Resolución de la Agencia Española de Protección de Datos PS/00120/2021

Resolución de la Agencia Española de Protección de Datos EXP202208166

Resolución de la Agencia Española de Protección de Datos EXP202211675

Resolución de la Agencia Española de Protección de Datos PS/00340/2021

Resolución de la Agencia Española de Protección de Datos EXP202201254

Resolución de la Agencia Española de Protección de Datos PS/00116/2021

Resolución de la Agencia Española de Protección de Datos PS/00003/2021

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos

AESIA: Agencia Española de Supervisión de Inteligencia Artificial.

CNI: Centro Nacional de Inteligencia

DNI: Documento Nacional de Identidad

ICO: Information Commissioners' Office (Oficina del Comisionado de Información de Reino Unido).

INCIBE: Instituto Nacional de Ciberseguridad

LECRIM: Ley de Enjuiciamiento Criminal

LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

RGPD: Reglamento General de Protección de Datos.

PYMES: Pequeñas y Medianas Empresas.

SIM: Subscriber Identify Module (Módulo de identificación del abonado).