Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

Consecuencias de la exención doméstica en redes sociales. RGPD, artículo 2.2.c) en relación con el Considerando 18

Trabajo fin de estudio presentado por:	Nabil Caballero Caballero
Tipo de trabajo:	Trabajo Fin de Máster
Director/a:	Nuria del Carmen Gómez Hervás
Fecha:	18 de julio de 2025

Resumen

En este trabajo se realiza un estudio de la *exención doméstica* en el contexto de las redes sociales conforme a lo establecido en el *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*, abordando las implicaciones y dificultades que plantea su aplicación práctica. Con este fin, se analizan diversas resoluciones y sentencias atendiendo a los criterios interpretativos empleados por los organismos competentes en la resolución de controversias e identificando los puntos críticos que se derivan de una concepción obsoleta de estos espacios digitales. Para contextualizar este estudio, se analiza la realidad actual de las redes sociales, con especial atención en su evolución, diversidad y el funcionamiento normal derivado de la actividad desarrollada por los usuarios.

Palabras clave:

- Actividad personal o doméstica
- Exención doméstica
- Redes Sociales
- Seguridad jurídica
- Criterios

Abstract

This thesis presents a study of the household exemption in the context of social media, in accordance with the provisions of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Adressing the implications and challenges from its practical application. To this end, many decisions and court rulings are examined, taking into account the interpretative criteria used by the authorities when resolving legal conflicts, and identifying the key issues that stem from an outdated conception of these digital spaces. To contextualize the analysis, this thesis explores the current reality of social media, focusing on its evolution, diversity, and the normal functioning driven by the users activity.

Keywords:

- Personal or household activity
- Household exemption
- Social media
- Legal certainty
- Criteria

Índice de contenidos

1. Introducción

El desarrollo de las tecnologías de la información y comunicación (TIC), ha transformado radicalmente el modo en que se relacionan las personas. Ejemplo de ello son las redes sociales (en adelante RRSS) y aplicaciones de mensajería instantánea como WhatsApp, Facebook, Instagram o YouTube, que facilitan la interacción y una difusión continua de todo tipo de datos personales, tanto propios como ajenos. Debido a ello, tiene especial importancia realizar un estudio sobre el concepto de *exención personal o doméstica* recogido en el art. 2.2.c) en relación con el Considerando 18 del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (en lo sucesivo RGPD), mediante el cual, la actividad desplegada por el usuario en RRSS queda excluida, de modo general, del ámbito de aplicación de la normativa de protección de datos, lo que puede generar riesgos para los derechos tanto de usuarios como de no usuarios.

Conviene analizar la actividad desarrollada por los usuarios en RRSS con el fin de entender el impacto que puede tener sobre el derecho a la protección de datos en un mundo en el que estas plataformas se están convirtiendo en la evolución tecnológica de la realidad actual, y a su vez, para comprender la conveniencia o no de la *exención doméstica* y su extensión.

Ya con la redacción del RGPD, el legislador abordó la posible problemática de la amplitud de la *exención doméstica* con la sugerencia 91 del Supervisor Europeo de Protección de Datos (SEPD) de 7 de marzo de 2012 y reiterada por el Grupo de Trabajo del artículo 29 (GT29), sobre la necesidad de establecer ciertos límites a su extensión, pero se acabó optando por la inaplicación general del RGPD, incluyendo de manera específica, ciertas áreas dentro de la actividad puramente personal o doméstica, como es la actividad en línea realizada en el contexto de las redes sociales, entendiendo que debido a que la actividad se producía dentro de un círculo limitado de amistades, se englobaba dentro de la esfera privada de los usuarios.

Con el desarrollo de las tecnologías y la disponibilidad generalizada de dispositivos con cámaras de fotos integradas y otras tecnologías, las RRSS han experimentado un enorme crecimiento y diversificación, tanto en forma como en contenido, quedando muy atrás esa esfera de la privacidad en la que se compartía la información y dando lugar a conceptos ya

conocidos como *algoritmo*, *meme* o *viralización* de ciertas publicaciones que son visualizadas de manera masiva por usuarios ubicados en cualquier rincón del mundo.

Debido a esta rápida evolución y a los grandes cambios en las RRSS, los criterios aplicables en interpretación de la normativa en este ámbito quedan obsoletos con rapidez y es imprescindible adaptarlos a la nueva realidad debido al riesgo que supone la aplicación de unos conceptos desfasados que no se adecúan a la actualidad.

La noción de *privacidad* no puede ser entendida del mismo modo hoy que hace unas décadas teniendo en consideración el nuevo concepto de RRSS y el gran abanico de plataformas con funciones propias, ello, en relación con la actividad real dentro de las mismas, así como el alcance y consecuencias de la difusión. Por ello, resulta esencial abordar ciertos conceptos y funciones que determinadas plataformas ponen a disposición del usuario, y trasladarlas al contexto de la protección de datos donde la *exención doméstica* cobra especial importancia ante el riesgo que suponen los usuarios para terceros.

1.1. Justificación del tema elegido

La elección de este tema surge de la necesidad de delimitar el alcance de la *exención doméstica* del RGPD. Fenómenos como la viralización y el uso de algoritmos han desdibujado los límites entre lo personal y lo público en el contexto de las RRSS, lo que provoca incertidumbre en el momento de conocer si una actividad es considerada doméstica o no y por ende, si está sujeta o no a la normativa de protección de datos.

Los criterios que en su día estableció el GT29 en interpretación de la *exención doméstica*, han sido realmente útiles a lo largo de los años, utilizados de manera sistemática por la jurisprudencia hasta la actualidad. No obstante, dada la rápida evolución de las tecnologías y el desarrollo y diversificación de las RRSS, han quedado desfasados.

La desactualización de los criterios dificulta la labor de los tribunales y de la AEPD en la toma de sus decisiones y resolución de conflictos, impidiendo que se ajusten a la realidad actual, lo cual, implica que pueda afectar al principio constitucional de seguridad jurídica debido a la incertidumbre de los usuarios en el desarrollo de su actividad en RRSS tras la enorme evolución que han sufrido las mismas durante los últimos años. Por ello, parece conveniente analizar los criterios existentes, estudiar su aplicación en función de la realidad tecnológica y

encontrar unos criterios que permitan una interpretación más adaptada a la finalidad de la normativa en el contexto actual.

1.2. Problema y finalidad del trabajo

La búsqueda activa de la viralización ha provocado que los usuarios de las redes sociales ya no se limiten a publicar información y contenido propios, sino a permanecer en alerta constante a fin de captar cualquier suceso que pueda servir de contenido, con total independencia de cómo, dónde y a quién se pudiera estar afectando.

La *exención doméstica* en RRSS tiene como consecuencia más inmediata, la publicación continua de imágenes y videos de terceros. Esto, unido a la ausencia de unos criterios actuales, que sean efectivos y homogéneos acerca de lo que se entiende por *actividad personal o doméstica* en el ámbito digital, provoca cierta incertidumbre en los usuarios de RRSS, cuya actividad y la difusión de muchas de sus publicaciones queda en manos del azar y de los algoritmos de estas plataformas.

La Agencia Española de Protección de datos (AEPD), así como los tribunales, han optado en más de una ocasión por realizar una interpretación restrictiva de la *exención doméstica* en aras de salvaguardar los derechos de terceros que han podido verse perjudicados por determinadas publicaciones, lo que ha derivado en la imposición de sanciones a usuarios que han llevado a cabo determinadas conductas en redes sociales, amparadas, en principio, en esta exención.

Son numerosos los casos en que esta interpretación ha determinado la aplicación de la normativa de protección de datos para proteger la vulneración de ciertos derechos, cuya tutela más bien pudiera corresponder a jurisdicciones como la civil o penal en materia de derechos al honor, intimidad y propia imagen, lo que, a pesar de las buenas intenciones, resulta desacertado en cuanto que puede afectar a principios tan importantes como el de seguridad jurídica.

1.3. Objetivos

El objetivo principal de este trabajo es **ofrecer un análisis que permita encontrar, en el marco de la protección de datos, los puntos más críticos en relación con la actividad del usuario en redes sociales**, abordando el concepto de *actividad personal o doméstica* del artículo 2.2.c) RGPD y, atendiendo a las circunstancias del tiempo y lugar, analizar su aplicación en el contexto actual proponiendo una serie de mejoras para solventar las debilidades detectadas. Para alcanzar este objetivo se fijan cuatro objetivos secundarios.

Primero.- Debido a la complejidad de la figura de los usuarios en las redes sociales por la doble posición que ocupan, como creadores de contenido y como interesados (SÁEZ DE PROPIOS 2025, p. 161), es necesario **analizar las implicaciones derivadas de la *exención doméstica* y en el caso de identificar deficiencias, proponer ideas de mejora que faciliten su aplicación**, pues las RRSS no pueden actuar como un «*paraíso de la información»* donde cualquier comportamiento se permite a los usuarios ante el descontrol de la información que esto supone, pero tampoco puede restringirse sin más, la libertad de los usuarios que se ampara en esta exención.

Segundo.- También se realizará un **estudio de la propia redacción de los preceptos referidos a la actividad personal o doméstica con el fin de verificar la claridad y certeza en cuanto a su extensión.**

Tercero.- Es imprescindible tener en cuenta la realidad actual, ante la enorme diversidad de redes sociales, muy distintas entre sí en cuanto a forma, contenido y funcionamiento por lo que se abordarán los distintos criterios empleados por los organismos competentes en el momento de decidir sobre la aplicación de la *exención doméstica* en función del uso de las RRSS por parte de los usuarios, **comprobando la necesidad o no, de actualizar estos criterios en función de su adecuación a la realidad actual,** ello con el fin de permitir una mayor certeza sobre las actividades incluidas en el ámbito personal o doméstico.

Cuarto.- Finalmente, debe quedar definido el alcance de esta exención de modo que no pueda dar lugar a amplias interpretaciones por parte de los organismos competentes en el momento de conocer y resolver las controversias surgidas, ya que esto compromete gravemente la seguridad jurídica debido a la falta de certeza o de previsibilidad en cuanto a la conducta que es exigible a los usuarios de redes sociales. El resultado de estas interpretaciones supone la

consideración o no, de la existencia de un tratamiento de datos personales y por tanto, determina la competencia o incompetencia de la AEPD en aplicación de la normativa de protección de datos y su régimen sancionador o la aplicación de otras normas relativas a la privacidad de las personas por la jurisdicción competente. Por este motivo, mediante el examen de los criterios empleados por la AEPD y la jurisprudencia en interpretación de la excepción recogida en el artículo 2.2.c) RGPD, se podrá **evaluar en qué medida, estos organismos, adaptan la normativa a la realidad actual mediante una labor interpretativa de modo que permita una aplicación coherente y homogénea en la resolución de los conflictos** que puedan producirse en este ámbito en el contexto actual.

2. Marco teórico y desarrollo

2.1. La actividad personal o doméstica

2.1.1. Antecedentes

El concepto de *actividad personal o doméstica* parte del de *privacidad,* evolucionado a lo largo de los años desde la concepción dada por sus precursores Samuel D. Warren y Louis D. Brandeis, configurado como una extensión de la esfera privada de las personas. (WARREN y BRANDEIS 1980).

En Europa ha sido definido por el Tribunal Europeo de Derechos Humanos (TEDH), en sentencias como LEANDER v. Suecia (1987), ROTARU v. Rumanía (2000) y S. y Marper v. Reino Unido (2008), en interpretación del artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), como un derecho amplio, al desarrollo de la personalidad y a defenderse de las intromisiones externas (SUÁREZ RUBIO 2015).

Tradicionalmente este concepto se ha limitado a la esfera más íntima de las personas, al domicilio y la correspondencia, en aquellas situaciones donde existía una expectativa razonable de privacidad. El Considerando 12 de la Directiva 95/46/CE, así como su artículo 3.2, excluían ya, de su ámbito de aplicación, la actividad personal o doméstica, haciendo alusión a actividades tales como la correspondencia y la llevanza de un repertorio de direcciones, que a lo largo de los años han sido los ejemplos más empleados en cuanto a la actividad desarrollada dentro de la esfera privada de las personas.

En este contexto, la sentencia del caso Lindvisq (STJUE C-101/01 de 6 de noviembre de 2003), entendía que la excepción no aplicaba ante la publicación de datos en una página web de tal modo, que resultasen accesibles por un grupo indeterminado de personas.

Siguiendo esta línea, en virtud de aquella Directiva y la jurisprudencia recaída a partir de la conocida sentencia, en el campo de las RRSS sería aplicable la *exención doméstica* únicamente cuando la red social se configurase de manera que solo fuera accesible por un grupo concreto de amistades, dejando fuera cualquier tipo de actividad que excediera estos límites, pero hoy, y puesto que el plano privado se ha ido diluyendo cada vez más, el RGPD incluye expresamente, en el ámbito de esta exención, la actividad realizada por los usuarios en las

RRSS, dejando fuera, únicamente, a la actividad profesional y a los responsables que proporcionan los medios para tratar datos personales en este contexto.

Por su parte, el GT29 elaboró un Dictamen en este sentido (Dict. GT29 de 12 de junio de 2009), en el cual, en concordancia con la anterior jurisprudencia y acogiendo la sugerencia incluida en la observación 91 del SEPD de 2012, estableció varios criterios a tener en cuenta respecto de esta exención, entre los que se encuentran la actividad profesional o colaboración con asociaciones o empresas, la limitación o restricción de las cuentas de usuario, facilitándose el acceso únicamente a un público seleccionado y por otro lado, la naturaleza de la información publicada, especialmente en cuanto a los datos sensibles. Así, la Comisión Europea en la propuesta del RGPD del año 2012 (*Propuesta de la Comisión Europea de Reglamento del Parlamento Europeo y del Consejo 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 2012)* incluyó ya, en su art. 2.2.d), la exclusión de su ámbito de aplicación al tratamiento efectuado «por parte de una persona física sin interés lucrativo*»,* en la línea de su Considerando 15 que mantenía el criterio del interés lucrativo o sin conexión con la actividad profesional.

2.1.2. Regulación actual en el RGPD

El Reglamento de Protección de Datos garantiza, en el ámbito de las redes sociales, la protección de los derechos de los interesados frente a las empresas que las gestionan, quienes deben velar, como responsables del tratamiento, por el cumplimiento normativo en cuanto a los datos personales que recogen. Esta protección viene explicada de manera general en el Considerando 26 RGPD: «Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable»*,* así como en el último inciso del Considerando 18 que de manera expresa incluye dentro de su ámbito de aplicación, a los responsables y encargados del tratamiento que proporcionan los medios para el desarrollo de la actividad personal o doméstica de los usuarios en RRSS.

No obstante, si bien se protege su información en cuanto a los tratamientos efectuados por parte de un responsable o encargado del tratamiento, no tiene en cuenta que en el contexto de las RRSS existe otra relación al margen de la que existe entre los interesados y la plataforma, y es la relación *de facto* entre las personas físicas, o más bien, entre usuarios y el

resto de potenciales interesados. Esta relación que, *a priori,* no parece tener especial trascendencia, carece de la protección que proporciona el RGPD a los datos personales, de conformidad con su artículo 2.2.c), en cuanto a la exclusión de su ámbito de aplicación, como es el «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*»* ello, en relación con el Considerando 18 RGPD: «Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades*».*

Cabe destacar cómo la AEPD parece cuestionar la amplitud de esta exención toda vez que recomienda al usuario de RRSS y a los internautas en general cumplir, en la medida de lo posible, con ciertas de las exigencias del RGPD, como no compartir información de terceros sin contar con los consentimientos, apelando a la responsabilidad y el respeto a los derechos de los demás, del mismo modo que el GT29, en su Dictamen 5/2009 (Dict. GT29, de 12 de junio de 2009), en su apartado «Resumen de las obligaciones de los SRS*»,* estima que los servicios de redes sociales (SRS) deberían recomendar a los usuarios no publicar imágenes o información relativa a otras personas sin su consentimiento.

Debe tenerse en cuenta que las actividades desplegadas en RRSS y, especialmente sus efectos, no son los mismos hoy que hace años, durante la redacción del RGPD con la propuesta de reglamento del año 2012 y sus fases posteriores, y esto da lugar a una problemática conceptual que debe abordarse.

Conviene referirse en primer lugar, a la conjunción disyuntiva «o» incluida en el art. 2.2.c) RGPD al referirse a las actividades *personales o domésticas*, tomando la definición dada por la Real Academia Española (RAE) sobre el concepto de *disyuntivo* como: «Alternativa entre dos cosas, por una de las cuales hay que optar*»*, con lo que bastará la adecuación de la actividad a cualquiera de las dos alternativas para entenderla incluida en su ámbito de aplicación.

Como resulta evidente, el legislador en el desarrollo de un texto normativo no emplea las conjunciones disyuntivas «o*»*, «u» y las copulativas «y*»*, «e*»* de manera indistinta o sin un propósito, lo cual ha sido tenido en cuenta en reiteradas ocasiones por la jurisprudencia en interpretación de los textos legales. Entre otras: STS 312/2003, 5 de Marzo de 2003 y STS 904/2023, 3 de Julio de 2023.

No se cumple del mismo modo en un supuesto de hecho como: «*el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales Y domésticas»*, que en el supuesto de: «*en el ejercicio de actividades exclusivamente personales O domésticas»*.

Tal y como explica la RAE, en el primer caso, la conjunción copulativa «Y» requiere, para que se dé el supuesto, que se cumplan de manera conjunta o acumulativa ambas notas definitorias ya que deben tenerse en cuenta de manera colectiva.

Por su parte, la conjunción disyuntiva «O», implica dos opciones diferenciadas y alternativas (SERRANO BONILLA 2016), entendiendo que se cumple con el supuesto de manera completa en el caso de ocurrencia de cualquiera de ellas, por lo que, en este sentido, la exención de las RRSS aplicaría en el supuesto de realizarse una actividad considerada personal aunque saliera del ámbito doméstico o viceversa.

Analizado lo anterior, conviene definir los siguientes conceptos:

En cuanto a la *actividad personal*, puede ser contrapuesta a la *actividad profesional*, y guarda relación con la finalidad, tal y como se indica por la AEPD en su Informe 0077/2013: «Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos*».* Del mismo modo que en su informe 0615/2008 en referencia a la Sentencia de 15 de junio de 2006 de la Audiencia Nacional: «No deja de ser personal aquella actividad de tratamiento de datos que aun siendo desarrollada por varias personas físicas su finalidad no trasciende de su esfera más íntima o familiar*».*

La *actividad doméstica* por otro lado, no tiene en consideración la finalidad, debemos entenderla como aquella actividad que no excede de la esfera privada de cada uno, sin injerencias externas y bajo el control de las personas. Así lo indica la AEPD en resoluciones como EXP202308427 de 11 de marzo de 2025, donde establece la necesidad de «evaluar si efectivamente el tratamiento de las imágenes es doméstico o si se captan propiedades de terceros*».*

Teniendo en cuenta la amplia libertad para la actividad que se desarrolla en estos entornos digitales, conviene analizar lo que entendemos por una red social a día de hoy y analizar algunas de las funciones que se ponen a disposición de los usuarios, así como el

funcionamiento normal de estas plataformas de acuerdo a la finalidad para la que están diseñadas.

2.2. Redes Sociales

2.2.1. Evolución y diversidad de redes sociales

La evolución de las redes sociales desde la redacción del RGPD ha sido enorme, por lo que resulta fundamental, en el año 2025, analizar los avances para definir lo que es una red social a día de hoy y comprender cómo interactúan los usuarios en este contexto.

Inicialmente, las redes sociales se han limitado a la interacción entre usuarios pertenecientes a un círculo muy limitado de amistades y que, a grandes rasgos, no han sido sino programas de mensajería instantánea o álbumes de fotos en línea que permitían ser compartidos con una red de contactos, aunque en muy poco tiempo, se ha extendido tanto su uso que ha surgido una gran variedad de plataformas con funcionalidades muy diversas y lo habitual ya no se limita a interactuar y compartir con amistades cercanas, sino con usuarios a nivel mundial (HERMOSO RUIZ 2010, p. 22). Recordemos por un momento los inicios con precursoras como Fotolog (2002) o MSN Messenger (1999), cuyas capacidades y por supuesto las funcionalidades, eran mucho más restringidas, por lo que la cantidad de información que se difundía era ínfima en comparación con el nuevo concepto de *redes sociales*. Por lo general, estas no disponían de una interfaz por la que poder navegar entre usuarios o no contaban con una red de contactos o registro de seguidores por lo que, con el fin de poder interactuar y compartir contenido, era imprescindible disponer de los contactos, habitualmente la dirección de correo electrónico de otros usuarios, lo que unido a la limitación de la tecnología que impedía la posibilidad de tomar y transferir imágenes y videos con la facilidad de hoy día, limitaba en gran medida ese interés actual de las grandes empresas en crear interfaces enfocadas al intercambio de grandes cantidades de información, de modo que gran parte de las interacciones entre usuarios se limitaban al intercambio de mensajes de texto dentro de ese círculo personal de amistades.

Desde luego los años han transcurrido y las tecnologías han avanzado de tal modo que las funciones y, por ende, las posibilidades que ofrecen las redes sociales son enormes, con las amenazas que supone un mal uso de las mismas, vulnerándose de manera sistemática los

derechos de terceros mediante la publicación de imágenes y videos sin el consentimiento de sus titulares, lo que a día de hoy, se ha normalizado hasta tal punto que resulta difícil encontrar un límite en el tipo de información que se difunde a diario (BAÑO CARVAJAL y REYES ESTRADA 2020).

En la actualidad, plataformas como Facebook o Instagram permiten encontrar y visualizar de manera rápida y sencilla, la información y contenido de usuarios repartidos por cualquier parte del mundo. Es cierto que algunas de estas plataformas ofrecen la opción de controlar quién puede acceder al contenido que uno publica, mediante las opciones de perfil público o privado, pero pensemos también en YouTube, o incluso Instagram en su sección de «*reels»* como publicaciones sugeridas donde no se requiere acceder a un usuario concreto. Basta con el conocido «*scroll»* (desplazarse verticalmente por la pantalla) para acceder a una publicación aleatoria tras otra, lo que, si bien se basa en las preferencias de cada uno, tiene completa independencia del autor de la publicación. Estas funciones están pensadas para que usuarios a nivel global puedan acceder y visualizar el contenido producido y publicado desde cualquier lugar, olvidando ese reducido entorno de amistades dentro de la esfera privada de cada usuario al que se limitaba la actividad en las redes sociales predecesoras.

Existen otros tipos de redes sociales, como puede ser WhatsApp, Telegram o Snapchat, basadas principalmente en la mensajería instantánea que, si bien no cuentan con una plataforma en la que crear una red de contactos, sí permiten compartir contenido con los contactos de los que dispone cada usuario, por lo que el público potencial es, en principio, más reducido. Si bien solo en principio, dado que nada obsta para que esa información pueda llegar a otras plataformas dada la facilidad que proporcionan las tecnologías en el mundo interconectado actual.

A la hora de crear estas redes de contactos entre usuarios, por lo general las RRSS facilitan al usuario la búsqueda de amistades por medio de sus interfaces, así como mediante opciones ya clásicas como la sugerencia de contactos en función de otra información almacenada como son las interrelaciones existentes entre usuarios, pero hay otras funciones que se ponen a disposición del usuario y que pueden resultar cuestionables cuando pensamos en los derechos de terceros. Se trata de funciones que permiten a cualquier usuario sincronizar los contactos de su agenda personal almacenada en la nube o en un dispositivo móvil con la aplicación, con el fin de vincularlos en su cuenta de usuario en la plataforma. Esto significa que la lista de

contactos es introducida con el fin de encontrar coincidencias, lo que facilita mucho a los usuarios a la hora de encontrar a sus amistades dentro de la plataforma. Ahora bien, aquellos usuarios que no son localizados, es decir, aquellos que no forman parte de la red social en el momento de la sincronización de contactos, aun tratándose de usuarios no registrados, la plataforma almacena, al menos, sus datos identificativos y de contacto (nombres, números de teléfono o correos electrónicos). En este sentido, la política de privacidad de la empresa Meta, entre otras, establece cláusulas como la siguiente:

> Tratamos el nombre, el número de teléfono móvil o la dirección de correo electrónico si recibimos estos datos de nuestros usuarios mediante las funciones de subida de contactos o sincronización de contactos disponibles en Facebook, Messenger o Instagram ("Subida de contactos"). Tratamos esta información aunque no seas usuario de Facebook, Messenger o Instagram, y también en el caso de que no tengas ninguna cuenta con nosotros ("Persona no usuaria"*).*
>
> *(…)*
>
> Meta comparte la información que recopila, su infraestructura, sus sistemas y su tecnología con el resto de las Empresas de Meta. Compartimos los datos de Personas no usuarias con otras Empresas de Meta para proporcionar la función "Subida de contactos" y con los fines expuestos anteriormente.

Igualmente destacable por su actualidad, es la intención de la empresa META de utilizar toda la información de sus redes sociales para la mejora continua de su IA, incluyendo los contenidos públicos, comentarios de las cuentas de personas mayores de 18 años e interacciones con las funciones de la IA tal y como se indica en su política de privacidad. Esto significa que cualquier imagen de terceros publicada sin su conocimiento ni consentimiento, al amparo de la *exención doméstica,* ahora será utilizada para educar a su inteligencia artificial (IA), sin posibilidad de oposición por parte de aquellos al depender exclusivamente de la decisión del autor de la publicación.

La plataforma permite al usuario oponerse a este tratamiento, pero resulta cuanto menos curioso, que el consentimiento venga dado por defecto, más teniendo en cuenta la gran cantidad de información de terceros que se incluye por lo general, en las publicaciones de un usuario medio, y no solo referida a información de otros usuarios, sino especialmente teniendo en cuenta a todos aquellos que no son usuarios y cuyos datos e imágenes también

se encuentran en la plataforma sin el conocimiento de estas personas que pueden aparecer en numerosas imágenes de espacios multitudinarios, eventos o en cualquier espacio público de manera casual. La falta de oposición de los usuarios que han publicado este tipo de imágenes supondrá la cesión de los datos de aquellos terceros por igual.

Estos ejemplos son muestra de que, cada una de las plataformas de RRSS cuenta con sus propias funciones, si bien algunas similares, otras completamente distintas y a medida que la tecnología avanza, cualquier actividad desplegada por el usuario mediante el uso de las funciones que se ponen a su disposición afecta de manera directa a los derechos y libertades de terceros. Es importante entender bien el funcionamiento y la actividad desarrollada dentro de estas, si no de todas, al menos sí de las RRSS más habituales, para comprender que criterios pueden ser tenidos en cuenta para identificar lo que es considerado dentro de la esfera personal o doméstica y lo que no, con especial atención a la enorme diversidad, donde es plenamente aplicable el principio que rige el derecho a la igualdad, en cuanto a la igualdad entendida no en términos absolutos sino solo en circunstancias iguales (GARCÍA ROCA 2020; OLIVERAS JANÉ 2023).

2.2.2. Desafíos de la actividad en redes sociales

El simple uso de las RRSS por su propia naturaleza implica una pérdida de privacidad. Además, los ciberataques y otros incidentes de seguridad están a la orden del día y, el escenario de las redes sociales no es una excepción, donde el impacto es enorme dada la gran cantidad de información que manejan de usuarios a nivel mundial.

La ausencia de una regulación específica y fuerte en los espacios digitales que son las RRSS puede dar lugar a abusos, tanto por parte de las propias plataformas como de terceros, dada la facilidad de acceso a toda la información que se encuentra publicada en RRSS y la utilización inadecuada de toda esta información supone un grave riesgo para la privacidad y por supuesto, para la *autodeterminación informativa*, convirtiendo a las RRSS en un auténtico «*paraíso de la información»* donde no existe un control real sobre los datos propios.

La publicación de información de terceros bajo la *exención doméstica* supone la posibilidad de apropiación por otros usuarios y su reutilización en otras RRSS, el riesgo de viralización o el aprovechamiento por parte de las plataformas para fines sobrevenidos como la educación de

IAs en desarrollo, todo ello, sin el conocimiento de los afectados que, hoy en día, incluye tanto a usuarios como no usuarios, dada la masificación en el uso de RRSS y la proliferación de las tecnologías.

2.2.2.1. Metadatos y Big Data

Uno de los principales riesgos que existen con los datos que se publican en internet es que contienen más información de lo que, por lo general, se conoce. Se trata de los metadatos, información que describe otros datos, proporcionan información acerca de los archivos que se publican, describiendo el día, hora y lugar de creación o el dispositivo que lo creó. Todos estos datos en conexión facilitan, aún más, la identificación e incluso ubicación de su autor (RAVENTÓS PAJARES 2009).

Cada vez que una imagen o video es publicado en internet o en RRSS, a su vez puede estar publicando toda esta información. Aunque se dice que muchas plataformas de RRSS eliminan los metadatos de manera automática al publicar información, en realidad esto depende del modo en que la información es compartida. Cualquier imagen puede ser compartida como imagen propiamente dicha o como documento o archivo, y esta eliminación de metadatos solo tiene efecto cuando se activan las funciones de compresión de los datos compartidos, por ejemplo en el caso de WhatsApp, solo ocurre cuando una imagen es compartida como imagen en sí y no como archivo.

Es importante tener esto en cuenta ya que, en determinadas ocasiones, puede ser aprovechado por terceros, lo que, en conexión con otras tecnologías de fácil acceso, como Google Maps o las IAs, puede permitir conocer con precisión la identidad de su autor o determinar ubicaciones entre otras muchas posibilidades (PÉREZ 2022) con el consecuente incremento de los riesgos.

Todos los metadatos publicados por los usuarios e internautas, en unión con el resto de información que se recopila en internet constituyen lo que se conoce como Big Data. Se trata del rastro que permanece en internet tras su mera utilización, un conjunto masivo de datos que se extraen de diversas fuentes, entre ellas, las RRSS, con los que se consigue evaluar, predecir y analizar comportamientos y tendencias a gran escala (SERRANO-COBOS 2013), obteniendo información personal que va más allá de la proporcionada y que constituye la

esencia de las Inteligencias artificiales, conocidas ya como las precursoras de una nueva revolución industrial o «*Revolución 4.0»* (GÓMEZ SALADO 2021, citado por MOLINA HERMOSILLA 2023, p.91).

Teniendo en cuenta lo anterior, es preciso estudiar determinados conceptos en relación al funcionamiento de las RRSS y el alcance en la difusión que se consigue mediante estas plataformas.

2.2.2.2. Algoritmo y viralización

No todas las plataformas de RRSS son iguales y no todas tienen implementados algoritmos encargados de evaluar y analizar las preferencias de los usuarios, por lo que deben diferenciarse las plataformas de RRSS destinadas a la creación y consumo de contenido como YouTube, Facebook o Instagram de otras RRSS destinadas a la mensajería instantánea como puede ser WhatsApp, Telegram, Messenger o Snapchat.

Por lo general, la actividad en estas RRSS de creación de contenido comienza con una publicación inicial en una plataforma determinada que puede ser una imagen, un video o cualquier tipo de contenido que se comparte. Al ser recibida por la comunidad, esta publicación podrá resultar graciosa o llamativa por cualquier motivo, siendo así, que otros usuarios decidirán comentar, reaccionar y compartir, provocando que el algoritmo de la plataforma comience a sugerir esta publicación a otros usuarios, con lo que se consigue un alcance aún mayor en la difusión.

El algoritmo como distribuidor de la información, es quien la selecciona y decide cómo y en qué medida se difunde. Si bien, toma las decisiones en base a su programación, es, en última instancia, el propio algoritmo quien, mediante cálculos lógicos y el aprendizaje continuo, decide sobre la importancia de los contenidos (CETINA PRESUEL Y MARTÍNEZ SIERRA 2019), graduando la relevancia de cada publicación en función de la acogida e interacción del resto de los usuarios, como puede ser el tiempo de visualización, el número de reproducciones, los «click», o las suscripciones, teniendo en cuenta tanto la actual información publicada como contenidos anteriores con características similares y analizados en base a usuarios con perfiles similares (PEREZ RUFÍ 2019). Así, y completamente ajeno al control de los usuarios, entra en juego el fenómeno de la viralización, favorecido por las recomendaciones del algoritmo, en

que, de manera completamente imprevisible, una información determinada sale de la esfera privada en la que se encontraba para ser visualizada por parte de millones de usuarios en cuestión de minutos.

La viralización es, en cierto modo, equiparable a una brecha de seguridad, en que, en función de los controles y medidas de seguridad que desplieguen los usuarios, la probabilidad de ocurrencia disminuiría en mayor o menor medida. Ahora bien, dado que nos encontramos en un ámbito fuera de la aplicación de la normativa de protección de datos, es preciso señalar que, al usuario, previo a la viralización de su contenido, no le es exigible medida alguna al no considerarse tratamiento de datos personales. Lo que sucede con la repentina ocurrencia de este fenómeno es que, el usuario, debido a la amplia difusión de su publicación, de acuerdo con los criterios seguidos por la APED, entraría automáticamente en la categoría de responsable del tratamiento con todas las consecuencias y obligaciones que esto supone. Esto es buscado de forma activa por la comunidad en RRSS, con lo que la publicación de contenido y, especialmente de imágenes, es continua en estas plataformas, introduciéndose datos tanto propios como de terceros y buscando aumentar drásticamente el número propio de seguidores a fin de lograr la viralización. Todo esto supone una difusión masiva e incontrolada de la información que se comparte, con un alcance geográfico amplísimo.

Al margen de lo anterior, conviene destacar que la viralización no depende realmente del propio autor ni de la cantidad de contactos o de seguidores con los que cuenta (FALCONÍ MONARD y ARGUDO PALOMEQUE 2025), sino de la acogida por parte de los destinatarios y de los algoritmos, y además responde al funcionamiento normal de estas plataformas, por lo que resulta al menos llamativo como, teniendo esto en cuenta, pueden repercutir en un usuario que se limita a desarrollar su actividad con normalidad y que no busca la ocurrencia de este fenómeno, las consecuencias desfavorables que conllevaría su consideración como responsable de tratamiento.

2.2.2.3. Meme

En determinados casos, los usuarios comparten imágenes ya publicadas anteriormente por otros, apropiándose del contenido, modificándolo e incluyendo palabras, frases o citas de cualquier tipo, otorgándolas un significado propio que puede ser cómico, sarcástico,

dramático o de cualquier otra clase, que es aceptado por la comunidad, dando lugar al llamado *meme* (DE JESÚS OLIVEIRA, DE MAGALHÃES PORTO y LUIZ ALVES, 2019).

Todos estos conceptos suponen un descontrol completo de la información, comentarios y visualizaciones a escala global y un reconocimiento generalizado por parte, tanto de usuarios de las plataformas como no usuarios, ya que los contenidos virales y los memes, trascienden de la propia plataforma y son conocidos y empleados por todos los rincones de internet así como por los medios de comunicación más tradicionales como pueden ser determinados programas de televisión.

Cuando la imagen o información convertida en meme pertenece al propio autor del contenido original no tiene mayor relevancia, pues cada uno es dueño de sus propios datos y decide cómo, cuándo y en qué medida los comparte, ello en base al principio de autodeterminación informativa acogido de manera unánime por la doctrina (WESTIN 1967; CUELLO 1986), y en relación con el principio de coherencia con los actos propios recogido tanto en el artículo 9.2.e) RGPD como en el art. 15.1 de la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTAIBG), modificado por la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD). No obstante, en ocasiones puede resultar desproporcionado debido a la imprevisibilidad de las consecuencias, pues, si bien el RGPD no resulta aplicable en la publicación del contenido, tampoco resulta aplicable posteriormente, careciendo de cualquier protección mientras se encuentre en RRSS.

Con frecuencia, y sirva de ejemplo el concepto de *meme*, la imagen publicada en primera instancia, deriva en el uso generalizado por parte del resto de usuarios, quienes comienzan a utilizarla, difundiéndola y adaptándola a todo tipo de circunstancias.

Si bien la finalidad principal de su autor puede ser la de ser publicada y accedida por un círculo limitado de contactos, en ocasiones esta información es tomada por otros usuarios, incluso dentro de ese círculo inicial, que lo introducen en otras plataformas ampliando exponencialmente el número de potenciales destinatarios hasta que eventualmente y si se dan las circunstancias, es visualizada y compartida de manera generalizada a lo largo y ancho de todo el planeta.

2.2.2.4. Monetización

La monetización de contenido, ha sido uno de los fenómenos más relevantes en este ámbito. Tiene una vinculación directa con el criterio de la finalidad profesional o lucrativa, empleado en la actualidad como límite a la exención del artículo 2.2.c) RGPD, pero conviene señalar algunas cuestiones que complican la aplicación sistemática de este criterio.

La posibilidad de monetización de determinadas publicaciones en RRSS puede ocurrir en cualquier momento. Cada plataforma establece sus propios requisitos para monetizar los contenidos. Por ejemplo, en el caso de YouTube, sus normas establecen requisitos tales como la necesidad de contar con un determinado número de visualizaciones en los últimos 365 días o contar con un número mínimo de suscriptores entre otros.

La monetización por medio de patrocinadores o publicidad se aplica a publicaciones individuales, no al propio canal o cuenta de usuario en su totalidad, lo que, de entrada, supone varios problemas en cuanto a la aplicación o inaplicación del RGPD.

Los interesados por lo general, no tendrán conocimiento sobre la monetización o no de contenidos determinados, lo cual afectaría a la posibilidad de reclamar ante la AEPD en materia de protección de datos.

Es necesario señalar, que una cuenta de usuario en estas plataformas no es algo estático, por lo que el contenido publicado por los usuarios en sus cuentas puede pasar de contar con unas decenas de seguidores en un momento puntual, a contar con cientos, miles e incluso más, en un momento posterior, siendo así, que los requisitos para la monetización podrán cumplirse en cualquier momento a lo largo de la vida de estos canales, lo que no solo afecta a los contenidos considerados dentro del ámbito profesional por haber sido monetizados. El hecho de cumplir con estos requisitos afectará inevitablemente a aquellos otros contenidos que, en principio, permanecen en la esfera doméstica, debido al aumento del público general o los seguidores en una cuenta de usuario determinada. Esto, unido al fenómeno de la viralización, puede ocurrir en cuestión de minutos, lo que supone la exigencia al usuario de redes sociales la observancia de los principios y obligaciones de la normativa de protección de datos desde el inicio, en vistas a posibles acontecimientos que excluyan su actividad del ámbito personal o doméstico en el que inicialmente se desarrollan. Así, en la práctica, esta exención que ampara la actividad en RRSS, perdería toda razón de ser, al tratarse de un concepto sin aplicación real,

otorgando a los usuarios una falsa confianza en la publicación de sus contenidos casi con total libertad pero concediendo a cualquier perjudicado la posibilidad de reclamar contra las publicaciones que consideran una injerencia en su esfera privada, eso sí, solo en los limitados casos en que los afectados lleguen a tener conocimiento de tales publicaciones, así como del hecho de su monetización, permitiéndoles ejercitar su derecho fundamental a la protección de los datos personales en detrimento de la seguridad de los autores de la publicación que confían en que su actividad se ampara bajo la *exención doméstica*.

Conociendo el alcance actual y la tipología de estas plataformas, es imprescindible analizar los criterios a tener en cuenta sobre lo que debe entenderse comprendido dentro de una *actividad personal o doméstica* y la problemática que se deriva de la aplicación común de estos criterios a todas las RRSS de manera indistinta.

2.3. Tutela del derecho a la protección de datos

2.3.1. Análisis e implicaciones de los criterios aplicables

Conviene repasar los límites de la *exención doméstica* y los criterios que deben tenerse en cuenta para determinar cuándo una actividad sobrepasa lo que debe ser considerado como privado para dar lugar a la aplicación de la normativa de protección de datos.

A continuación se detallan algunos de los criterios que pueden identificarse en el contexto de las RRSS, algunos de ellos ya empleados por la jurisprudencia.

Uno de los criterios más claros y empleados es el de la finalidad profesional de la actividad llevada a cabo en la cuenta de los usuarios, en función tanto del propio contenido de la misma como de si ese contenido está siendo monetizado mediante patrocinadores, publicidad o colaboraciones comerciales. Incluso cuando no se obtienen beneficios directamente de la propia publicación, puede tratarse de cuentas profesionales asociadas a empresas o negocios, destinadas a dar publicidad lo que, de manera indirecta y fuera de la plataforma, sí estaría reportando beneficios. Aunque se trata de un criterio claro y ampliamente empleado, la realidad es que no es suficiente por sí solo, ya que permite identificar la contraparte de lo considerado como actividad personal, pero el ámbito doméstico es una cuestión distinta que no atiende a la finalidad sino a la extensión en cuanto a los destinatarios.

Un criterio a considerar en contraposición de lo doméstico, sería el número de amistades o seguidores de cada usuario, y por ende, la potencial difusión de cualquier tipo de información publicada desde una cuenta de usuario determinada. Si bien esto permitiría conocer el posible impacto inicial, computado en función del número de contactos, no serviría en el medio y largo plazo debido a la gran cantidad de variables que introduce la inmensa red de conexiones existentes en estas plataformas, ello, unido a los algoritmos que sugerirán determinados contenidos en función de la recepción e interacción del resto de usuarios con ese contenido.

Si bien podrían establecerse unos mínimos en cuanto a la posible extensión de la difusión inicial, no serviría para conocer el impacto real posterior ni si esta difusión se extendería más allá del círculo cercano de contactos del usuario.

Gran parte de las grandes plataformas de redes sociales funcionan con el recuento de «*viewers»*, es decir, visitas o visualizaciones en las publicaciones. En ello se basan los algoritmos a la hora de recomendar y sugerir determinados contenidos, entre muchas otras variables.

El criterio del número de visualizaciones en cada publicación catalogaría, de la manera más objetiva posible, cada tipo de contenido en función de su impacto real, definiéndolo como doméstico o no en base a unos límites prestablecidos. No obstante y teniendo en cuenta que esa categorización dentro de lo doméstico o no, implicaría la consecuente obligación o no, de cumplimiento de la normativa de protección de datos con respecto del contenido de la propia publicación, hace preciso conocer si la actividad se encuentra amparada dentro de la *exención doméstica* con carácter previo al de la propia publicación, por lo que no es viable el recuento de visualizaciones, en caso contrario, el cumplimiento o incumplimiento correspondiente de las obligaciones impuestas por la normativa vigente quedarían al azar, en manos del propio algoritmo de redes sociales y por supuesto, infringiendo el principio de seguridad jurídica ante la incertidumbre en cuanto a la regulación aplicable en el momento de iniciar la actividad.

Uno de los criterios propuestos por el GT29 y aplicados por la jurisprudencia en reiteradas ocasiones, es el carácter público o privado de cada cuenta de usuario. Una opción que permite al usuario controlar el número de personas que pueden acceder a las publicaciones propias, estableciendo el límite, en función de cada plataforma, en usuarios concretos o categorías y grupos tales como: Amistades, seguidores, o a todo el público de manera general, lo que puede ser un indicador de que la actividad es personal o doméstica pero no es decisivo.

Al restringir el acceso a cada publicación, se limitaría, en principio, su difusión. Sin embargo, quienes sí tienen acceso podrían extraer la información, y existen herramientas como la captura de pantalla que dejan sin efecto muchas de estas restricciones que el usuario pueda establecer, permitiendo a otros usuarios obtener la información y publicarla con independencia de los límites establecidos inicialmente por su autor original al definir su perfil como privado, accediendo a la información, destinada, en principio, solo a ese número limitado de personas prestablecidas como pueden ser las amistades, y consiguiendo una copia de la información que podrá ser compartida de manera libre y generalizada en otros perfiles y plataformas.

No puede obviarse que una cuenta de usuario puede ser pública y pese a ello, permanecer en un círculo íntimo de amistades al contar con un número muy limitado de contactos o seguidores, siendo así que, el algoritmo por lo general, no recomendará este contenido dada las escasas interacciones, pudiendo el usuario desarrollar una actividad estrictamente personal o doméstica en estas circunstancias sin impedimento alguno. En cambio, una cuenta determinada podría contar con miles o millones de contactos, por lo que, el hecho de restringir las publicaciones únicamente a sus contactos no tendría un efecto apreciable que limite la difusión.

Todos estos criterios deben ser complementados con otros, pues de nada sirve considerar como doméstica la actividad de una cuenta de usuario por el mero hecho de ser privada si el número de amistades o de seguidores se cuenta por millones. Observar el número de amistades o seguidores con los que cuenta cada usuario a fin de establecer un límite en la concepción de lo *personal o doméstico* podría parecer razonable y así lo entendió la AEPD en su informe 0615/2008, cuando indicaba que un número elevado de contactos puede implicar que el usuario no conozca a algunos de ellos, provocando que no se aplique la exclusión a la normativa al extenderse más allá de una «actividad propia de una relación personal o familiar, equiparable a la que podría realizarse sin la utilización de Internet». No obstante, esta observación corre el riesgo de vulnerar un derecho tan fundamental como el de la igualdad si se opta por establecer un límite al número de amistades que un usuario puede tener antes de ser considerado tratamiento de datos personales.

En cualquier caso, es de todo punto necesario tener en cuenta la evolución y diversificación de las redes sociales, primero de todo, debido a la actividad más habitual que se desarrolla en

las mismas, actualmente basada precisamente en la acumulación progresiva de contactos, seguidores o suscriptores en función de las preferencias de contenidos de cada usuario y no en base al conocimiento efectivo de las personas a las que se decide seguir.

También es necesario observar las funciones implementadas, ya que estas varían necesariamente en función de cada plataforma, y así, ciertos criterios que pueden parecer aplicables en determinadas situaciones no lo serán en una situación idéntica pero ocurrida en una plataforma distinta. Por ejemplo, el incumplimiento del criterio de la restricción de contactos en base a un perfil público o privado, no tendrá el mismo efecto en WhatsApp que en plataformas de creación de contenido que cuentan con algoritmos de sugerencias o recomendaciones como pueden ser Facebook, Instagram o YouTube.

2.3.2. Vulneración de la seguridad jurídica en la tutela de derechos

Son muchos los usuarios de RRSS que se dedican a grabar su vida cotidiana con el fin de publicarla, sin importar el momento ni el lugar. Espacios públicos, centros comerciales, restaurantes, sitios turísticos y eventos multitudinarios se han convertido en lugares habituales para este tipo de actividades, debido a la normalización del uso continuo de los dispositivos móviles para tomar fotografías, videos o «*selfies*» y su conexión directa con las plataformas de RRSS.

La consecuencia más inmediata de este comportamiento es el hecho de que muchas personas habrán sido captadas en imágenes o videos que permanecen almacenados en dispositivos ajenos, de personas con las que no existe ningún tipo de relación, y debido a esta normalización, con frecuencia sucede de manera inadvertida (DOMÍNGUEZ MARTÍNEZ 2011).

En este sentido, no resulta del todo alentador, aunque sí coherente con la *exención doméstica*, cuando en su página web, la AEPD, dada la inaplicación del RGPD en el marco de las RRSS, informa a las personas afectadas, que ante la publicación de datos propios por parte de otros usuarios, cabe solicitar amistosamente la retirada del contenido al propio autor de la publicación. A pesar de ello, la AEPD y los tribunales han aplicado la normativa de protección de datos a determinados supuestos, interpretando de manera restrictiva la exención por el uso doméstico con el fin de sancionar determinadas conductas que, aunque cuestionables, no parecen encajar con el marco normativo, lo que puede generar cierta inseguridad jurídica al

no existir unos criterios claros y bien definidos que puedan ser informados a los usuarios en su actividad en RRSS. Esto no significa que las personas queden desamparadas, por supuesto, existen cauces y mecanismos legales para denunciar y evitar estas injerencias, a través de los cuales se pueden ejercer los derechos al honor, intimidad y propia imagen, ante la jurisdicción competente de acuerdo con la legislación vigente. Derechos estos reconocidos en el art. 18 CE y desarrollados por la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, así como en su caso, ante la jurisdicción penal.

La AEPD, en resoluciones como la PS-00695-2014 de 28 de octubre de 2016 y en su *guía sobre consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles*, siguiendo la línea en que se expresa el GT29 en su Dictamen 5/2009 (Dict. GT29, de 12 de junio de 2009), indica de manera precisa que, aun cuando no aplica la *exención doméstica*, cabrá exigir responsabilidades de conformidad con la legislación civil o penal para proteger los derechos de terceros, así como la AI-00404-2024 de 3 de Octubre de 2024, al entender que no se han producido hechos dentro del ámbito de las competencias de la propia AEPD por encontrarse ante la aplicación de la *exención doméstica*.

El principio de seguridad jurídica previsto en el art. 9.3CE, tal y como señala en reiteradas ocasiones el Tribunal Constitucional (TC) en sentencias como STC 136/2011 y STC 234/2012, es entendido como:

> la certeza sobre el ordenamiento jurídico aplicable y los intereses jurídicamente tutelados (STC 15/1986, de 31 de enero, FJ 1), como la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en la aplicación del Derecho (STC 36/1991, de 14 de febrero, FJ 5), o como la claridad del legislador y no la confusión normativa (STC 46/1990, de 15 de marzo, FJ 4). De tal modo, que si en el Ordenamiento jurídico en que se insertan las normas, teniendo en cuenta las reglas de interpretación admisibles en Derecho, el contenido o las omisiones de un texto normativo produjeran confusión o dudas que generaran en sus destinatarios una incertidumbre razonablemente insuperable acerca de la conducta exigible para su cumplimiento o sobre la previsibilidad de sus efectos, podría concluirse que la norma infringe el principio de seguridad jurídica" (SSTC 150/1990, de 4 de octubre, FJ 8; 142/1993, de 22 de abril, FJ 4; 212/1996, de 19 de diciembre, FJ 15; 104/2000, de 13 de abril, FJ 7; 96/2002, de 25 de abril, FJ 5; y 248/2007, de 13 de diciembre, FJ 5).

Es importante tener en cuenta esta definición dada por la jurisprudencia a efectos de comprender, como la ausencia de unos criterios homogéneos y efectivos en cuanto a la interpretación de la normativa puede afectar a la seguridad jurídica.

A continuación se detallan algunos casos concretos.

2.3.2.1. Sentencia de la Audiencia Nacional 2264/2018

Existen casos como la sentencia de la Audiencia Nacional de fecha 11 de mayo 2018 (SAN 2264/2018), que resuelve el recurso interpuesto contra la resolución de 20 de julio de 2016 de la Agencia Española de Protección de Datos, recaída en el procedimiento sancionador nº PS/00070/2016, en relación a una denuncia por colgar en un perfil de Facebook, un video correspondiente a una vista de juicio oral por delito.

En este caso se concluyó, confirmando la resolución de la AEPD, que se había realizado un tratamiento ilícito de datos personales al no contar con el consentimiento de las personas afectadas, considerando que la actividad no encontraba amparo dentro de la *exención doméstica* al no concurrir los criterios señalados por el GT29, en concreto, por la publicación de datos personales en Facebook sin restricciones de acceso para el resto de usuarios de la red social.

Tanto la AEPD como la Audiencia Nacional en sus resoluciones, entendieron que la potencial difusión de la publicación excedía del entorno doméstico, pero resulta esencial tener en cuenta de manera extensiva, las implicaciones de estas resoluciones pues, el objetivo es la aplicación uniforme de unos criterios que permitan obtener resoluciones coherentes, que se adecúen tanto a la normativa como a la realidad actual de las RRSS en función de la actividad real que se desarrolla en el seno de las mismas.

La aplicación de un criterio tan genérico sin ser complementado con otros da lugar a tratamientos ilícitos generalizados en RRSS por los usuarios, convirtiendo a gran parte de estos, en responsables del tratamiento, de manera que cualquier usuario que comparte imágenes en Facebook o Instagram, por ejemplo en lugares turísticos, sería sancionado en virtud de la aplicación de este criterio. Así, incluso la modificación puntual de un perfil privado a público daría lugar a la ilicitud del tratamiento en ausencia de los consentimientos de todo

aquel que pudiera aparecer en aquellas imágenes que han sido colgadas a lo largo de los años por un usuario medio.

Si bien es cierto que la sentencia tiene en consideración el tiempo transcurrido durante el cual el video se mantuvo publicado, es solo a efectos de modular la correspondiente sanción, pues como se aprecia en su fundamentación, la ilicitud del tratamiento se originó con la mera publicación.

2.3.2.2. Resolución de la AEPD Nº PS/00334/2019

Conviene destacar la resolución de la AEPD Nº PS/00334/2019 de 18 de diciembre 2019, por medio de la cual se sancionó, con 10.000€, a una persona física por compartir en su estado de WhatsApp, fotografías íntimas de otra persona sin su consentimiento, fundado de la manera siguiente:

> se evidencia que el reclamado ha vulnerado el artículo 6.1 del RGPD, puesto que ha realizado un tratamiento ilícito al dar a conocer a terceros datos personales de la reclamante contenidos en un pendrive, que le fue sustraído según sus manifestaciones, sin su consentimiento ni autorización y con la agravante de que en el pie de algunas de las fotografías se vierten comentarios vejatorios y degradantes para la reclamante.

En primer lugar, la resolución omite aludir a los criterios señalados por el GT29, entendiendo que existe tratamiento con la mera publicación de las fotografías y con independencia de encontrarnos en el escenario de las RRSS, en atención a que el pendrive donde se encontraban las imágenes fue sustraído de la reclamante con el componente añadido de incluir comentarios denigrantes y vejatorios.

Al margen de valoraciones éticas u opiniones de carácter personal, resulta imprescindible comprender el funcionamiento de este tipo de aplicaciones al analizar incidentes como este.

En el caso de WhatsApp, las publicaciones en la sección de «*estados»* solo son accesibles para aquellos contactos que disponen del número de teléfono de su autor, a diferencia de otras RRSS como YouTube, Instagram, TikTok o Facebook, donde el contenido puede difundirse de manera mucho más amplia gracias a los algoritmos, sugerencias de contenido y el funcionamiento de las propias plataformas.

Es evidente que el alcance de la actividad realizada por el denunciado no puede tener el mismo alcance que habría tenido en otras RRSS como en el caso anterior referente a la SAN 2264/2018. Por lo que, desde una interpretación estricta del criterio relativo a la restricción del público potencial, dicha publicación habría permanecido dentro del círculo privado de su red de contactos como, de hecho, la propia resolución reconoce cuando indica «El alcance meramente local del tratamiento llevado a cabo por el reclamado». De este modo no se cumpliría con ninguno de los ya conocidos criterios establecidos por el GT29, y excluyendo por tanto, la obligación de recabar el consentimiento por no ser considerado un tratamiento de datos personales, encontrando amparo en la *exención doméstica* de la actividad en redes sociales, y por ende, excediendo de las competencias de la AEPD en cuanto al conocimiento y resolución de estos casos de acuerdo con los artículos 44.3 y 47 LOPDGDD, debiendo proceder de acuerdo con el artículo 65.2 LOPDGDD, tal y como la propia agencia señala en resoluciones como la Nº: E/01825/2019 de 9 de abril de 2019: «La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales».

El hecho de incluir contenidos íntimos o comentarios vejatorios o degradantes para terceros no guarda relación con los conceptos que incumben a la protección de datos, ni excluyen la actividad del contexto personal o doméstico desarrollado en redes sociales, por lo que el conocimiento de estas causas no corresponde a los organismos de protección de datos mediante interpretaciones que no encajan en el objeto de la normativa a pesar de proteger bienes jurídicos similares.

Resulta imprescindible establecer una distinción clara entre el derecho a la protección de datos y otros derechos relativos a la esfera privada de las personas, y es que, la confusión de estos derechos y el conflicto de competencias en cuanto a su tutela por parte de los organismos, y especialmente en cuanto implican consecuencias desfavorables como son las sanciones, supone un riesgo importante para la seguridad jurídica.

2.3.2.3. Resolución de la AEPD Nº PS-00126-2024

Finalmente merece destacar la resolución Nº PS-00126-2024 de 23 de septiembre de 2024, por cuanto entiende que existe un tratamiento de datos personales por el mero hecho de

difundir la imagen de un tercero, independientemente de que se realice en el marco de una red social como Telegram y por ende, omitiendo un necesario análisis y fundamentación acerca de la aplicación o inaplicación de la *exención doméstica.*

En esencia, conviene señalar que la *exención doméstica,* no es una mera declaración sin aplicación práctica que pueda descartarse a fin de salvaguardar los derechos de terceros en detrimento de las libertades de los usuarios. Resulta de obligada observancia por cuanto se encuentra recogida en el RGPD, y su inaplicación debe ser fundada con el fin de garantizar la seguridad jurídica.

Por otro lado, basa su decisión en los criterios seguidos por numerosas sentencias, tanto del Tribunal Constitucional el Tribunal Supremo, todas ellas relativas al derecho al honor, intimidad, propia imagen y a la protección de la juventud y de la infancia, cuya tutela correspondería a los órdenes civil y penal, ante la falta de competencia de la AEPD por inaplicación de la normativa de protección de datos al amparo de la exención doméstica, que descartaría la existencia de un tratamiento de datos personales.

Por último, destacar la aplicación análoga de la decisión tomada por la Sentencia de 20 de octubre de 2011 de la Audiencia Nacional, Sala de lo Contencioso-administrativo (Rec.347/2009) «por la que se desestima recurso presentado contra resolución sancionadora de la Agencia Española de Protección de Datos por la publicación de un video en YOUTUBE con imágenes captadas en la calle de menores de edad que permiten su identificación*».* Aplicando así, la decisión de la AN referida a una plataforma de creación de contenido y algoritmos de recomendación como YouTube, a la publicación en una aplicación de mensajería instantánea como Telegram, sin tener en consideración las enormes diferencias existentes entre estas redes sociales en cuanto a la difusión de la información.

2.4. Puntos críticos susceptibles de mejora

2.4.1. Consideración a la diversidad de redes sociales

En primer lugar y con el fin de mantener la actividad en RRSS, con carácter general, dentro del ámbito de la *exención doméstica*, debe definirse minuciosamente lo que es considerado *personal* y lo que es considerado *doméstico* en este contexto, dada la dificultad de establecer una línea divisoria entre lo público y lo privado en el mundo de las RRSS y, una vez sentadas

estas definiciones, establecer una interpretación en cuanto a la necesidad o no, de cumplimiento de ambos conceptos en base a la conjunción «*O»,* con la que se redacta el artículo 2.2 RGPD.

Es evidente que no pueden existir derechos ni límites absolutos, pero tanto unos como otros deben ser ciertos y quedar bien definidos, ya que está en riesgo la seguridad jurídica, afectando a derechos tan fundamentales como la igualdad o la tutela judicial efectiva.

Se requieren unos criterios uniformes y actualizados que sean efectivos para comprender con exactitud los límites de esta exención, y para ello, las RRSS no deben ser entendidas como una única figura, sino que es necesario atender a la gran variedad de RRSS con las características y funciones con las que cuenta cada una de ellas de manera individual ya que estas características suponen una gran diferencia en cuanto al impacto para la privacidad que provoca la publicación de contenidos en unas y otras.

Han de distinguirse las RRSS de mensajería instantánea como puede ser WhatsApp, de plataformas con algoritmos de recomendación como pueden ser YouTube, Facebook o Instagram, donde la difusión puede ser masiva al implicar un riesgo de viralización sin necesidad de extraer la información de la propia plataforma como si sucede en aquellas de mensajería instantánea.

Deben tenerse en cuenta criterios específicos relativos al funcionamiento de las mismas, distinguiendo en primer lugar, las plataformas de creación y consumo de contenido que cuentan con algoritmos de recomendación o sugerencias, de aquellas destinadas a la mensajería instantánea y, dentro de estas, analizar funciones que van más allá, como puede ser la publicación de «*estados»* en WhatsApp, Telegram o Messenger, determinando el grado en que estas RRSS facilitan a usuarios ajenos a los contactos propios, el acceso a estas publicaciones mediante características que las diferencian, como el buscador de contactos con el que cuenta Telegram. Estos buscadores facilitan la búsqueda de otros usuarios por medio de nombres o apodos, contando incluso con sugerencias de usuarios con nombres similares a los que se introducen, con lo que, en este caso, el criterio de la restricción del contenido a usuarios determinados ganará importancia con respecto a WhatsApp que no dispone de este buscador y obliga a contar con el número de teléfono de cada usuario, lo cual impide el acceso a usuarios ajenos al círculo más estrecho del usuario.

En cualquier caso, el carácter público o privado de una cuenta de usuario en base al criterio de restricción de acceso, que viene empleándose de manera generalizada, debe ser complementado con otras observaciones debido a la realidad actual de las RRSS, especialmente en aquellas plataformas de creación masiva de contenido, donde la actividad normal ya no se desarrolla dentro del círculo más estrecho de contactos, lo que provoca la toma de decisiones y resoluciones discordantes con la realidad actual.

También han de tenerse en cuenta características y configuraciones como la eliminación automática de publicaciones con el transcurso del tiempo. WhatsApp implementa la eliminación por defecto en la publicación de «*estados»*, con lo que no supone el mismo riesgo que la publicación en otras plataformas donde permanecen con carácter indefinido.

2.4.2. Equilibrio entre derechos y deberes

Debe existir un equilibrio entre derechos y obligaciones en los bienes jurídicos protegidos.

En el caso de las RRSS, el aumento tan drástico de la libertad del usuario en la utilización de los datos personales ante la exención de responsabilidad que ampara su actividad, provoca un fuerte desbalance en el equilibrio entre esos derechos y obligaciones en torno a los datos personales.

La amplitud de las libertades de los usuarios debe implicar un refuerzo correlativo en las obligaciones exigibles, en este caso, a los responsables de las plataformas, no bastando la diligencia común y el cumplimiento de los principios y obligaciones exigidos por el RGPD a todo responsable del tratamiento, sino que esta debe contar con un plus de responsabilidad en aras de garantizar, o al menos disminuir, el impacto sobre la privacidad tanto de los usuarios como no usuarios.

Ejemplo de esta necesidad de refuerzo la encontramos en la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTAIBG), entorno a las administraciones públicas, donde el debilitamiento de los derechos del interesado, especialmente en cuanto al consentimiento para el tratamiento de sus datos personales y la comunicación entre administraciones, debe verse compensado mediante un refuerzo del deber de información.

En el ámbito de las RRSS es preciso encontrar este refuerzo en las obligaciones de los responsables, pero no en detrimento de la libertad de los usuarios pues esto iría en contra de la *exención doméstica* que les reconoce el Considerando 18 RGPD, sino mediante la exigencia de un mayor control a los responsables, mediante la implementación de funciones por defecto que contribuyan a la información de los interesados cuando sus derechos sean vulnerados.

El reconocimiento facial se ha llegado a utilizar incluso para la gestión de la «*galería de imágenes»* de los dispositivos móviles, permitiendo crear álbumes específicos en función de las personas que aparecen en cada imagen.

Si bien se prohíbe con carácter general el tratamiento de datos biométricos dado el alto riesgo que implican este tipo de datos, mediante una ponderación de derechos, podría prevalecer la implementación de esta medida, superando el requisito de necesidad del artículo 35.7.b) RGPD, aun implicando tecnologías de reconocimiento facial al configurarse como una medida de protección en beneficio de los interesados, con el fin exclusivo de informar, al menos a los usuarios registrados, cuando una publicación ajena incluya su imagen, permitiéndoles decidir si oponerse o no a la publicación ajena, o al menos, que su oposición suponga el difuminado o pixelado automático de su imagen, devolviendo a los interesados cierto control en el mundo de las RRSS, sobre su información personal.

3. Conclusiones

De lo expuesto en este trabajo, podemos extraer las siguientes conclusiones.

Primera.- Necesidad de una interpretación flexible por parte de los organismos competentes en la aplicación del RGPD

Nos encontramos en un contexto de constante cambio debido a la velocidad a la que avanza el mundo de las tecnologías y redes sociales. Por este motivo el panorama pronto será muy distinto, y la nueva realidad obligará a adaptar el marco normativo a las circunstancias de manera continua tal y como indica el principio clásico, *ius sequitur vitam*. Es así, que muchas de las observaciones contenidas en este estudio quedarán rápidamente obsoletas, de lo que se desprende la necesidad de abordar estos desafíos de una forma flexible que permita seguir el ritmo del desarrollo tecnológico.

Dada la naturaleza estática de los cuerpos legislativos, está adaptación continua debe llevarse a cabo de manera inevitable por medio de la interpretación por parte de los organismos competentes, en base a los criterios que vayan definiendo, bien mediante informes y guías de la AEPD, o bien mediante sus resoluciones y la jurisprudencia, lo que, en cualquier caso debe realizarse mediante una interpretación flexible o evolutiva de la normativa que adopte los conceptos más actuales del contexto digital con el fin de permitir una aplicación de la *exención doméstica* que sea coherente con la realidad actual de las RRSS.

Segunda.- Posibilidad de mejora en la redacción de los preceptos del RGPD

La certeza por parte de los ciudadanos en cuanto a la normativa vigente es parte de la garantía de un Estado de Derecho como el nuestro. Detalles que en principio parecen no tener importancia como las conjunciones «***Y***» u «***O***», pueden derivar en problemas de interpretación, provocando disparidad de criterios y resoluciones contradictorias por parte de los organismos competentes en la resolución de conflictos y afectando a quienes recaban el auxilio de la justicia al amparo de su derecho fundamental a la tutela judicial efectiva recogido en la Constitución.

El uso de la conjunción «***O***» entre dos posibilidades supone la aceptación más amplia posible, pues entre dos opciones cualquiera de ambas es válida. En la actualidad, para la aplicación de la *exención doméstica* debe admitirse tanto una actividad meramente *personal,* como una actividad meramente *doméstica*, sin la necesidad de concurrencia de ambas y por ello resulta imprescindible establecer una distinción clara de ambos conceptos lo que, desde luego, se solventaría con su inclusión entre las definiciones del artículo 4 RGPD con referencia al mundo de las RRSS.

En todo caso, si la intención del legislador fue la de utilizar los conceptos *personal* y *doméstico* como sinónimos, entonces bastaría con que la redacción del artículo 2.2.c) RGPD incluyese solo uno de ellos. Por el contrario, la inclusión de ambos conceptos supone la existencia de dos supuestos diferenciados con lo que, al amparo de la conjunción «***O***», bastará con el cumplimiento de cualquiera de ellos por separado para entender que la *exención doméstica* resulta plenamente aplicable a cualquier caso en cuestión. De este modo, un usuario estará en su derecho de ampararse en el uso personal por la falta de profesionalización, en su caso, de la actividad en redes, a pesar de la amplia difusión de la información cuando va más allá de una actividad doméstica como hemos visto.

Tercera.- Necesidad de actualizar los criterios interpretativos del GT29 empleados por los organismos competentes

Hemos comprobado que, en la actualidad, el riesgo de la difusión incontrolada de datos existe con independencia de las restricciones de acceso que un usuario pueda establecer en una determinada plataforma de RRSS, pues el mero hecho de publicar información en internet supone la pérdida de control de los datos ante la huella que deja toda información.

En el contexto actual de las redes sociales, la difusión de la información es sin duda la más amplia posible y, con esto en mente, la exclusión de la actividad en redes, del ámbito de aplicación del RGPD, no puede quedar limitada precisamente por la mera difusión, o al menos no exclusivamente por la difusión, independientemente del alcance.

Dada la tecnología actual, aquellos contactos que se encuentran dentro del círculo de amistades de un usuario concreto y que sí tienen acceso a su perfil, pueden tomar la información de manera sencilla y difundirla libremente, con lo que no constituye una

diferencia real o al menos, no efectiva, el hecho de que la información sea publicada en una cuenta de usuario privada, restringida a contactos determinados, pues esto dependerá del comportamiento de sus contactos o seguidores.

Contando con los tres criterios que en su día propuso el GT29, referidos a la actividad profesional, la limitación del público y la naturaleza de la información en cuanto a su sensibilidad, en el momento en el que se excluye la actividad profesional o la inclusión de categorías especiales de datos, nos encontramos ante un único criterio aplicable que determina la plena aplicación del RGPD a todo el contenido que se encuentra en plataformas de redes sociales destinadas a la creación y consumo de contenido masivo como son YouTube, los «*Reels»* de Instagram o TikTok entre otras, al tratarse de contenidos públicos accesibles a cualquier usuario sin restricciones. Teniendo en cuenta que esta es la actividad normal y esperada en las plataformas mencionadas, debemos concluir que, a día de hoy, lo doméstico ya no equivale a lo privado, al menos no en el contexto de las redes sociales y es aquí donde nos encontramos con una incompatibilidad entre el mundo del derecho y la realidad actual.

La actividad en RRSS es calificada como *actividad personal o domestica* por el RGPD mientras que la AEPD y la jurisprudencia, en aquellos supuestos en los que media una denuncia por publicaciones no consentidas, resuelven imponiendo sanciones fundadas en la necesidad de restringir el público, sin considerar la evolución de las redes sociales y su naturaleza actual, lo que significa tanto como permitir a los usuarios el desarrollo de su actividad con total libertad bajo la creencia de estar amparados en la *exención doméstica*, mientras que, por otro lado, esta libertad o exención será cierta en tanto en cuanto nadie interpone la correspondiente denuncia, momento en el cual, el autor incurre, de manera automática, en una infracción por tratamiento ilícito de datos personales.

De este modo, comprobamos que el criterio de la restricción de contenidos a usuarios concretos no se ajusta a la realidad actual de las RRSS y su aplicación supone tanto como negar los avances tecnológicos impidiendo la necesaria interpretación evolutiva del Derecho desde que el uso personal o doméstico de las RRSS ya no es equiparable a un uso que permanece en la esfera íntima o privada, convirtiendo a la *exención doméstica* en una mera declaración sin aplicación práctica que conlleva una inseguridad jurídica importante. Si bien encajaba con la naturaleza de las RRSS en sus inicios y servía para guiar el comportamiento de los usuarios en estos espacios digitales, el derecho debe adaptarse a la realidad social con la incorporación de

nuevos criterios compatibles tanto con las amplias diferencias entre redes sociales, como con el propósito o uso habitual y esperado de muchos de estos espacios digitales, que no es otro que la difusión de contenidos a nivel global.

Cuarta.- Debida separación de los derechos relacionados con la privacidad de las personas

La privacidad en internet y especialmente en RRSS, es un concepto casi ideal en la actualidad, que se enfrenta a una amenaza continua y requerirá un gran esfuerzo legislativo si ha de alcanzarse. No obstante, como hemos visto, la *exención doméstica* en el uso de las RRSS no supone el desamparo o la desprotección de los afectados ante las publicaciones no consentidas por parte de los usuarios, especialmente cuando se trata de información sensible. Para ello existe el derecho al honor, intimidad y propia imagen tutelados principalmente por la jurisdicción civil, pero es imprescindible comprender que el RGPD solo aplica al tratamiento de datos personales con independencia del contenido, permitiendo, dentro de unos límites, la publicación de todo tipo de información en redes sociales siempre y cuando no se englobe dentro del ámbito profesional, por lo que la tutela de los afectados deberá proporcionarse por medio del derecho común ante la jurisdicción competente.

Dada la enorme relación entre estos derechos destinados a la protección de la esfera privada de las personas frente a intromisiones ilegítimas, es fundamental precisar el alcance de cada uno de ellos en base al ámbito de aplicación de la normativa y acudir a la jurisdicción competente, de modo que la tutela efectiva quede garantizada, evitando de este modo, el conflicto de competencias que se produce *de facto* entre las distintas jurisdicciones donde, con el fin de salvaguardar los derechos de las personas de intromisiones ilegítimas que afectan a su privacidad, dignidad o imagen personal, se dictan resoluciones al amparo del derecho a la protección de datos en supuestos donde no existe un tratamiento de datos personales de conformidad con el RGPD, por medio de interpretaciones de la *exención doméstica* que resultan demasiado restrictivas a la luz de la actualidad social, afectando de manera directa a la seguridad jurídica en cuanto a la certeza sobre el ordenamiento jurídico por parte de los usuarios.

Referencias bibliográficas

Doctrina

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles*. [Consulta: abril de 2025]. Disponible en: https://www.aepd.es/guias/consecuencias-administrativas-disciplinarias-civiles-penales.pdf

BAÑO CARVAJAL, Á. E., y REYES ESTRADA, J. L. «Vulneración del derecho a la intimidad personal y familiar en las redes sociales». *Crítica y Derecho: Revista Jurídica*. 2020, vol. 1, núm. 1, pp. 49-60 [consulta: abril de 2024]. E-ISSN 2737-6281. Disponible en: https://revistadigital.uce.edu.ec/index.php/criticayderecho/article/view/2447/2518

CETINA PRESUEL, R. y MARTÍNEZ SIERRA, J. M. «Algoritmos y noticias: Redes sociales como editores y distribuidores de noticias». *Revista de Comunicación*, 2019, vol. 18, núm. 2, 261-285. Disponible en: https://doi.org/10.26441/RC18.2-2019-A13

CUELLO, C. «La privacidad individual y el impacto en ella de la tecnología de computadora». *Ciencia y Sociedad*, 1986, vol. XI, núm. 3, 291-308. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7483767

DE JESÚS OLIVEIRA K.E., DE MAGALHÃES PORTO, C., LUIZ ALVES, A. «Memes de redes sociais digitais enquanto objetos de aprendizagem na Cibercultura: da viralização à educação». *Acta Scientiarum. Education,* 2019, vol. 41, núm. 1, 1-11. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6775650.pdf

DOMÍNGUEZ MARTÍNEZ, S. «La publicación en las redes sociales de fotografías realizadas en ámbitos personales o domésticos». *La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, 2011, núm. 52. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7483767

FALCONÍ MONARD, D. N., ARGUDO PALOMEQUE, F. V. «Análisis de narrativas digitales de influencers de masculinidades de TikTok y su influencia en la viralización de contenido». *RUNAS. Journal of Education & Culture,* 2025, vol. 6, núm. 11, 1-22. Disponible en: https://doi.org/10.46652/runas.v6i11.227

GARCÍA ROCA, F.J. «Igualdad ante la ley», 828-830. Benigno Pendrás (ed.). *Enciclopedia de las Ciencias Morales y Políticas para el siglo XXI: Ciencias Políticas y Jurídicas (con especial referencia a la sociedad poscovid 19)*. Madrid: Boletín Oficial del Estado y Real Academia de Ciencias Morales y Políticas, 2020. Disponible en: https://racmyp.es/wp-content/uploads/2023/06/2020-0592_enciclopedia_ciencias_morales_acc_ee_final.pdf

GÓMEZ SALADO, M.A. *La cuarta revolución industrial y su impacto sobre la productividad, el empleo y las relaciones jurídico-laborales: Desafíos tecnológicos del siglo XX.* Navarra: Aranzadi, 2021.

HERMOSO RUIZ, F. «Redes Sociales». *Aula Magna Extremadura*, 2010, núm. 29, 22. Disponible en: https://programamayores.unex.es/wp-content/uploads/sites/72/2024/07/revista-aula-magna-29.pdf

MOLINA HERMOSILLA, O. «Inteligencia artificial, Bigdata y Derecho a la protección de datos de las personas trabajadoras». *Revista de Estudios Jurídico Laborales y de Seguridad Social (REJLSS)*, 2023, núm. 6, 89-117. Disponible en: https://dialnet.unirioja.es/descarga/articulo/8954369.pdf

OLIVERAS JANÉ, N. «La ley de igualdad en perspectiva constitucional», 39-53. Inma Pastor Gosálbez (coord.). *Una ley para la igualdad: Avances y desafíos 15 años después de la aprobación de la L.O. 3/2007 para la igualdad efectiva de mujeres y hombres*. Tarragona: Publicacions de la Universitat Rovira i Virgili, 2023. Disponible en: https://llibres.urv.cat/index.php/purv/catalog/view/540/561/1237

PÉREZ, I. «Metadatos: tus fotos podrían mostrar más de lo que ves» [en línea]. *Welivesecurity*. 19 diciembre 2022 [consulta: 10 mayo 2025]. Disponible en: https://www.welivesecurity.com/la-es/2022/12/19/metadatos-fotos-podrian-mostrar-mas/?utm_source=chatgpt.com

PÉREZ RUFÍ, J. P. YouTube y la economía del algoritmo, Biblioteca virtual de Derecho, Economía, Ciencias Sociales y Tesis Doctorales, Málaga, 2019. Disponible en: https://www.eumed.net/libros/1844/index.html

RAVENTÓS PAJARES, P. «Los Metadatos: Qué son y para qué sirven». *Revista d'arxius*, 2009, núm. 8, 9-32. Disponible en: https://arxiversvalencians.org/wp-content/uploads/2020/04/revista2009_raventos.pdf

SÁEZ DE PROPIOS, M. «La libertad de expresión en el nuevo estilo de comunicación de las redes sociales: ¿Quién pone los límites?». *Revista Jurídica de Castilla y León*. 2025, 161-191. ISSN 2254-3805. Disponible en: https://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1131978346397/Publicacion/1285473758986/Redaccion

SERRANO BONILLA, G. «Las implicaciones jurídicas de la utilización del término "y/o" en los contratos bancarios». *Revista Jurídica*. 1991, actualización 2016, núm. 3, 81-99. Disponible en: https://www.revistajuridicaonline.com/wp-content/uploads/1991/02/03_Implicaciones_Juridicas_De_Utilizacion_Del_Term.pdf

SERRANO-COBOS, J. «Big data y not so big data». *Anuario ThinkEPI*. 2013, vol. 7, núm. 1, 161-163, ISSN 1886-6344. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4234739.pdf

SUÁREZ RUBIO, S. M. «Los menores como usuarios de redes sociales y su privacidad». *Parlamento y Constitución. Anuario*, 2014, núm. 16, 115-140. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7483767

WARREN, S. y BRANDEIS, L. D. «The Right to Privacy». *Harvard Law Review*. 1980, vol. 4, núm. 5, 193-220. Disponible en: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

WESTIN, A. F. *Privacy and Freedom*. New York: Atheneum, 1967, 7.

Recursos web

«Europa multa a TikTok con 530 millones de euros por la protección de datos». *La Vanguardia*. 10 mayo 2025, 19:57. Disponible en: https://www.lavanguardia.com/vida/20250502/10640009/europa-multa-tiktok-530-millones-euros-proteccion-datos.html

«Protección de datos». *Abogacía Española Consejo General*. 17 abril 2025, 18:13. Disponible en: https://www.abogacia.es/conocenos/bruselas/documentos-juridicos-y-utilidades/fichas-legislativas-ue/proteccion-de-datos/

«Las fotos de la cena de navidad del trabajo». *AEPD*. 2 mayo 2025, 18:41. Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/las-fotos-de-la-cena-de-navidad-del-trabajo

«Información para las personas que no usan productos de Meta». *Facebook*. 18 abril 2025, 18:28. Disponible en: https://www.facebook.com/help/637205020878504/?locale=es_ES

«Política de privacidad». *Facebook*. 26 abril 2025, 13:23. Disponible en: https://es-es.facebook.com/privacy/policy?section_id=1-WhatInformationDoWe

«Obtener ingresos en YouTube». *Google*. 18 abril 2025, 18:38. Disponible en: https://support.google.com/youtube/answer/72857?sjid=4604223167075288228-EU

«¿Qué puedo hacer si se difunden imágenes en las que aparezco?». *AEPD*. 17 abril 2025, 16:13. Disponible en: https://www.aepd.es/preguntas-frecuentes/17-internet-y-redes-sociales/FAQ-1704-que-hacer-si-se-difunden-imagenes-en-las-que-aparezco

«Protección de datos y privacidad online». *Web oficial de la Unión Europea*. 18 abril 2025, 18:10. Disponible en: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_es.htm

Real Academia Española. Disyuntivo. En: *Diccionario de la lengua española* [en línea]. 23 ed., sin fecha [consulta: 17 abril 2025]. Disponible en: https://dle.rae.es/disyuntivo

Real Academia Española. Coordinación copulativa y pluralidad. En: *Diccionario de la lengua española* [en línea]. 23 ed., sin fecha [consulta: 17 abril 2025]. Disponible en: https://www.rae.es/gram%C3%A1tica/sintaxis/coordinaci%C3%B3n-copulativa-y-pluralidad

Real Academia Española. La coordinación disyuntiva. En: *Diccionario de la lengua española* [en línea]. 23 ed., sin fecha [consulta: 17 abril 2025]. Disponible en: https://www.rae.es/gram%C3%A1tica/sintaxis/la-coordinaci%C3%B3n-disyuntiva

Museonat Actividades. *Las redes sociales y sus implicaciones en protección de datos* [Vídeo]. YouTube, 30 de octubre 2023 [consulta: 18 de abril 2025]. Disponible en: https://www.youtube.com/watch?v=grvSxeG8Iv0

«Qué son los metadatos y cómo eliminarlos». *INCIBE*. 1 junio 2025, 13:32. Disponible en: https://www.incibe.es/empresas/blog/son-los-metadatos-y-eliminarlos

DOÑA, C. «Cómo pedir a Meta que No use tus Datos para Entrenar su IA» [en línea]. *Metricool*. 28 mayo 2025 [consulta: 1 junio 2025]. Disponible en: https://metricool.com/es/como-pedir-a-meta-que-no-use-tus-datos-para-entrenar-ia/

Legislación citada

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado, 3 de junio de 1982, núm. 115. Disponible en: https://www.boe.es/eli/es/lo/1982/05/05/1/con

Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, 23 de noviembre de 1995, núm. 281. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Dictamen 5/2009, del Grupo de Trabajo sobre Protección de Datos del Artículo 29, de 12 de junio de 2009, sobre las redes sociales en línea (01189/09/ES WP 163) [consulta: abril de 2025]. Disponible en: https://www.samuelparra.com/wp-content/uploads/2010/01/dictamen-5-2009-g29.pdf

Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 25 de enero de 2012, 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 (Reglamento general de protección de datos). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012PC0011

SUPERVISOR EUROPEO DE PROTECCÓN DE DATOS. Opinion of the European Data Protection Supervisor, de 7 de marzo de 2012 [consulta: mayo de 2024]. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Boletín Oficial del Estado, 10 de diciembre de 2013, núm. 295. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887

Propuesta de Directiva del Parlamento Europeo y del Consejo, de 9 de diciembre de 2015, relativa a determinados aspectos de los contratos de suministro de contenidos digitales. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015PC0634&from=LV

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). Diario Oficial de la Unión Europea, 4 de mayo de 2016, núm. 119. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, núm. 294. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, de 2 de septiembre de 2020 [consulta: noviembre de 2024]. Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_es

Jurisprudencia referenciada

Sentencia del Tribunal Constitucional, núm. 15/1986 de 31 de enero de 1986, ECLI:ES:TC:1986:15. Disponible en: https://vlex.es/vid/1-2-lpl-15034373

Sentencia de 26 de marzo de 1987, Leander v. Suecia, C-9248/81, ECLI:CE:ECHR:1987:0326JUD000924881. Disponible en: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22leander%20v.%20suecia%22],%22languageisocode%22:[%22SPA%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-165080%22]}

Sentencia del Tribunal Constitucional, núm. 46/1990 de 15 de marzo de 1990, ECLI:ES:TC:1990:46: https://vlex.es/vid/1-2-3-9-c-15356978?_gl=1*oek73t*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Constitucional, núm. 150/1990 de 4 de octubre de 1990. Disponible en: https://vlex.es/vid/an-32-lotc-f-31-v-33-ba-149-15356876?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Constitucional, núm. 36/1991 de 14 de febrero de 1991, ECLI:ES:TC:1991:36. Disponible en: https://vlex.es/vid/stc-aatc-35-lotc-ma-t-as-i-an-8-9-15356776?_gl=1*oek73t*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Constitucional, núm. 142/1993 de 22 de abril de 1993. Disponible en: https://vlex.es/vid/j-64-ba-15356182?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Constitucional, núm. 212/1996 de 19 de diciembre de 1996. Disponible en: https://vlex.es/vid/stc-53-sstc-32-37-35-36-15355214?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Constitucional, núm. 104/2000 de 13 de abril de 2000, ECLI:ES:TC:2000:104. Disponible en: https://vlex.es/vid/ri-16-1990-143351?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia de 4 de mayo de 2000, Rotaru v. Rumanía, C-28341/95, ECLI:CE:ECHR:2000:0504JUD002833195. Disponible en: https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%2228341/95%20rotaru%20v.%20rumania%22],%22languageisocode%22:[%22SPA%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-162581%22]}

Sentencia del Tribunal Constitucional, núm. 96/2002 de 25 de abril de 2002. Disponible en: https://vlex.es/vid/154139?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia del Tribunal Supremo, núm. 312/2003 de 5 de marzo de 2003. Disponible en: https://vlex.es/vid/trafico-tenencia-armas-presuncion-inocencia-15556379

Sentencia de 6 noviembre 2003, Lindvisq, C-101/01, EU:C:2003:596 [consulta: abril de 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

Sentencia del Tribunal Constitucional, núm. 248/2007 de 13 de diciembre de 2007, ECLI:ES:TC:2007:248. Disponible en: https://vlex.es/vid/2003-76-32-30-stc-35309391?_gl=1*11letqa*_up*MQ..*_ga*OTAwMDE5OTE0LjE3NDU5NDg0NDg.*_ga_XYV763W66C*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA..*_ga_M8NHSPJ5LE*MTc0NTk0ODQ0Ni4xLjAuMTc0NTk0ODQ0Ni4wLjAuMA

Sentencia de 4 de diciembre de 2008, S. y Marper v. Reino Unido, CC-30562/04 y 30566/04. Disponible en: https://hudoc.echr.coe.int/spa?i=001-90051

Sentencia del Tribunal Constitucional, núm. 136/2011 de 13 de septiembre de 2011. Disponible en: https://vlex.es/vid/327223095

Sentencia del Tribunal Constitucional, núm. 234/2012 de 13 de diciembre de 2012. Disponible en: https://vlex.es/vid/414837586

Sentencia de 13 de mayo de 2014, Google Spain, S.L: y Google Inc. contra Agencia Española de Protección de datos (AEPD) y Mario Costeja González, C-131/12, ECLI:EU:C:2014:317. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131

Sentencia de la Audiencia Nacional, núm. 2264/2018 de 11 de mayo de 2018, ECLI:ES:AN:2018:2264. Disponible en: https://www.poderjudicial.es/search/AN/openDocument/00ca14b4570a9695/20180614

Sentencia del Tribunal Supremo, núm. 904/2023 de 3 de julio de 2023. Disponible en: https://vlex.es/vid/939424800

Resoluciones AEPD

Agencia Española de Protección de Datos. Informe 0615/2008. Disponible en: https://www.aepd.es/documento/2008-0615.pdf

Agencia Española de Protección de Datos. Informe 0077/2013. Disponible en: https://www.aepd.es/documento/2013-0077.pdf

Agencia Española de Protección de Datos. Resolución de archivo de actuaciones, E/03872/2012, 20 de marzo de 2013. Disponible en: https://www.aepd.es/documento/e-03872-2012.pdf

Agencia Española de Protección de Datos. Resolución de procedimiento sancionador, PS/00070/2016, 20 de julio de 2016. Disponible en: https://www.aepd.es/documento/ps-00070-2016.pdf

Agencia Española de Protección de Datos. Resolución de procedimiento sancionador, PS/00695/2014, 28 de Octubre de 2016. Disponible en: https://www.aepd.es/documento/ps-00695-2014.pdf

Agencia Española de Protección de Datos. Resolución de archivo de actuaciones, E/01849/2018, 17 de julio 2018. Disponible en: https://www.aepd.es/documento/e-01849-2018.pdf

Agencia Española de Protección de Datos. Resolución de archivo de actuaciones, E/01825/2019, 9 de abril de 2019. Disponible en: https://www.aepd.es/documento/e-01825-2019.pdf

Agencia Española de Protección de Datos. Resolución de procedimiento sancionador, PS/00334/2019, 18 de diciembre 2019. Disponible en: https://www.aepd.es/documento/ps-00334-

2019.pdf?fbclid=IwAR1IT0sV8Thc7y3HtBZgM7YOqdPRZXksi6o5xs2MOvxNhV9b922qMNIv404

Agencia Española de Protección de Datos. Resolución de procedimiento sancionador, PS/00126-2024, 23 de septiembre de 2024. Disponible en: https://www.aepd.es/documento/ps-00126-2024.pdf

Agencia Española de Protección de Datos. Resolución de archivo de actuaciones, AI/00404/2024, 3 de Octubre de 2024. Disponible en: https://www.aepd.es/documento/ai-00404-2024.pdf

Agencia Española de Protección de Datos. Resolución de procedimiento de apercibimiento, PA/00078/2023, 11 de marzo de 2025. Disponible en: https://www.aepd.es/documento/pa-00078-2023.pdf

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos.

AN: Audiencia Nacional.

CE: Constitución Española.

CEDH: Convenio Europeo de Derechos Humanos.

GT29: Grupo de Trabajo del artículo 29.

IA: Inteligencia Artificial.

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

LTAIBG: Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

RAE: Real Academia Española.

RGPD: 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 (Reglamento general de protección de datos).

RRSS: Redes Sociales.

SAN: Sentencia de la Audiencia Nacional.

SEPD: Supervisor Europeo de Protección de Datos.

SRS: Servicios de redes sociales.

STC: Sentencia del Tribunal Constitucional.

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea.

STS: Sentencia del Tribunal Supremo.

TC: Tribunal Constitucional.

TEDH: Tribunal Europeo de Derechos Humanos.

TIC: Tecnologías de la Información y Comunicación.

TS: Tribunal Supremo.

UE: Unión Europea.