



Facultad de Ciencias Sociales y Jurídicas de Elche

Grado en Derecho

## Trabajo Fin de Grado

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS,  
¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**



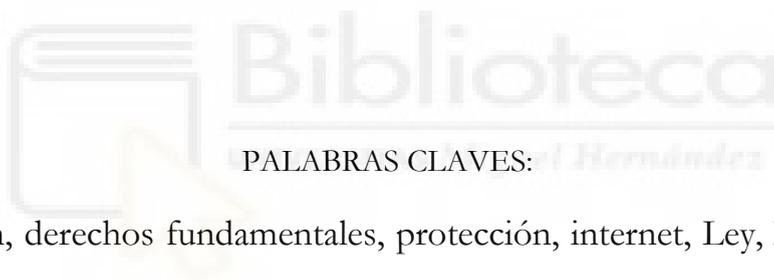
Curso académico 2020/2021

**ALUMNO: Luis Daniel Sánchez López**

TUTOR: Francisco Javier Sanjuán Andrés

**NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ  
SIENDO REALMENTE RESPETADO EN INTERNET?  
RESUMEN**

En el trabajo que vamos a presentar abordamos las problemáticas que nos podemos encontrar a la hora de la protección de nuestros derechos fundamentales en internet, más concretamente, la protección de nuestro derecho a la intimidad y nuestro derecho a la protección de datos. Para ello ha sido necesario llevar a cabo un breve análisis de los derechos constitucionales vinculados al tema principal de este trabajo, recogidos en el artículo 18 Constitución Española –en adelante, CE-, exactamente 18.1 CE y el 18.4. También analizaremos y explicaremos el marco jurídico relacionado a los derechos anteriormente nombrados y a la jurisprudencia que ha tenido cierta relevancia a la hora de tratar con la protección de estos derechos frente a terceros. Finalmente una vez terminado el citado análisis reflexionaremos sobre algunos ejemplos que puedan o hayan vulnerado los derechos antes citados.



PALABRAS CLAVES:

Constitución, derechos fundamentales, protección, internet, Ley, Reglamento, Unión Europea.

SUMMARY

In the present work, we address the problems we may encounter when it comes to the protection of our Fundamental Rights on the internet, specifically the protection of our Privacy and Data protection's rights. For this it has been necessary to carry out a brief analysis of the constitutional rights linked to the main theme of this work, collected in article 18 CE, exactly in the 18.1 and 18.4. We will also analyze and explain the legal framework related to the previous mentioned rights and to the jurisprudence that has had some relevance when dealing with the protection of these rights against thirds. Finally, once the previous mentioned analysis is finished, we will reflect on some examples that have or may have violated this rights.

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO  
REALMENTE RESPETADO EN INTERNET?**

KEYWORDS

Constitution, fundamental rights, protection, internet, Law, Regulation,  
European Union.



**NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

**ABREVIATURAS**

AEDP	Agencia Española de Protección de Datos.
CE	Constitución Española 1978
GDPR	Reglamento General de Protección de Datos de la Unión Europea.
LOPD	Ley Orgánica de Protección de Datos.
STC	Sentencia del Tribunal Constitucional.
TC	Tribunal Constitucional.
TJUE	Tribunal de Justicia de la Unión Europea.
UE	Unión Europea.
UMH	Universidad Miguel Hernández.



DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO  
REALMENTE RESPETADO EN INTERNET?

ÍNDICE

1. INTRODUCCIÓN.....	7
2. ¿QUÉ SON LOS DERECHOS FUNDAMENTALES Y QUE DERECHO O DERECHOS VAMOS A TRATAR EN ESTE TRABAJO ?.....	7
2.1 Derecho a la intimidad art. 18.1 CE.....	8
2.2 Derecho a la protección de datos art. 18.4 CE.....	8
3. MARCO LEGISLATIVO.....	9
3.1 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.....	9
3.2 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	10
3.3 Reglamento General de Protección de Datos de la Unión Europea.....	16
4. JURISPRUDENCIA.....	19
4.1 Facebook.....	19
4.1.1 C-40/17 del TJUE.....	19
4.2 Google.....	23
4.2.1 C-131/12 del TJUE.....	23
5. CÓMO LA FALTA DE INFORMACIÓN, AFECTA A LA CIUDADANÍA Y PERMITE LA VULNERACIÓN DE LOS DERECHOS NOMBRADOS ANTERIORMENTE.....	28
6. EJEMPLOS SOBRE SITUACIONES DONDE PUEDEN HABERSE VISTO VULNERADO NUESTRO DERECHO A LA INTIMIDAD O A LA PROTECCIÓN DE DATOS.....	29
6.1 Dot SCV- ¿Te escucha Google a través del móvil? -Análisis y experimento.....	29
6.2 Artículo relacionado con las multas que se ciernen sobre las grandes empresas de internet THE ECONOMIST.....	30
7. CONCLUSIONES.....	32
8. FUENTES CONSULTADAS.....	33
8.1 Bibliográficas.....	33

NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

8.2	<i>Legislativas.....</i>	<i>33</i>
8.2.1	<i>Españolas.....</i>	<i>33</i>
8.2.2	<i>Europeas.....</i>	<i>34</i>
8.3	<i>Otras fuentes consultadas.....</i>	<i>34</i>
8.3.1	<i>Periodísticas.....</i>	<i>34</i>
8.3.2	<i>Jurisprudenciales.....</i>	<i>35</i>
8.3.3	<i>Audiovisuales o internet.....</i>	<i>35</i>



## **1. Introducción.**

En este trabajo de investigación titulado " Derecho a la intimidad y a la protección de datos, ¿Está siendo realmente respetado en internet?" se analiza si la protección que disfrutamos de nuestros derechos en internet es respetada por terceros y es suficiente.

Para dar una respuesta basada en derecho a una cuestión como la nombrada en el título es necesario que en los siguientes apartados se lleve a cabo un análisis de la Constitución, más concretamente de los derechos fundamentales en ella recogidos así como de las leyes y artículos que regulan la protección de estos derechos.

Para ello haremos uso de la metodología propia de la ciencia jurídica, realizando una revisión doctrinal, legislativa y jurisprudencial a nivel estatal cumpliendo con todo ello, los objetivos generales de los trabajos de investigación de fin de grado y los específicos de este en concreto.

## **2. ¿Qué son los derechos fundamentales y que derecho o derechos vamos a tratar en este trabajo?**

A continuación nos centraremos en la definición o conceptualización de los derechos fundamentales, qué tienen de especial y en qué se diferencian de otros derechos como por ejemplo los derechos humanos. También veremos y haremos un pequeño análisis de los derechos fundamentales que trataremos en este trabajo, que son: el derecho a la intimidad y el derecho a la protección de datos.

Serán derechos fundamentales todos aquellos privilegios o garantías inherentes a las personas y que se encuentran expresados y regulados en el ordenamiento jurídico de un país.

Los derechos fundamentales al derivar directamente de los derechos humanos, suelen confundirse y usarse como si fueran iguales; sin embargo son dos conceptos distintos.

Por un lado tenemos a los derechos humanos los cuales son "*universales*"<sup>1</sup> y por otro lado tenemos a los derechos fundamentales que "*solo se aplican dentro del territorio al cual pertenecen las leyes que los contemplan*"<sup>2</sup>.

---

<sup>1</sup> "Derechos fundamentales" Significados.com 24/01/2020 Consultado 26/01/2021.  
¿Qué son los derechos fundamentales y cuáles son los más importantes? - Significados

<sup>2</sup> "Derechos fundamentales" Significados.com 24/01/2020 Consultado 26/01/2021.  
¿Qué son los derechos fundamentales y cuáles son los más importantes? - Significados

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

Los derechos fundamentales están recogidos y regulados en la Constitución, sin embargo pueden ser desarrollados mediante ley y específicamente mediante ley orgánica cuando afecte al contenido esencial del derecho -artículo 53 CE-.

### 2.1 Derecho a la intimidad art, 18.1 CE

*“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”<sup>3</sup>.*

El derecho a la intimidad se define como “derecho de disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre”.

Aquellos que pueden disfrutar de este derecho son toda persona física, sin embargo, las personas jurídicas solo disfrutarán del derecho al honor y al domicilio (inviolabilidad del domicilio).

El ámbito de aplicación del derecho a la intimidad comprende el derecho a la intimidad familiar y corporal.

El derecho a la intimidad es un derecho relativamente reciente, debido a la necesidad de protección de la misma a causa de la rápida evolución de las nuevas tecnologías. El Tribunal Constitucional explica de una forma clara la necesidad de protección nombrada anteriormente: *“el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto de la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De ahí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que, por cualquier medio, puedan realizarse en ese ámbito reservado de la vida”<sup>4</sup>. El derecho a la intimidad conlleva según el Tribunal Constitucional *“la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana”<sup>5</sup>.**

### 2.2 Derecho a la protección de datos art. 18.4 CE

*“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”<sup>6</sup>*

---

<sup>3</sup> Constitución Española. Boletín Oficial del Estado, Artículo 18.1, 29 de diciembre 1978.

<sup>4</sup> STC 110/84, de 26 de noviembre, FJ 3.º

<sup>5</sup> STC 231/88, de 2 de diciembre, FJ 3.º

<sup>6</sup> Constitución Española. Boletín Oficial del Estado, Artículo 18.4, 29 de diciembre 1978.

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

El derecho a la protección de datos radica en la protección de nuestra información personal contra terceros para que no pueda ser tratada sin nuestro consentimiento.

Éste derecho está regulado por el Reglamento General de Protección de Datos de la Unión Europea (en adelante GDPR), la Constitución Española (en adelante CE) y la Ley Orgánica de Protección de Datos (en adelante LOPD). La autoridad pública encargada de velar por el cumplimiento de las normas relativas a la seguridad de los datos privados es la Agencia Española de Protección de Datos (en adelante AEPD).

La AEDP actúa de forma autónoma pero se encuentra bajo el mando del Ministerio de Justicia.

La AEDP es donde debemos acudir cuando las empresas hayan recabado nuestra información sin nuestro consentimiento, utilicen nuestra información para fines no establecidos en el acuerdo, no dispongan de un consentimiento válido para tratar nuestra información o se nieguen a respetar nuestros derechos.

Por último señalar que la AEDP es la encargada de imponer sanciones pecuniarias cuando se conozca de un incumplimiento legal.

### **3. Marco legislativo.**

Para un mejor entendimiento del tema sobre el que versa el trabajo necesitamos profundizar y analizar de manera breve el contexto normativo que rodea el fondo del asunto del estudio que estamos llevando a cabo.

En este apartado nos centraremos en examinar dos leyes que es importante que sean comentadas, ya que, al tener una relación con el tema a tratar en este trabajo es necesario que las interpretemos.

Las leyes que vamos a ver son: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. También abordaremos el Reglamento General de Protección de Datos de la Unión Europea.

#### **3.1 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.**

La Ley 34/2002, de 11 de julio, tiene como objeto la implementación a nuestro ordenamiento jurídico la Directiva 2000/31/CE, del

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

Parlamento Europeo y del Consejo, de 8 de junio, concerniente a señalados aspectos de los servicios de la sociedad de la información, concreto, los servicios relacionados con el comercio electrónico.

También destacar que integra de manera parcial la Directiva 98/27/CE, del Parlamento Europeo y del Consejo. De 19 de Mayo, centrada en las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, acciones de cesación contra los comportamientos que estén en contra de lo dispuesto en la Ley.

El origen de esta Ley se encuentra en la asombrosa y rápida evolución y expansión de internet y la necesidad por parte de los Estados de proveer una protección legítima y apropiada de los derechos de los consumidores, debido a que la incorporación de la vida social y económica en internet ofrece numerosas ventajas, como nuevas fuentes de empleo, también es necesaria la implementación de un marco jurídico adecuado para así salvaguardar la confianza de todos aquellos individuos que intervienen en este nuevo medio.

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

A los efectos del trabajo de fin de grado consideramos que para tener una mejor comprensión del tema principal que estamos tratando, es necesario un análisis más minucioso de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Antes de empezar el análisis de esta Ley es necesario explicar qué es una Ley Orgánica y en que se diferencian dichas Leyes Orgánicas de las otras Leyes.

La definición de Ley Orgánica la encontramos recogida en el artículo 81.1 de la Constitución Española y dice así: *“Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.”*<sup>7</sup>, es decir: las Leyes Orgánicas son Leyes que regulan materias constitucionalmente reservadas a las mismas, como por ejemplo, el desarrollo de los derechos fundamentales y de las libertades públicas entre otros.

La CE en su artículo 81.2 regula los métodos de aprobación, modificación o derogación de las mismas, en los que serán necesarios una mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto. *“La aprobación, modificación o derogación de las leyes*

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

*orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto*<sup>8</sup>.

En lo que respecta a las Leyes ordinarias, abarcan todas las materias no reservadas expresamente a las Leyes Orgánicas. En cuanto al método de aprobación, no requiere cómo obtener la mayoría absoluta requerida por el derecho común. Por lo tanto, la Ley ordinaria se aprobará por mayoría simple en la Cámara. En vista de todo esto, podemos decir muy claramente cuál es la diferencia entre unos y otros. Por tanto la relación entre Ley ordinaria y Ley Orgánica rige el principio de competencia.

Una vez visto que es una Ley Orgánica y en que se diferencia con el resto de Leyes, pasaremos a analizarla.

La primera cosa que vamos a hacer es señalar que esta Ley está compuesta por noventa y siete artículos que están organizados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

A diferencia de la normativa general, el Título I establece en primer lugar el objeto de la Ley Orgánica. Según el contenido señalado, el objeto es dual. Por tanto, en primer lugar, su finalidad es adecuar el ordenamiento jurídico español al Reglamento (UE) 2016/679 “Reglamento General de Protección de Datos” emitido por el Parlamento Europeo y el Consejo el 27 de abril de 2016, y completar sus disposiciones. A su vez, determinó que las personas físicas amparadas por el artículo 18.4 de la Constitución ejercerán sus derechos básicos al disfrute de los datos personales de acuerdo con el Reglamento (UE) 2016/679 y lo dispuesto en esta Ley Orgánica. Las comunidades autónomas tienen el poder de regular el desarrollo y hacer cumplir los derechos básicos de protección de datos personales en sus campos de actividad, y los organismos autónomos de protección de datos consideran que tienen la responsabilidad de ayudar a proteger este derecho civil básico. En segundo lugar, de acuerdo con el artículo 18.4 de la Constitución, la ley también tiene por objeto proteger los derechos digitales de la ciudadanía.

Llama la atención la nueva normativa relativa a los datos del fallecido porque tras excluir el tratamiento del fallecido del ámbito de aplicación de la ley, permite a las personas en contacto con el fallecido por motivos familiares o de facto o sus herederos solicitar también el acceso a ellos mismos como corrección o supresión estarán sujetos a las instrucciones del fallecido cuando corresponda.

---

<sup>8</sup> Constitución Española. Boletín Oficial del Estado, Artículo 81.2, 29 de diciembre 1978.

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

En el Título II "Principios de Protección de Datos", se determina que en lo que respecta al Reglamento (UE) 2016/679, no serán atribuidos al responsable del tratamiento, siempre que haya tomado todas las medidas razonables para detener o corregir la inexactitud de los datos recibidos por el afectado, cuando hubiera obtenido los datos de otro responsable mediante el ejercicio del derecho de portabilidad por parte del afectado o cuando obtuviese los datos del mediador o cuando hubieren sido obtenidos del registro público. También incluye claramente las obligaciones de confidencialidad, el procesamiento de datos protegidos por la ley, categorías especiales de datos y el procesamiento de datos delictivos, especialmente cuando se trata de consentimiento. Estos deben provenir de una declaración o acción clara sobre lo siguiente: la parte afectada no incluye el consentimiento tácito, es decir, el consentimiento de la parte afectada debe expresarse claramente para múltiples propósitos, y debe otorgarse a todos los propietarios, y se mantiene a la edad de catorce años la edad a partir de la cual los menores pueden estar de acuerdo.

Cuando dicho tratamiento provenga del ejercicio del poder público o del cumplimiento de obligaciones legales, también podrán imponerse condiciones especiales, como medidas de seguridad adicionales u otras medidas, y tales condiciones especiales sólo podrán ser consideradas en función de las tareas desempeñadas por el interesado o el ejercicio de los poderes públicos otorgados al responsable por los derechos estipulados en el reglamento europeo que se fundamenta en la autoridad otorgada por la ley. Y conserva la prohibición de procesamiento por consentimiento con el fin de almacenar la información de identificación de ciertos tipos de datos especialmente protegidos, lo que no impedirá que sean procesados en otras circunstancias especificadas en el Reglamento (UE) 2016/679.

El Título III, está dedicado a los derechos de las personas, es de aplicación a la legislación española y es el principio de transparencia de la normativa europea, que regula el derecho de conocimiento de los afectados y recoge la denominada "información por capas". Y suele ser aceptado en campos como la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (como las "cookies"), y proporciona información básica para el afectado, aunque le da la dirección electrónica u otra dirección que permita un acceso sencillo y directo a la información restante.

El Título IV contiene "Normativa aplicable a tratamientos específicos", que contiene una serie de supuestos que no deben considerarse exhaustivos de todos los tratamientos legales en ningún caso. Entre ellos, lo primero que se puede entender es que el legislador estableció la

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

presunción "iuris tantum" de que prevalecen los derechos e intereses legales del responsable de acuerdo con una serie de requisitos. Cuando no se cumplan las condiciones previstas en el texto cumplido estrictamente, esto no descarta la licitud de dicho tratamiento, aunque en este caso, el responsable deberá realizar la ponderación exigida por la ley, pues no se puede asumir la universalidad de sus derechos legales. Además de estos supuestos, también se incluyen otros contenidos, como la videovigilancia, los documentos de exclusión publicitaria o los sistemas internos de denuncia, en los que, según el artículo 6.1.e) del Reglamento de la Unión Europea 2016/679, la legalidad del tratamiento deriva de la existencia de interés público. Finalmente, en este título, mencionar la legalidad de otros métodos de procesamiento especificados en el Capítulo IX del Reglamento, como los métodos de procesamiento relacionados con funciones estadísticas o con fines de archivo para fines generales.

El Título V se refiere a quien es el responsable y quien es el encargado del tratamiento. Hay que considerar que la mayor novedad que propone el Reglamento (UE) 2016/679 es la evolución de un modelo que se basa fundamentalmente en el control del cumplimiento a otro modelo que se basa en el principio de responsabilidad activa, que requiere que el personal encargado o responsable realice una evaluación con antelación de los riesgos que puedan derivarse del tratamiento de los datos personales por parte del responsable, de manera que se puedan tomar las medidas oportunas en base a la valoración anterior. Para aclarar estas novedades, la Ley Orgánica mantiene el mismo título del Capítulo 4 del "Reglamento" y divide cada cláusula en cuatro capítulos, que se dirigen respectivamente a las medidas generales de responsabilidad activa y al sistema de responsables. El mecanismo de identidad y autorregulación y autenticación del delegado de protección de datos. Cabe destacar que el delegado de protección de datos permite configurar un método amigable de resolución de reclamaciones, pues un interesado puede copiar reclamaciones que no fueron tramitadas por el responsable o el encargado de llevarlo a cabo.

El Título VI trata sobre transmisión internacional de datos y se centra en lo dispuesto en el Reglamento (UE) 2016/679, que hace referencia a un determinadas especialidades relativas a los procedimientos para que la agencia de protección de datos apruebe modelos de contrato o normas societarias vinculantes y autorice casos Transferencia o información previa.

El Título VII está dedicado a las agencias de protección de datos autorizadas de acuerdo con la normativa (UE) 2016/679, y debe ser establecido por la legislación nacional. La Ley Orgánica mantiene los

## **NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

esquemas recogidos en sus precedentes normativos, regulando así el sistema de la Agencia Española de Protección de Datos y reflejando la existencia de agencias autonómicas de protección de datos y la necesaria cooperación entre agencias de control. Según la Ley N ° 40/2015, de 1 de octubre, de ordenamiento jurídico del sector público, la Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente, y que se relaciona con el gobierno a través del Ministerio de Justicia.

El Título VIII recoge "los procedimientos en las situaciones en las que se puedan vulnerar la normativa de protección de datos". El Reglamento (UE) 2016/679 establece un nuevo sistema complejo, avanzando hacia un modelo de "ventanilla única", en el que existe una importante agencia reguladora y otras agencias relacionadas. También establece un procedimiento de cooperación entre las autoridades de los estados miembros y proporciona una decisión vinculante de la Comisión Europea de Protección de Datos en caso de discrepancias. Por tanto, antes de tramitar cualquier trámite, es necesario determinar si el tratamiento es transfronterizo y, de ser así, qué agencia de protección de datos debe considerarse la agencia principal.

El reglamento se limita a la delimitación del ordenamiento jurídico; el inicio del procedimiento puede ser que la Agencia Española de Protección de Datos transfiera la reclamación al representante de protección de datos o al organismo o entidad responsable de la resolución extrajudicial de conflictos de acuerdo con lo establecido en la código de conducta; el reclamo no es aceptado; acción de investigación preliminar; medidas temporales, en las que el orden de bloqueo de los datos es prominente; y la terminología de los procedimientos de procesamiento, y suspenderlos en su caso. La particularidad de este procedimiento pasa por la formulación de normativas.

Tenemos que apreciar que el título IX del régimen de sanciones comienza con el hecho de que el Reglamento (UE) 2016/679 implanta un sistema de sanciones o acciones correctivas que permite una apreciación generalizada. En este marco, la Ley Orgánica se propone describir comportamientos típicos y tiene en cuenta las diferencias que establece el Reglamento General de Protección de Datos a la hora de determinar el número de sanciones, distinguiendo así los delitos muy graves, graves y leves. La introducción de la tipificación de delitos tiene como único objetivo determinar el plazo de prescripción, con la descripción de comportamientos típicos como único objetivo, y algunos listados ejemplares de comportamientos punibles, que deben entenderse incluidos en los tipos generales establecidos en Europa. La ley orgánica regula los hechos de la persona interrumpida de acuerdo

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

con los requisitos constitucionales que constituyen conocimiento, pero debe tener en cuenta las problemáticas derivadas de los procedimientos establecidos por la normativa europea, en función de si los procedimientos son tratados específicamente por la Agencia Española de Protección de Datos o utilizar el Reglamento General de Protección de Datos del artículo 60 se trata en el procedimiento de coordinación. El Reglamento (UE) 2016/679 establece un amplio margen para determinar el importe de las multas. Esta Ley Orgánica hace uso de las restantes cláusulas del artículo 83.2 de la Norma Europea, referidas a factores agravantes o atenuantes, para aclarar que los elementos a considerar pueden incluir elementos ya presentes en la Ley Orgánica 15/1999 en los artículos 45.4 y 45.5 (la ley ya está derogada), y que esto era conocido por los operadores legítimos.

Finalmente, el Título X de la ley asume la tarea de reconocer y garantizar las listas de derechos digitales de los ciudadanos de acuerdo con las tareas previstas en la Constitución. En particular, se regulan los derechos y libertades aplicables al entorno de Internet, como la neutralidad de la red y los derechos de acceso universal o el derecho a la seguridad y educación digital, así como el derecho al olvido, la portabilidad y la voluntad digital. El reconocimiento del derecho a la desconexión digital y la protección de los menores en Internet juegan un papel importante en el marco del derecho a la privacidad del uso de dispositivos digitales en el lugar de trabajo. Finalmente, cabe destacar la garantía de la libertad de expresión y el derecho a esclarecer la información en los medios digitales.

Las cláusulas adicionales tratan temas como medidas de seguridad del sector público, protección y transparencia de datos, y acceso a la información pública, cálculo de plazos, autorización judicial para la transmisión internacional de datos, prevención de posibles abusos por parte de ciertos operadores o manejo de ciertos temas. Datos de salud, etc.

Entre otras cosas, las cláusulas transitorias se utilizan exclusivamente para la normativa de la Agencia Española de Protección de Datos, procedimientos o sistemas transitorios regidos por la Directiva (UE) 2016/680. Se enumeran las disposiciones de derogación, y a continuación se enumeran las disposiciones de derecho consuetudinario pertinentes, el título de autoridad y las disposiciones finales vigentes.

Finalmente, en materia de protección de los derechos digitales, se modificaron la Ley Orgánica 2/2006 de Educación de 3 de mayo, la Ley Orgánica 6/2001 de 21/12 de Universidades y el texto refundido

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

de universidades. En el texto integral de la Ley del Trabajo y la Ley Fundamental de los Empleados Públicos.

### **3.3 Reglamento General de Protección de Datos de la Unión Europea.**

Antes de empezar con el análisis del Reglamento de Protección de Datos de la Unión Europea, vamos a explicar brevemente que es un reglamento y que tiene de diferente con otros actos legislativos que lleva a cabo la Unión Europea.

Los objetivos de los tratados que la UE lleva a cabo se logran a través de diferentes tipos de proyectos de ley. Algunos son vinculantes, otros no. Algunos se aplican a todos los países de la UE, otros se aplican solo a unos pocos países. Estos diferentes tipos de proyectos de Ley son: Reglamentos, Directivas, Decisiones, Recomendaciones y Dictámenes.

Los reglamentos son actos legislativos vinculantes que deben aplicarse en toda la Unión Europea. Por ejemplo, cuando la Unión Europea quiso garantizar salvaguardias comunes para las mercancías importadas de fuera de la Unión Europea, el Consejo aprobó un reglamento.

Las directivas son actos legislativos que establecen objetivos que todos los países de la UE deben alcanzar. Sin embargo, cada país debe formular sus propias leyes sobre cómo lograr estos objetivos –trasposición de la norma comunitaria al ordenamiento interno-. Un ejemplo es la "Directiva de derechos del consumidor", que mejora los derechos del consumidor en toda la Unión Europea al eliminar tarifas y costos ocultos en Internet y extender el período durante el cual los consumidores pueden retirarse de los contratos de venta.

La decisión es vinculante para la persona objetivo (país de la UE o empresa específica) y es directamente aplicable. Por ejemplo, la Comisión emitió una decisión sobre la participación de la UE en el trabajo de varias agencias de lucha contra el terrorismo. La decisión solo concierne a estas organizaciones.

Las recomendaciones no son vinculantes. Cuando el comité emitió una propuesta para alentar a la legislatura a utilizar más las videoconferencias para facilitar los servicios judiciales transfronterizos, su propuesta no tuvo consecuencias legales. A través de recomendaciones, las instituciones pueden expresar sus puntos de vista y proponer planes de acción sin imponer obligaciones legales a sus obligaciones.

## DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

Los Dictámenes son un medio que permite a las instituciones realizar declaraciones de forma no vinculante, es decir, no imponer obligaciones legales sobre los objetos que tratan. Los Dictámenes no son vinculantes. Puede ser emitido por las principales instituciones de la UE (comisiones, consejos y parlamentos), comisiones regionales y el Comité Económico y Social Europeo. Al redactar la ley, los comités expresan sus opiniones desde sus respectivas perspectivas regionales o económicas y sociales. Por ejemplo, el comité regional emitió dictámenes sobre el programa europeo de "aire limpio".

Una vez vistos los diferentes tipos de actos legislativos que la Unión Europea tiene a su disposición, es hora de empezar con el análisis del reglamento que hemos nombrado anteriormente. Reglamento General de Protección de Datos de la Unión Europea.

El Reglamento General de Protección de Datos tiene como objetivo superar directa y eficazmente los obstáculos que dificultan los objetivos unificados de la Directiva 95/46 / CE sobre protección de las personas físicas emitida por el Parlamento Europeo y el Consejo el 24 de octubre de 1995. El tratamiento de datos personales y la libre circulación de dichos datos. La conversión de las directivas por parte de los estados miembros ha dado lugar a irregularidades en el patrón regulatorio de toda la Unión Europea, lo que finalmente derivó en evidentes diferencias en la protección de los derechos civiles.

Asimismo, también debemos afrontar nuevas situaciones, principalmente por el incremento del flujo transfronterizo de datos personales debido al funcionamiento del mercado interior, el rápido desarrollo de la tecnología y los retos que trae la globalización, que hacen de los datos personales un recurso básico de la sociedad de la información. La centralidad de la información personal tiene un aspecto positivo porque permite nuevos y mejores servicios, productos o descubrimientos científicos. Pero también tiene riesgos, porque la información sobre las personas se ha multiplicado, más participantes pueden acceder a ellos con mayor facilidad y se vuelve cada vez más fácil de procesar, mientras que controlar los destinos y el uso es más difícil.

El Reglamento General de Protección de Datos implica modificaciones en la base legal del modelo europeo de protección de datos, no solo actualizaciones de la normativa vigente. Se enfoca en fortalecer la seguridad jurídica y la transparencia, al tiempo que permite que sus leyes sean reguladas o restringidas en cierta medida por las leyes de los estados miembros para mantener la continuidad,

## **NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

de modo que el receptor pueda comprender sus regulaciones nacionales. Por tanto, el "Reglamento General de Protección de Datos" contiene un gran número de autorizaciones (aunque no impuestas) a los Estados miembros para regular determinadas materias, e incluso lo permite en su considerando 8, que está en consonancia con los principios generales que constituyen el Derecho cuando los Estados creen que sus reglas deben ser estipuladas, interpretadas o excepcionalmente restringidas por las leyes de los estados miembros, pueden, en cierta medida, por razones de coherencia y comprensión, incorporar las disposiciones específicamente contenidas en las reglas en sus leyes nacionales.

En este punto, se debe enfatizar que no se excluye cualquier interferencia con la legislación nacional en las áreas cubiertas por la normativa europea. Por el contrario, este tipo de intervención puede ser adecuada tanto para depurar el sistema legal nacional como para desarrollar o complementar las regulaciones pertinentes. Por tanto, en sus aspectos positivos, el principio de seguridad jurídica obliga a los Estados miembros a integrar internamente el sistema jurídico europeo de forma suficientemente clara y abierta para que los encargados de hacer cumplir la ley y los propios ciudadanos puedan comprender plenamente el sistema jurídico europeo. Por otro lado en el aspecto negativo, esto significa que estos países están obligados a eliminar las incertidumbres derivadas de la existencia de normas en el derecho interno que son incompatibles con Europa. Partiendo del segundo aspecto, lo que sigue es la obligación de eliminar el ordenamiento jurídico. En última instancia, el principio de seguridad jurídica requiere "aprobar cláusulas internas obligatorias con el mismo valor legal que las cláusulas internas que deben ser modificadas, y finalmente eliminar las regulaciones internas que sean incompatibles con la legislación de la UE" (decisión judicial de febrero) (23 de julio de 2006 , Comisión Europea contra España; 13 de julio de 2000, Comisión Europea contra Francia; 15 de octubre de 1986, Comisión Europea contra Italia). Finalmente, si bien estas normas tienen las características de aplicabilidad directa, en realidad pueden necesitar otras normas internas complementarias para que su aplicación sea plenamente efectiva. En este sentido, no se trata tanto de una fusión como de un "desarrollo" o un complemento de la legislación de la UE.

De acuerdo con lo dispuesto en el artículo 99, los requisitos para la modificación del Reglamento General de Protección de Datos que entrará en vigor el 25 de mayo de 2018 son simplemente para redactar una nueva ley orgánica que sustituya a la actual. En este trabajo se preservan unos buenos principios de supervisión, porque se trata de una norma necesaria para adecuar el ordenamiento jurídico español a

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

la normativa europea mencionada y ser proporcional a este objetivo, siendo el motivo último la búsqueda de seguridad jurídica.

Con esta última explicación finalmente concluimos con el apartado del marco jurídico y esperamos que los análisis tanto de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cómo del Reglamento General de Protección de Datos de la Unión Europea, les hayan sido de ayuda para comprender mejor el tema principal que estamos tratando en este trabajo de fin de grado.

### **4. JURISPRUDENCIA**

En este apartado, cómo su propio nombre indica analizaremos la jurisprudencia que es relevante y significativa para el trabajo que estamos llevando a cabo. De entre toda la jurisprudencia existente hemos decidido analizar dos sentencias que a nuestro parecer es necesario tener en cuenta, debido a su importancia, ya que, se tratan de dos sentencias que resuelven cuestiones prejudiciales y que están relacionadas directa o indirectamente con dos de las empresas más importantes, por no decir las más importantes, de la sociedad de internet. Las empresas relacionadas en dichas sentencias son nada más ni nada menos que la empresa Facebook y la empresa Google.

#### **4.1 Facebook.**

Fashion ID GmbH & Co. KG es una empresa online dedicada a la moda. Insertó un complemento en su sitio web: el botón "Me gusta" de Facebook. De esta forma, cuando un usuario visita el sitio web de Fashion ID, la información sobre la dirección IP del usuario y la secuencia del navegador se transmitirá a Facebook. Cuando se carga el sitio web de Fashion ID, esta transferencia se realiza automáticamente independientemente de si el usuario hace clic en el botón "Me gusta" o tiene una cuenta de Facebook. La asociación alemana de protección del consumidor Verbraucherzentrale NRW eV prohíbe el uso de Fashion ID porque el uso de este complemento viola las normas de protección de datos. El Tribunal Superior alemán de Dusseldorf (Oberlandesgericht Düsseldorf), que conoce del caso, solicitó una explicación de las disposiciones de la Directiva 95/46 / CE.

##### **4.1.1 C-40/17 del TJUE**

Fashion ID, una empresa de comercio electrónico que vende ropa, ha insertado el módulo social "Me gusta" en su sitio web de la red social Facebook. Una característica de Internet es permitir que los navegadores de los visitantes de los sitios de Internet presenten

## **NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

contenido de diferentes fuentes. Entonces, por ejemplo, en la situación actual, las fotos, videos, noticias y botones "Me gusta" de Facebook discutidos pueden estar vinculados y aparecer en sitios de Internet. Si el administrador del sitio de Internet tiene la intención de insertar dicho contenido externo, se puede colocar en el sitio un enlace que haga referencia al contenido externo. Cuando el navegador de un visitante del sitio abre el enlace, solicitará contenido externo y lo insertará en la posición de visualización deseada en el sitio. Para ello, el navegador envía la dirección IP del ordenador del visitante y los datos técnicos del navegador al servidor del proveedor externo para que el servidor pueda determinar en qué formato se entrega el contenido a la dirección. El navegador también envía información sobre el contenido deseado. En particular, se refiere al botón "Me gusta" de Facebook. Cuando un visitante visita el sitio de Internet de Fashion ID, los datos personales del visitante se transmitirán a Facebook Irlanda, porque el sitio contiene los botones anteriores. Parece que esta transmisión se lleva a cabo sin que el visitante se dé cuenta, y sin importar si es miembro de la red social Facebook o si ha hecho clic en el botón "Me gusta" de Facebook.

La Verbraucherzentrale NRW, una asociación de utilidad pública que defiende los derechos del consumidor, condenó Fashion ID por transferir los datos personales de sus visitantes a Facebook Irlanda sin su consentimiento, y por violar las obligaciones de información estipuladas en la normativa sobre protección de datos personales.

Verbraucherzentrale NRW emitió una orden judicial contra Fashion ID a Landgericht Düsseldorf (el tribunal local civil y penal en Düsseldorf, Alemania) para poner fin a la práctica de este último.

El Tribunal de Distrito de Düsseldorf (Tribunal Civil y Penal del Distrito de Düsseldorf) emitió un fallo el 9 de marzo de 2016. Después de confirmar su posición en virtud del artículo 8, párrafo 3, punto 3 del Grupo de Trabajo Ad Hoc, se mantiene parte de la afirmación de Verbraucherzentrale NRW .

Fashion ID apeló la decisión ante el tribunal recomendado Oberlandesgericht Düsseldorf (Tribunal Superior Civil y Penal de Düsseldorf, Alemania). Facebook Irlanda intervino en la llamada para apoyar Fashion ID. Verbraucherzentrale NRW participó en el llamamiento para ampliar la sentencia impuesta a Fashion ID en primera instancia.

Antes de escuchar al tribunal, Fashion ID insistió en que la sentencia del Tribunal de Distrito de Düsseldorf (Tribunal Civil y Penal del Distrito de Düsseldorf) era incompatible con la Directiva 95/46.

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

A causa de las alegaciones aportadas el tribunal cuestiona en primer lugar si la Directiva 95/46 permite a las asociaciones de servicios públicos iniciar procedimientos legales para proteger los intereses de la parte perjudicada. Por otro lado, quiere saber si, en el sentido del artículo 2, se cree que el administrador de un sitio de Internet (como Fashion ID) ha insertado un módulo social que permite la recopilación de datos personales en el sitio, y si se considera que ha provocado dicho tratamiento el motivo es debido a la letra d) de la Directiva 95/46, porque no afecta al tratamiento de los datos transmitidos al proveedor del módulo.

En este caso, Düsseldorf Oberlandesgericht (Tribunal Civil y Penal del Distrito Superior de Düsseldorf) decidió suspender el proceso y remitió las siguientes cuestiones al tribunal para una determinación preliminar:

1- ¿Los artículos 22, 23 y 24 de la Directiva [95/46] entran en conflicto con las leyes nacionales? Además del poder de intervención de la agencia de protección de datos y la posibilidad de ayudar a las partes interesadas a apelar, ¿reconoce los servicios públicos? ¿Tiene la Asociación de Protección al Consumidor el derecho a tomar medidas contra los infractores en caso de violaciones?

En caso de responderse negativamente la primera pregunta

2- En la situación actual, una persona inserta un código de programación que permite que el navegador del usuario solicite contenido de un tercero en su página web, y transmite datos personales al tercero, ¿quién es "responsable del procesamiento", en el sentido del artículo 2 d) de la Directiva [95/46], incluso si no puede influir en las operaciones de tratamiento de datos antes mencionadas?

3- Si la respuesta a la segunda pregunta es negativa: ¿el artículo 2, letra d), de la Directiva [95/46] debe estipularse rigurosamente para evitar que un tercero emprenda una acción civil para explicar la responsabilidad de quien no es responsable del tratamiento. Pero es quien opera el tratamiento sin afectar al mismo?

4- En una situación como la actual, ¿qué "intereses legítimos" deben considerarse de acuerdo con el artículo 7 de la Directiva [95/46], f)? ¿Está inclinado en insertar al interés del contenido de terceros o al interés del tercero?

5- En este caso, ¿qué consentimiento debe darse en virtud del artículo 7, letra a), y del artículo 2, letra h), de la Directiva [95/46]?

**NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

6- En este caso, ¿los operadores de sitios web que inserten contenido de terceros deben cumplir con las obligaciones de información estipuladas en el artículo 10 de la Directiva [95/46], provocando así el tratamiento de los datos de las personas que han sido proporcionados por terceros?

Mediante la sentencia el Tribunal Superior de Justicia de la Unión Europea da solución a las cuestiones prejudiciales antes mencionadas:

1º) *“Los artículos 22 a 24 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, deben interpretarse en el sentido de que no se oponen a una normativa nacional que permita a las asociaciones de defensa de los intereses de los consumidores ejercitar acciones judiciales contra el presunto infractor de la protección de los datos personales”*<sup>9</sup>.

2º) El administrador de un sitio de Internet como Fashion ID GmbH & Co. KG ha insertado un módulo social en el sitio web, que permite que el navegador del visitante del sitio solicite contenido del proveedor del módulo y transmita los datos de acuerdo con el significado de Artículo 2 d) de la Directiva 95/46, los datos personales del proveedor pueden ser considerados responsables del procesamiento. Sin embargo, esta responsabilidad se limita a las operaciones que determinan efectivamente el propósito y los medios o un conjunto de operaciones de procesamiento de datos personales, es decir, la recolección y comunicación a través de la transmisión de datos relevantes.

3º) *“En una situación como la del litigio principal, en la que el administrador de un sitio de Internet inserta en dicho sitio un módulo social que permite que el navegador del visitante de ese sitio solicite contenidos del proveedor de dicho módulo y transmita para ello a dicho proveedor datos personales del visitante, es necesario que el administrador y el proveedor persigan, cada uno de ellos, con esas operaciones de tratamiento, un interés legítimo, en el sentido del artículo 7, letra f), de la Directiva 95/46, para que estas queden justificadas.”*<sup>10</sup>

4º) El artículo 2, letra h), y el artículo 7, letra a), de la Directiva 95/46 deben interpretarse como en algunos casos, como en el litigio principal, el administrador del sitio de Internet inserta un módulo social en el sitio. Si el navegador del visitante del sitio web requiere que el proveedor del módulo proporcione contenido y transfiera los datos personales del visitante al proveedor, el consentimiento mencionado en tales regulaciones solo debe ser requerido por el administrador para involucrar la operación o un grupo de operaciones de procesamiento de

<sup>9</sup> Sentencia del Tribunal de Justicia (TJUE) en el asunto C-40/17 de 29 de julio de 2019.

<sup>10</sup> Sentencia del Tribunal de Justicia (TJUE) en el asunto C-40/17 de 29 de julio de 2019.

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

datos personales , cuyo propósito y método son determinados por el administrador. Además, el artículo 10 de la citada directiva debe ser interpretado en cierto sentido. En este caso, la obligación de información prevista en este reglamento también correrá a cargo del administrador, sin embargo, la información de este último debe ser comunicada a los interesados del conjunto de operaciones de tratamiento de datos personales que solo implican la operación o la finalidad y los medios por ella determinados.

Las opiniones vertidas por el Tribunal de Justicia de las Comunidades Europeas tienen por un lado reforzar los derechos de los usuarios en el ámbito de las páginas web, y por otro, sientan un precedente sobre cómo llevar a cabo estas actividades y las obligaciones de los gestores en estos populares sitios de redes sociales.

### **4.2 Google.**

#### **4.2.2 C-131/12 del TJUE**

El 5 de marzo de 2010 el señor Costeja González, de nacionalidad española, instalado en España presentó una demanda contra La Vanguardia Ediciones. SL ante la AEPD, que editó durante un periodo de amplia difusión en Cataluña (en adelante, “La Vanguardia”), así como las acusaciones contra Google España y Google Inc. Este reclamo se fundamenta en que cuando los internautas ingresaron el nombre del señor Costeja González en el motor de búsqueda de Google (en adelante, "Google Search"), los enlaces llevan a dos páginas del 19 de enero y el 9 de marzo de 1998 del diario la Vanguardia en el que se publicó un anuncio sobre una subasta inmobiliaria relacionada con la incautación de deudas de la seguridad social, en el que se mencionaba el nombre del señor Costeja González.

En respuesta a esta solicitud, el Sr. Costeja González solicitó a La Vanguardia eliminar o modificar publicaciones para evitar que aparezcan sus datos personales, o utilizar herramientas proporcionadas por los buscadores para proteger estos datos. Por otro lado, exige que Google España o Google Inc. borren u oculten sus datos personales para que dejen de estar incluidos en los resultados de búsqueda y dejen de estar vinculados a los enlaces de La Vanguardia. Al respecto, el señor Costeja González manifestó que el embargo que sufrió en ese momento se encuentra resuelto en su totalidad desde hace varios años y es irrelevante en la actualidad.

La AEPD rechazó la solicitud de La Vanguardia en su resolución de 30 de julio de 2010, y consideró que el informe se hizo de acuerdo con la

**NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

orden del Ministerio de Trabajo y Asuntos Sociales y era legalmente razonable para promover al máximo la subasta para poder atraer a la mayor cantidad de postores.

Por el contrario, en el caso de Google España y Google Inc., el reclamo sigue siendo válido. En este sentido, AEPD cree que las personas que gestionan buscadores deben cumplir con la normativa de protección de datos porque el tratamiento de datos que realizan es responsable de ellos y actúa como intermediario de la sociedad de la información. AEPD cree que su ubicación y difusión pueden dañar los derechos básicos de protección de datos y la dignidad de las personas ampliamente comprendidas, por lo que AEPD tiene derecho a ordenar la retirada y evitar que los gestores de motores de búsqueda accedan a determinados datos. Incluyendo los simples deseos de los afectados cuando quieran que terceros desconozcan los datos. La AEPD cree que esta solicitud se puede realizar directamente al operador del motor de búsqueda sin eliminar los datos o información de la página que originalmente alojó la página, incluso si el mantenimiento de esta información en la página cumple con la normativa legal.

Google España y Google recurrieron ante la audiencia nacional contra la mencionada resolución.

El citado tribunal señaló en el auto que estos recursos han suscitado las siguientes cuestiones: ¿Cuál es la obligación de los gestores de buscadores de proteger los datos personales de las personas interesadas que no deseen obtener determinada información, que se publica en páginas web de terceros?, que contiene sus datos personales y le permite relacionarse con ellos, localizarlos, indexarlos y facilitarlos a los usuarios de Internet de forma indefinida. Considera que la respuesta a esta pregunta depende de la interpretación de la Directiva 95/46 en el contexto de estas tecnologías que surgieron después del lanzamiento de estas tecnologías.

En el presente caso, la Audiencia Nacional decidió suspender el procedimiento y someter a juicio prejudicial las siguientes cuestiones:

1- En cuanto a la aplicación territorial de la Directiva [95/46], y el ámbito de aplicación de la normativa española de protección de datos que sigue:

a) Cabe aclarar que existe "establecimiento" en los términos descritos en el art. [Directiva 95/46] 4.1.a), cuando ocurra uno o más de los siguientes supuestos:

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

Cuando una empresa proveedora de motores de búsqueda crea una oficina o subsidiaria en un país miembro para promover y vender espacios publicitarios en buscadores, que dirija sus actividades a los residentes de ese estado.

Cuando la (empresa)matriz designa como representante a una subsidiaria ubicada en el país miembro y es responsable de procesar dos documentos específicos relacionados con los datos de los clientes que han firmado un contrato publicitario con la empresa.

Cuando una oficina o filial establecida en un estado miembro transfiera a una empresa matriz ubicada fuera de la Unión Europea, ¿la persona afectada y la autoridad competente respetarán los requisitos de los derechos de protección de datos, incluso si la cooperación antes mencionada se realiza de forma voluntaria?

b) Hay que explicar el art [Directiva 95/46] 4.1.c, en cierto sentido "dependen de medios ubicados en el territorio del estado miembro":

Cuando un motor de búsqueda utiliza arañas o robots para localizar e indexar información contenida en páginas web en el servidor del país miembro.

¿Cuándo se utiliza el nombre de dominio de un país miembro y la búsqueda directa y los resultados se basan en el idioma del país miembro?

c) En lo que al artículo se refiere, ¿se puede considerar como un recurso de medios? [Directiva 95/46] 4.1.c, el almacenamiento temporal de información indexada por motores de búsqueda en Internet? Si la respuesta a la última pregunta es sí, ¿es comprensible que cuando la empresa se niega a revelar la ubicación donde almacena estos índices por razones competitivas, el estándar de conexión es consistente?

d) Independientemente de la respuesta a la pregunta anterior, especialmente si el Tribunal de Justicia de la Unión considera que no concurren los estándares de conexión especificados en el art. 4 en la [Directiva 95/46]:

¿Debe utilizarse la [Directiva 95/46] según lo dispuesto en el [Carta] Artículo 8 si es posible proteger los derechos de los ciudadanos de la Unión de forma más eficaz en los Estados miembros donde se concentra el conflicto?

**NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

2- En cuanto a las actividades del motor de búsqueda como proveedor de contenidos en relación con la [Directiva 95/46]:

a) En cuanto a las actividades de [Búsqueda de Google], como proveedor de contenidos, incluye buscar información publicada por un tercero o incluida en la red, indexarla automáticamente, almacenarla temporalmente y finalmente proporcionarla a los usuarios de Internet en un orden específico. la información anterior contiene datos personales de terceros, ¿Deben incluirse actividades como las descritas en el concepto de "procesamiento de datos" en el campo? [Directiva 95/46] 2.b?

b) Si la respuesta anterior es sí y siempre está relacionada con una actividad (como ya se describió):

¿Debe interpretarse el artículo 2.d) de la [Directiva 95/46] en el sentido de que la empresa que gestiona [Búsqueda de Google] es "responsable del tratamiento" de los datos personales contenidos en sus páginas indexadas?

c) Si la respuesta anterior es sí:

¿Puede la AEDP proteger los derechos contenidos en los artículos 12.b) y 14.a) de la [Directiva 95/46] y solicitar directamente a [Búsqueda de Google] que inicie la supresión del índice de información publicado por terceros sin tener que dirigirse al titular del sitio web con antelación?

d) Si la respuesta a la última pregunta es sí:

Cuando la información que contiene estos datos haya sido publicada legalmente por un tercero y almacenada en el sitio web original, ¿se excluirá la obligación de los motores de búsqueda de proteger estos derechos?

3- En cuanto al alcance del derecho de revocación y / o derecho de oposición relacionado con el derecho al olvido, se plantean las siguientes cuestiones:

¿Debe interpretarse como el derecho a suprimir y bloquear datos, que está regulado en este campo. 12.b) Y la oposición, regulada por el art. 14.a) de la [Directiva 95/46] incluye que las partes interesadas pueden ponerse en contacto con los motores de búsqueda para evitar la indexación de información que les concierne a la publicación de información en el sitio web de un tercero se basa en el motivo por el cual desea que los usuarios de Internet no sepan de dichos datos, ya

**DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

que, pueden dañarlo o simplemente quiere olvidarlo. Incluso si la información es divulgada legalmente por un tercero de forma lícita?

El TJUE da solución ante las preguntas suscitadas:

1º) Artículo 2, b) y d) de la Directiva 95/46 / CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en términos del tratamiento de datos personales y libre circulación. En cierto sentido, debe interpretarse como una actividad de motor de búsqueda, que incluye encontrar información publicada por un tercero o colocada en Internet, indexarla automáticamente y almacenarla temporalmente y finalmente, se proporciona a los usuarios de Internet de acuerdo con un orden de prioridad específico. En el caso de que la información contenga datos personales, debe clasificarse como "procesamiento de datos personales" de acuerdo con el significado del párrafo 2 b) anterior, y por lo tanto, de acuerdo con el significado del párrafo 2 d) anterior, el administrador del motor de búsqueda debe ser considerado "responsable".

2º) El significado del artículo 4, apartado 1, letra a) de la Directiva 95/46, debe interpretarse en el sentido de que el tratamiento de datos personales se lleva a cabo dentro del ámbito de las actividades de la agencia responsable del tratamiento en el territorio del estado miembro. El significado de este reglamento es cuando el administrador del motor de búsqueda crea una sucursal o filial en un país miembro para garantizar la promoción y venta de los espacios publicitarios propuestos por el motor, y sus actividades están dirigidas a los residentes del país miembro.

3º) El artículo 12 b) y el artículo 14 a) de la Directiva 95/46 deben ser interpretados en el sentido que con el fin de respetar los derechos establecidos por este reglamento, pero para cumplir efectivamente establece que después de la búsqueda del nombre de una persona, el administrador del buscador está obligado a eliminar la lista de resultados obtenidos por el nombre de la persona de los enlaces web publicados por un tercero y que contengan información relacionada con esa persona. El nombre o esta información no se eliminará de estas páginas antes o al mismo tiempo, y en su caso, incluso si las publicaciones de estas páginas son en sí mismas legales.

4º) *“Los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados*

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

*obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.*<sup>11</sup>

La sentencia trata sobre la retirada de los datos personales del índice GOOGLE y la imposibilidad de acceder a ellos en el futuro, por lo que a partir de ahora, la Agencia Española de Protección de Datos (AEPD) podrá interferir administrativamente en los buscadores de datos personales que requieran la modificación o cancelación de estos datos personales. Comprendiendo que las acciones de GOOGLE implican el "procesamiento de datos" y se aplican las directivas europeas anteriores. De esta forma, a partir de ahora, en Europa, el derecho a proteger los datos personales es evidentemente más importante que los intereses económicos puros de los gestores de buscadores, pero con la excepción de si el interesado tiene relevancia pública el derecho de acceso a la información está abierto.

### 5. ¿Cómo la falta de información, afecta a la ciudadanía y permite la vulneración de los derechos nombrados anteriormente?

En este apartado nos detendremos de manera muy breve con un ejemplo muy sencillo de como la falta de información nos afecta de forma directa y permite que tanto las empresas como personas físicas se aprovechen de esta falta de conocimiento y puedan utilizar nuestra información personal que le hemos entregado sin siquiera nosotros saberlo.

El ejemplo que hemos comentado en el apartado anterior se trata nada más ni nada menos que las cookies<sup>12</sup>.

Muchos se preguntan que son las cookies<sup>13</sup>. Pues las cookies son archivos que contienen pequeñas cantidades de datos (como nombres de usuario o contraseñas), que se intercambian entre la computadora del usuario y el

<sup>11</sup> Sentencia del Tribunal de Justicia (TJUE) en el asunto C-131/12 de 13 de mayo de 2014.

<sup>12</sup> Cont4bl3, "Las cookies", Con4bl3, Nº 50, 2014, pág. 38, Consultado 01/02/2021. <https://www.dialnet.unirioja.es/servlet/articulo?codigo=4730460>

<sup>13</sup> Menéndez, Luis, "¿Qué son las `cookies`?", Escritura Pública, Nº 82, 2013, pags. 16-18, Consultado 03/02/2021 <https://www.dialnet.unirioja.es/servlet/articulo?codigo=4399705>

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

servidor web para identificar usuarios específicos y mejorar su experiencia de navegación. Por ejemplo, con la ayuda de cookies, los sitios web pueden reconocer a los usuarios y recordar su información de contacto o preferencias, que pueden ser noticias sobre deportes o sobre política. Los sitios web de compras utilizan cookies para realizar un seguimiento de los artículos que los usuarios han visto anteriormente, utilizarlos para sugerir artículos que puedan interesar a otros usuarios y guardar artículos en el carrito de compras a medida que continúan comprando.

Una vez visto lo que son las cookies, explicaremos el porque una cosa que puede ser inofensiva puede llegar a vulnerar nuestro derecho a la protección de datos.

La cuestión se centra en el momento en que tu entras a una página web y te aparece el banner de las cookies te aparecen dos opciones: Aceptar todo y Más información. Por lo general la persona en cuestión que está visitando esa página no se molesta en elegir la opción de "más información" debido a que la intención de la misma puede ser por ejemplo comprar una prenda por internet y al seleccionar la opción aceptar todo están dando permiso a quien sea dueño de la página web de hacer lo que quieran con tus datos personales. Aunque a priori es inofensivo puede ocurrir que al visitar una página web que sea dudosa(cualquier tipo de página web que no sea de alguna empresa conocida como por ejemplo Amazon) le estés dando tu información personal a extraños que tienen vía libre para aprovecharse del permiso que le has dado sobre tus datos y pueden hacer con los mismos lo que ellos quieran.<sup>14</sup>

Concluimos este apartado con un consejo o recomendación: los usuarios deben cerciorarse de que todo está correcto antes de aceptar nada.

### **6. Ejemplos sobre situaciones donde pueden haberse visto vulnerado nuestro derecho a la intimidad o a la protección de datos.**

#### **6.1 Dot SCV- ¿Te escucha google a través del móvil? -Análisis y experimento.**

El vídeo que analizamos trata un tema bastante curioso e importante que está relacionado con el tema principal del trabajo que estamos viendo. Y trata sobre si la empresa Google nos espía o nos escucha a través del asistente de voz Okay Google. El vídeo fue subido a la plataforma Youtube el 16 de diciembre del 2018. El video empieza con una serie de preguntas: ¿Es cierto que google nos espía?. ¿Es cierto que

---

<sup>14</sup> Un ejemplo de lo explicado anteriormente es el caso de un conocido que solía adquirir videojuegos, prendas, muebles... de una página dudosa(en este caso era una página rusa) y al final por aceptar las cookies acabaron sabiendo las contraseñas que usaba para su correo electrónico y mediante este despiste lograron saber la contraseña de su cuenta bancaria y finalmente acabaron robándole una suma considerable de dinero.

## **NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

el micro de nuestros dispositivos electrónicos está siempre conectado y nos escucha a lo largo de todos los días?

Las respuestas a estas preguntas se resuelven a lo largo de la grabación, pero antes de responderlas da una pequeña introducción sobre el tema.

Señala que hay una tendencia actual a monitorizar y analizar una cantidad ingente de datos y de fuentes de datos que tengan cierto valor, es decir, lo que buscan las empresas es tratar con la mayor cantidad de datos de calidad posibles para así tener una idea de lo que quieren los consumidores y poder desarrollar campañas de marketing, productos y varios servicios según los datos captados.

Para poder conseguir estos datos, por ejemplo, la compañía google tiene los micros de los dispositivos digitales activados todo el tiempo. Ojo, esto no quiere decir que google nos espíe, lo que quiere decir es que lo tiene activado todo el tiempo para poder comunicarnos con el asistente de virtual, como puede ser Okay Google, Siri o Cortana. Cuando uno escucha esto lo primero que piensa es que es cierto que nos están espionando o que nos están escuchando durante todo el día y todas nuestras conversaciones. La verdad es que nos están escuchando pero no tienen la tecnología para descifrar todas las conversaciones que tenemos a lo largo de un día. Por ello las empresas tienen programas o algoritmos que recogen ciertas palabras clave y las registra y almacenan. También destacar como un ejemplo que cuando dices Okay Google el micro empieza a registrar el audio hasta que termines de hablar y una prueba de ello se encuentra en la página ( <https://history.google.com/history/audio> ) en donde están recogidos todos los audios registrados por el asistente virtual al decir Okay google.

Se detallan los aspectos del reglamento de protección de datos de la Unión Europea en el minuto 10:56 y lleva a cabo un experimento sobre si es cierto que nos escuchan durante todo el día en el minuto 11:35.

Finalmente decir que en este vídeo te explica muy bien como algunas empresas no se aprovechan de todos los instrumento que tienen a su alcance para recabar información y como otras si que pueden estar aprovechándose y como la falta de información de los ciudadanos hace que nos comportemos de una manera muy extraña atendiendo a únicamente rumores.

### **6.2 Artículo relacionado con las multas que se ciernen sobre las grandes empresas de internet THE ECONOMIST**

Con la entrada en vigor del Reglamento General de Protección de Datos (RGPD) en Europa, siguieron una serie de demandas contra

## **DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?**

Facebook y Google alegando que obligaban a los usuarios compartir su información personal.

El caso liderado por el activista austriaco Max Schrems y la organización no gubernamental Noyb buscaba una compensación de 3.900 millones de euros a la red social más grande del mundo y 3.700 millones de euros en compensación para los principales motores de búsqueda de Internet.

Aunque tanto Facebook como Google han formulado nuevas políticas de privacidad para cumplir con las nuevas regulaciones europeas, Schrems se quejó de que estas medidas no eran suficientes.

Como demuestra la demanda, la nueva normativa y el fin del "consentimiento obligatorio" no impiden que las empresas sigan "utilizando estrictamente los datos de los clientes para servicios, pero utilizarlos con fines publicitarios o entregarlos a terceros requiere el consentimiento del usuario".

Otros argumentan que estas empresas aplican políticas de privacidad basadas en "aceptarlo o abandonarlo" e incluso recurren a "amenazas" de que si los usuarios no están de acuerdo con su sistema de gestión de datos, sus servicios dejarán de estar disponibles. Shrems explicó al "Financial Times" británico que tanto Facebook como Google están al tanto de esta violación y "ni siquiera intentarán ocultarla".

La denuncia ha sido presentada a la autoridad francesa de protección de datos (para Google), Bélgica (Instagram), Alemania (WhatsApp) y Austria (Facebook) para "promover la coordinación europea". Si se confirma que estas empresas han violado las nuevas regulaciones europeas, se enfrentarán a las multas más altas que van desde los 3.700 millones de euros de Google hasta los 1.300 millones de euros para los otros tres acusados, todos los cuales pertenecen a Facebook.

La entrada en vigor del RGPD en Europa afecta por completo a Alphabet, la empresa matriz de Facebook y Google. La analista de la industria de software y tecnología de Goldman Sachs (Goldman Sachs), Heather Bellini, señaló que la compañía de Zuckerberg "puede ver la posibilidad de una caída de ingresos de hasta un 7%, aunque si los usuarios están de acuerdo, el impacto puede ser pequeño". agregó: "Debido al impacto de esta nueva regulación, los ingresos por ventas de publicidad de Google pueden llegar al 2%."

Aun así, el impacto general seguirá siendo mínimo. Goldman Sachs predice que las ventas de Facebook en 2018 aumentarán un 35% (hasta

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

55 mil millones de dólares estadounidenses) y un margen de beneficio neto del 38%, mientras que las ventas de Alphabet aumentarán un 21% (hasta 134 mil millones de dólares estadounidenses) y un beneficio neto margen del 23%.

Por último señalar que hay una gran cantidad riesgos<sup>15</sup> en internet o situaciones peligrosas en las que no somos conscientes del mismo peligro que se puede dar, incluso compartiendo tu información en Facebook<sup>16</sup> y como también gracias a este desconocimiento se han creado grandes grupos de delincuencia organizada<sup>17</sup>.

### 7. Conclusiones.

Después de completar este trabajo y analizar todo lo comentado, es necesario hacer reflexiones finales sobre la protección de nuestros derechos en internet.

En primer lugar, tras analizar los hechos expuestos sobre la protección de nuestros derechos en internet, resulta evidente un ligero retraso en la adopción de nuevas medidas de protección. Con esto no queremos decir que no se estén adoptando, todo lo contrario, a lo que nos referimos es que las nuevas tecnologías están evolucionando mucho más rápido que las medidas de protección que se van implementando y puede que se si no se hace algo al respecto, como por ejemplo, implementar medidas cada cierto periodo de tiempo, la tecnología acabe por superar a las medidas nombradas y estas queden obsoletas.

En segundo lugar, sobre los Derechos fundamentales, la importancia jurídica de estos derechos es clara. No solo protegen los derechos básicos y necesarios de la humanidad, sino que también son considerados como una serie de protecciones que pueden desarrollar una vida digna que la Constitución y el país deben garantizar. Los derechos fundamentales definen el alcance de los derechos individuales para mantener el bienestar del individuo y ser responsable de mantener el orden y coexistir pacíficamente en un territorio.

En tercer lugar señalar que la jurisprudencia citada a lo largo del trabajo ha dejado en claro que las grandes empresas de internet como pueden ser Facebook y Google ponderan más el beneficio económico que los derechos de los usuarios.

---

<sup>15</sup> Marquès Graells, P.R, "Los riesgos de internet", Revista DIM, Nº 2 2005, pags. 1-9, Consultado 26/01/2021. <https://www.dialnet.unirioja.es/servlet/articulo?codigo=5008717>.

<sup>16</sup> Gómez Gallardo, Perla, "Los riesgos de compartir información", Revista Mexicana de comunicación, Vol 23. Nº.123 2010. Pags 33-35. Consultado 29/01/2021. <https://www.dialnet.unirioja.es/servlet/articulo?codigo=5670266>

<sup>17</sup> Caro Bejarano, M<sup>º</sup> José, "Delincuencia Organizada en internet", Instituto Español de Estudios Estratégicos (IEEE), págs. 1-4, 12/11/2013. Consultado 01/02/2021 <https://www.dialnet.unirioja.es/servlet/articulo?codigo=7531331>.

## DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

En cuarto lugar, decir que los ejemplos mostrados durante los apartados anteriores son un toque de atención a los Estados para que implementen medidas de protección más efectivas a la hora de proteger los derechos de los ciudadanos en el gran mundo que es internet.

Finalmente, conviene señalar que las metas del trabajo de fin de grado, ya sean metas específicas o metas generales se han cumplido (UMH). La cuestión jurídica analizada se ha realizado haciendo uso de la metodología propia de la Ciencia Jurídica.

### 8. Fuentes consultadas.

#### 8.1 Bibliográficas.

Montaner, Bárbara "Derechos Fundamentales" Derecho.com 15/03/2015 Consultado 26/01/2021.

##### [Derechos fundamentales - Definición](#)

Pardo Falcón, Javier "Los Derechos del artículo 18 de la Constitución Española en la jurisprudencia del Tribunal Constitucional" Revista Española de Derecho Constitucional Año 12, Núm. 34. Enero-Abril 1992 Página 141 ss. Consultado 27/01/2021

<file:///C:/Users/Usuario/Downloads/Dialnet-LosDerechosDelArticulo18DeLaConstitucionEspanolaEn-79453.pdf>

#### 8.2 Legislativas.

##### 8.2.1 Españolas

Constitución Española. Boletín Oficial del Estado, 29 de diciembre 1978.

Sempere Rodríguez, Cesar "Artículo 18: Derecho al honor, a la intimidad y a la propia imagen" Comentarios a la Constitución Española. Tomo II – Artículos 10 a 23 de la Constitución Española de 1978 Consultado 26/01/2021

[Artículo 18: Derecho al honor, a la intimidad y a la propia imagen - Comentarios a la Constitución Española. Tomo II - Artículos 10 a 23 de la Constitución Española de 1978 - Comentarios a la Constitución Española de 1978 - Libros y Revistas - VLEX 331379](#)

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

## NUESTRO DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

<https://app-vlex-com.publicaciones.umh.es/#/search/jurisdiction:ES/Ley+Org%C3%A1nica+3%2F2018%2C+de+5+de+diciembre%2C+de+Protecci%C3%B3n+de+Datos+Personales+y+garant%C3%ADa+de+los+derechos+digitales./WW/vid/829846989>

Ley 34/2002, de 11 de julio, de servicios de la sociedad de información y de comercio electrónico.

[https://app-vlex-com.publicaciones.umh.es/#search/\\*/Ley+34%2F2002%2C+de+11+de+julio%2C+de+servicios+de+la+sociedad+de+la+informaci%C3%B3n+y+de+comercio+electr%C3%B3nico./WW/vid/172670](https://app-vlex-com.publicaciones.umh.es/#search/*/Ley+34%2F2002%2C+de+11+de+julio%2C+de+servicios+de+la+sociedad+de+la+informaci%C3%B3n+y+de+comercio+electr%C3%B3nico./WW/vid/172670)

### 8.2.2 Europeas

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

<https://app-vlex-com.publicaciones.umh.es/#/vid/reglamento-ue-2016-679-637528825>

Unión Europea "Reglamentos, directivas y otros actos legislativos" Web oficial de la Unión Europea 29/09/2020 Consultado 01/02/2021

[Reglamentos, directivas y otros actos legislativos | Unión Europea \(europa.eu\)](https://reglamentos.directivas.y.otros.actos.legislativos.unioe.eu)

### 8.3 Otras fuentes consultadas.

#### 8.3.1 Periodísticas

Amuro "Sentencia TJUE, de 13 de mayo de 2014, sobre Googley datos personales" Carranza abogados. Consultado 02/02/2021.

**SENTENCIA TJUE, DE 13 DE MAYO DE 2014, SOBRE GOOGLE Y DATOS PERSONALES | Abogados Carranza**

De Haro, José Luis "Facebook y Google enfrentan demandas por 7.600 millones de euros tras la entrada en vigor del RGPD" El Economista 28/05/2018. Consultado 02/02/2021.

<https://www.eleconomista.es/tecnologia/noticias/9168633/05/18/Facebook-y-Google-enfrentan-demandas-por-7600-millones-de-euros-tras-la-entrada-en-vigor-de-la-GDPR.html>

Gonzalvo, Irene "Facebook y protección de datos. Sentencia C-40/17 del TJUE" Diario Jurídico. Consultado 02/02/2021.

[Facebook y protección de datos: sentencia C-40/17 del TJUE \(diariojuridico.com\)](https://diariojuridico.com)

#### 8.3.2 Jurisprudenciales.

## DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS, ¿ESTÁ SIENDO REALMENTE RESPETADO EN INTERNET?

Sentencia del Tribunal de Justicia (TJUE) en el asunto C-40/17 de 29 de julio de 2019.

[CURIA - Documentos \(europa.eu\)](#)

Sentencia del Tribunal de Justicia (TJUE) en el asunto C-131/12 de 13 de mayo de 2014.

[CURIA - Documentos \(europa.eu\)](#)

Sentencia del Tribunal Constitucional 213/88, de 2 de diciembre, FJ 3º.

Sentencia del Tribunal Constitucional 110/84, de 26 de noviembre, FJ 3º.

### 8.3.3 Audiovisuales e Internet.

Dot CSV “¿Te escucha google a través del móvil? - Análisis y Experimento” 16 de diciembre de 2018 Youtube.

<https://www.youtube.com/watch?v=-BG6WZcRJCg>

“Derechos fundamentales” Significados.com 24/01/2020 Consultado 26/01/2021.

[¿Qué son los derechos fundamentales y cuáles son los más importantes? - Significados](#)