

**TRABAJO FIN DE GRADO**

**Grado en Derecho**

**Facultad de Derecho**

**Universidad de La Laguna**

**Curso 2021/2022**

**Convocatoria: Septiembre**

**EL DERECHO A LA PROTECCIÓN DE DATOS EN LA ERA TECNOLÓGICA**

The right to data protection in the technological age



Realizado por el alumno D. Sergio Sosa Siverio

Tutorizado por el Profesor D. José Miguel Ruano

Departamento: Derecho Constitucional, Ciencias Políticas y Filosofía del Derecho.

Área de conocimiento: Derecho Constitucional

## ABSTRACT

The importance of the right to protection of personal data on the Internet is on the rise due to its great presence in society.

It is defined as the fundamental right of granting the power to the interested parties to dispose of and control their personal data submitted to computer processing.

Personal data are all those that allow the identification of the person and are subject to treatment, being any operation or set of operations that are carried out on personal data by automated procedures or not.

In this way, this power of control is diversified into different rights such as information and access, rectification, data portability, deletion or oblivion, which entail a series of guarantees and mechanisms to carry them out. cape.

Consent is a fundamental pillar necessary for the legality of the treatment, and must be a free, specific, informed and unequivocal expression of will by which the interested party accepts, deriving from a clear affirmative action, thus excluding the provision of tacit manner.

Cookies on the Internet are subject to the RGPD and the LOPDGDD since they store very sensitive personal information such as location, searches carried out or email. They must comply with what is established and must facilitate the provision of consent as well as the mechanism to withdraw it.

**Key Words: Fundamental right, data protection, consent, cookies, RGPD, LOPDGDD**

RESUMEN (entre 150 y 350 palabras)

La importancia del Derecho de protección de datos de carácter personal en Internet se encuentra en auge debido a su gran presencia en la sociedad.

Se define como el Derecho fundamental de otorgar la facultad a los interesados de disponer y controlar sus datos personales sometidos a tratamiento informático.

Los datos personales son todos aquellos que permitan la identificación de la persona y se encuentren sometidos a tratamiento, siendo cualquier operación o conjunto de operaciones que se realizan sobre los datos personales por procedimientos automatizados o no.

De este modo, esa facultad de control se diversifica en diferentes derechos como al de información y acceso, a la rectificación, a la portabilidad de los datos, a la supresión o al olvido, los cuales conllevan una serie de garantías y mecanismos para llevarse a cabo.

El consentimiento es un pilar fundamental necesario para la licitud del tratamiento, debiendo ser una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, derivando de una clara acción afirmativa excluyéndose, por tanto, la prestación de manera tácita.

Las *cookies* en Internet se encuentran sometidas al RGPD y a la LOPDGDD puesto que almacenan información de carácter personal muy sensible tal como la ubicación, las búsquedas realizadas o el correo electrónico. Deben cumplir con lo establecido debiendo facilitar la prestación del consentimiento, así como el mecanismo para retirarlo.

**Palabras clave: Derecho fundamental, protección de datos, consentimiento, cookies, RGPD, LOPDGDD**

## Índice

Introducción.

1. ¿Qué es el derecho a la protección de datos?:
  - Concepto
  - Tratamiento constitucional como Derecho fundamental independiente: Especial relevancia de la STC 292/2000
2. Relación directa con otros derechos fundamentales:
  - Derecho a la intimidad personal y familiar
  - Derecho al honor
3. Especial consideración en el ámbito penal: delito de revelación de secretos: protección penal
4. Régimen jurídico del derecho a la protección de datos: desarrollo normativo.
  - Reglamento UE Reglamento (UE) 2016/679
  - Adaptación al Ordenamiento Jurídico español: LO 3/2018
5. Derechos a favor del interesado en el tratamiento de los datos
  - Derecho de información y transparencia
  - Derecho de acceso
  - Derecho de rectificación
  - Derecho de supresión: **especial consideración en los motores de búsqueda y redes sociales**
  - Derecho a la limitación del tratamiento
  - Derecho a la portabilidad: **especial consideración en las redes sociales**
  - Derecho de oposición
  - Ejercicio de los Derechos: papel fundamental de la AEPD
6. El pilar fundamental: el consentimiento
  1. Requisitos
  2. Tratamiento de datos sin consentimiento: interés legítimo, interés público y obligación legal
  3. Especial consideración del consentimiento del niño: la Protección del menor en internet
7. Internet y las famosas *cookies*
  - Qué son y qué aceptamos

- Problemática desde una perspectiva jurídica
8. La desinformación en línea o *fake news*
  9. Conclusión
  10. Bibliografía

## **Introducción**

Es seguro que en los tiempos que corren pocas personas quedan al margen de usar las nuevas tecnologías, ya sea a través del dispositivo móvil al que acceder a sus redes sociales y compartir tus preferencias con el mundo; a un ordenador desde el trabajo en el que insertar tus credenciales; o un simple navegador de búsqueda para consultar si se encuentra abierto el establecimiento más cercano. Que no nos extrañe que al día siguiente nos salga publicidad acerca del producto que buscaste o que un número desconocido te llame para ofrecerte un producto relacionado con la búsqueda realizada.

Todos tienen algo en común: poseen información personal de sus usuarios sin que éstos siquiera se den cuenta. Una información muy valiosa que va desde tu ubicación y preferencias de compra hasta tu identidad y número de teléfono.

Con ello surgen diferentes preguntas como:

¿Qué información les he facilitado y con qué permiso?

¿Cómo puedo revertir la situación?

¿Y mis derechos fundamentales y quien se encarga de protegerlos?

¿Alguien ha subido una foto tuya sin tu consentimiento?

Ante esta situación y el auge de la concentración de la información en sistemas informáticos e internet se encuentra la sociedad con la obligación de regular y limitar los posibles comportamientos y extralimitaciones contrarios a los tan preciados derechos fundamentales, principalmente y entre otros, el derecho a la intimidad, el honor y la propia imagen inherente a toda persona física.

Cada vez se plantean mayores escenarios alrededor de internet, puesto que forma parte de nuestra vida, incluyendo una modificación hasta en la forma de relacionarnos, siendo ya incluso más importante la imagen creada en las redes que la presencia mostrada en la realidad.

Es por ello por lo que trataremos, en la medida de lo posible dada la magnitud de los múltiples escenarios que se pudiesen contemplar en el mundo digital, un campo limitado de actuación en el que interviene el Derecho a la Protección de datos de Carácter Personal. Y es en el momento en que cedemos nuestros datos y se ven almacenados en forma de información, la cual se encuentra en posesión de otro que la utilizará de una forma u otra,

será de vital importancia conocer los campos de actuación del interesado, así como el ejercicio de las garantías que nos brinda el Ordenamiento Jurídico.

Y es aquí, en este punto, en el que se encuentra la vital importancia del Derecho Fundamental a la protección de datos de carácter personal en la era tecnológica que, como veremos a lo largo de nuestro estudio de la materia, tiene mucho en que intervenir.

## **¿Qué es el Derecho a la Protección de Datos?**

Hemos de comenzar por entender el propio concepto del derecho a la protección de datos de carácter personal para conocer su alcance y las dimensiones que abarca.

### **Concepto**

Para ello, como primera aproximación, acudiremos al diccionario panhispánico de español jurídico de la Real Academia Española que define el derecho a la protección de datos como un <sup>1</sup>“Derecho fundamental de toda persona física que la faculta para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento”.

En una definición constitucional del derecho a la protección de datos se entiende como aquel que <sup>2</sup>“consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”. Deriva de la sentencia dictada por el Tribunal Constitucional, la cual analizaremos más adelante, dejando constancia de la importante trascendencia que ha tenido dentro de nuestro ordenamiento jurídico español.

---

<sup>1</sup> Disponible en <https://dpej.rae.es/lema/derecho-de-protección-de-datos-personales>

<sup>2</sup> STC de 30 de noviembre del 2000 (rec. núm 292/2000)

A su vez, puede verse mencionado este derecho, en la propia sentencia mencionada anteriormente con la denominación de <sup>3</sup>“libertad informática”, siendo este “el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros, la oposición del ciudadano a que determinados datos personales sean utilizados para fines de aquel legítimo que justificó su obtención”.

No sería desacertado, dado el carácter primordial que se le otorga a la voluntad del propio ciudadano al cual pertenezcan los datos objeto de protección, denominarlo derecho a la <sup>4</sup>“autodeterminación informativa”, puesto que se le otorga al ciudadano titular de este derecho el poder de disposición sobre los datos personales, pudiendo llevar a cabo comportamientos de control determinando, a su juicio, el régimen de privacidad acerca de su propia información.

Una vez determinado el concepto de lo que puede entenderse por el derecho a la protección de datos con carácter independiente, hemos de integrarlo en la Constitución Española, así como establecer su alcance, límites y régimen de protección de este derecho fundamental.

Se encuentra regulado en la sección primera del capítulo segundo de la CE, concretamente en el artículo 18 en su apartado 4 en el que se establece que <sup>5</sup>“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”.

Podemos destacar en primer lugar, del precepto jurídico destacado, la evidente relación que existe entre el derecho de protección de datos con el derecho al honor y la intimidad. Tanto es así que, en el propio apartado se hace referencia expresa al objeto propio del derecho, que no es otra que la protección de la intimidad y el honor de los ciudadanos. En segundo lugar, ha de destacarse que se trata de un derecho *fundamental* dado que se encuentra regulado en el título I, capítulo segundo en su sección primera de la Constitución Española. Por tanto, al tratarse de un derecho fundamental en sentido

---

<sup>3</sup> STC de 30 de noviembre del 2000 (rec. Núm 292/2000)

<sup>4</sup> STC de 20 de julio de 1993 (rec. Núm 254/1993)

<sup>5</sup> Constitución Española (En adelante CE)

estricto, se establecen una serie de garantías para hacer efectivo el ejercicio de estos, entre las cuales destaca:

- La imperativa vinculación a todos los poderes públicos al cumplimiento de los derechos fundamentales, sólo pudiendo ser limitados, y respetando ante todo su contenido esencial, por medio de leyes, establecido en virtud del artículo 53.1 de la CE.
- La necesidad de ser regulada, de modo imperativo, por medio de ley orgánica. Ha de tenerse en cuenta lo establecido en el artículo 81.1 de la CE, sólo pudiendo limitarse su ejercicio por dicho instrumento normativo. Ello modifica el régimen de mayorías a la hora de aprobar una norma por el Congreso, debiendo ser una mayoría absoluta por razón de la importancia de las materias a regular por leyes orgánicas.
- Se concede preferencia y sumariedad para aquellos procedimientos ordinarios que se insten para el ejercicio de la tutela de estos derechos.
- Como última instancia, se concede para la tutela de los derechos fundamentales el procedimiento de recurso de amparo ante el Tribunal Constitucional una vez agotada la vía ordinaria.

### **Tratamiento constitucional como Derecho fundamental independiente**

Tras el análisis del precepto constitucional, así como por la conexión entre los propios derechos mencionados, entendemos que sea posible considerar el propio contenido material de lo establecido en el Art 18.4 como instrumento para la realización efectiva del derecho al honor y la intimidad personal garantizado en el apartado 1 del mismo artículo 18 pero en el ámbito informático, y no como un Derecho fundamental en sentido estricto por sí mismo.

Es más, esta conclusión a la que llegamos con una posible primera interpretación del mismo podemos encontrarla en palabras del propio Tribunal Constitucional en la STC 254/1993, de 20 de julio, en su fundamento jurídico sexto. En ella comenta que ya el propio poder constituyente reconoce los posibles riesgos por el uso de la informática ante la vulneración de determinados derechos, por lo que <sup>6</sup>“incorpora *un instituto de garantía* como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los

---

<sup>6</sup> STC de 20 de julio de 1993 (rec. Núm 254/1993)

derechos de la persona”. Aun así, siempre se tuvo en cuenta que “es también, en sí mismo, un derecho o libertad fundamental”.

Por tanto, se establecía relación directa entre el artículo 18.1 del derecho a la intimidad (como el propio Derecho al honor, al que explícitamente se garantiza) con el artículo 18.4, puesto que se trataba de la protección del mismo frente al surgir de las nuevas tecnologías. Sin embargo, es la propia jurisprudencia la que, en el transcurso del tiempo y los problemas surgidos y solucionados en la práctica, cambia el criterio interpretativo, tratando de manera autónoma este derecho, marcando un antes y un después en nuestro ordenamiento jurídico.

La cuestión importante surge de la sentencia dictada por el Tribunal Constitucional en el que se pronuncia gracias a la interposición de un recurso de inconstitucionalidad planteado por el Defensor del Pueblo ante unos determinados preceptos de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal que, a su juicio, iban en contra de los artículos 18.1 y 4 y 53.1 de la Constitución.

Se trata de la sentencia STC 292/2000, de 30 de noviembre de 2000, la cual cambia, notablemente, el tratamiento jurídico del propio derecho a la protección de datos, así como el criterio de interpretación del propio artículo 18.4 de la Constitución. Ésta consolida el propio precepto del Art 18.4 como un derecho fundamental propio e independiente al derecho a la intimidad reflejado en el Art 18.1.

El motivo por el que el Tribunal entiende como derecho fundamental particular al derecho a la protección de datos es el creciente auge (que ya en el momento de dictar sentencia se preveía) que deparaba la tecnología y, en particular, en el almacenamiento de los datos personales. En los días que nos acontecen, bien entrado el siglo XXI, es una realidad la inmersión tecnológica en la sociedad, en la que cualquier dispositivo sirve para almacenar y compartir información, así como para recabarla, sobre todo en el tan desconocido mundo de internet, en el que la propia persona <sup>7</sup>“puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad”.

---

<sup>7</sup> STC de 30 de noviembre del 2000 (rec. Núm 292/2000)

Entiende el Tribunal, por tanto, que <sup>8</sup>“la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona”.

Esta diferencia conceptual modifica el alcance de dichos derechos fundamentales, focalizando la protección en un “nuevo” bien jurídico, como lo es la información personal en sí misma en lo relativo al tratamiento de datos personales contenidos en sistemas informáticos. Como resalta el Tribunal Constitucional en la STC 292/2000, el objeto de protección del derecho fundamental a la protección de datos “no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, sino los datos de carácter personal”. Por tanto, podemos comprender protegido cualquier dato relevante en el ámbito personal de cualquier ciudadano, ya sea que versa sobre ideología, afecte a su derecho al honor o cualesquiera otros derechos, constitucionales o no, a los que afecten.

### **Relación directa con otros Derechos Fundamentales:**

Es inevitable que, hablando de derechos fundamentales, nos refiramos a derechos inconexos entre sí, puesto que todos responden, en sus principios más básicos, a un mismo fin. Por ello, es normal que entre muchos de ellos veamos una correlación muy estrecha, dado que tienden a defender bienes jurídicos conexos y similares. Lo podemos comprobar en varios casos, como lo son los derechos relacionados con la tutela judicial efectiva, muy relacionados entre sí, no siendo muy diferente con lo que ocurre con el derecho a la protección de datos de carácter personal. Nos surge, por tanto, la cuestión acerca de *la* relación que existe del mismo con otros derechos, como lo son, principalmente, el derecho al honor y el derecho a la intimidad personal y familiar.

---

<sup>8</sup> STC de 30 de noviembre del 2000 (rec. Núm 292/2000)

Ya en el propio precepto constitucional mencionado anteriormente, esto es, el artículo 18.4 de la constitución, vemos que existe relación directa entre el derecho a la protección de datos para garantizar el <sup>9</sup>“honor y la intimidad personal y familiar de los ciudadanos”. En primer lugar, nos centraremos en la relación entre el derecho a la intimidad y el derecho a la protección de datos de carácter personal que, como hemos visto, en una primera etapa, se entendían difusos.

### **Derecho a la intimidad personal y familiar**

El “derecho a la intimidad personal y familiar” es aquel que garantiza a la persona un ámbito reservado de su vida vinculado con el respeto de su dignidad como persona, cuya concepción nos puede inducir a cuestionar si se encuentra dentro del propio derecho de protección de datos, ya que también protege la intimidad de la persona, pero en el ámbito tecnológico. Éste se encuentra orientado a procurar un respeto a “la existencia de un ámbito propio y reservado de la vida frente a la acción y el conocimiento de los demás”<sup>10</sup>. Es similar, como podemos comprobar, al propio derecho de protección de datos, puesto que determinada información personal contenida en sistemas informáticos, de ser revelada, atentaría contra la propia intimidad de la persona. Sin embargo, se realiza una distinción por parte de los tribunales, aceptando que el derecho a la intimidad no abarca toda vulneración a la misma, por lo que se encuentra complementada por la protección del derecho de protección de datos, puesto que ésta, como vimos anteriormente, protege en términos más amplios acerca de la esfera de elementos que componen la vida privada, incluyendo todo tipo de dato, sean íntimos o no, en el marco de las tecnologías<sup>11</sup>.

### **Derecho al honor**

Ocurre lo mismo con el propio “derecho al honor”. Siendo éste un derecho tendente a proteger de aquellas expresiones o imputaciones acerca de determinadas circunstancias que menoscaben el buen nombre de la persona, no abarca lo suficiente como para proteger en la medida en que se cometan infracciones de ese tipo en el ámbito tecnológico. Es por eso que entra en juego el derecho a la protección de datos que, como veremos más

---

<sup>9</sup> CE

<sup>10</sup> STC de 28 de Febrero de 1994 (rec.núm 57/1994)

<sup>11</sup> STC de 30 de noviembre del 2000 (re. Núm 292/2000)

adelante, en las nuevas normativas vigentes acerca de esta materia se incluyen potestades para los interesados como la rectificación, supresión u olvido, instrumentos para combatir con una posible intromisión que pudiera afectar a este bien jurídico.

Como síntesis de lo expuesto en estos párrafos observamos que, a pesar de considerarse bienes jurídicos plenamente independientes, encuentran su conexión en las cuestiones que garantizan siendo diferenciados entre sí por el ámbito en el que se desempeñan y aplican.

### **Protección jurídico penal del bien jurídico protegido por el Derecho a la protección de datos**

Como todo derecho fundamental, en caso de intromisiones ilegítimas por parte de un tercero que atenta, tiene protección jurídico penal para aquellas actividades dañosas graves. En este caso y para el propio derecho de protección de datos de carácter personal se encuentra, entre otros, como tipo básico, el artículo 197.2 del Código Penal. Éste establece como autor de un delito contra el bien jurídico protegido por el Derecho a la protección de datos de carácter personal “al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero”<sup>12</sup>.

Podemos destacar el requisito de realización de la conducta punible “sin estar autorizado” que, como bien vimos anteriormente, el propio derecho radica principalmente en el carácter dispositivo de los mismos al interesado en el que la única manera de obtener la información acorde al ordenamiento jurídico era a través de la figura del consentimiento. En palabras del Tribunal Supremo en la sentencia 1383/2019, “el bien jurídico protegido en este delito es la libertad o privacidad informática de los individuos proyectada sobre los datos personales”, concluyendo, por tanto, que el objeto de protección “no es la intimidad, entendida en el sentido que proclama el artículo 18.1 de la Constitución Española, sino la autodeterminación informativa a que se refiere el artículo 18.4 del texto constitucional”<sup>13</sup>.

---

<sup>12</sup> LO 10/1995, de 23 de noviembre, del Código Penal

<sup>13</sup> STS (sala de lo penal) de 29 de abril del 2019 (rec. núm 1383/2019)

En uno de sus tipos agravados de la misma conducta punible se tiene en cuenta la conducta posterior al haber tenido acceso a los datos en el caso de “si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas” (Artículo 197.3 CP).

Además, sus otros tipos agravados consideran en sus preceptos otras variables para fundamentar su mayor pena, como pueden serlo por:

-La condición de encargado o responsable del fichero, soporte informático o archivo donde se encuentren los datos (Artículo 197.4.a))

-Se lleve a cabo mediante el uso no autorizado de los datos personales del agraviado (Artículo 197.4.b))

-En razón del campo al que afecten los datos, siendo estos aquellos que revelen información acerca de la ideología, religión, creencias, salud, origen racial o vida sexual (Artículo 197.5 CP)

-En razón de ser el agraviado una persona menor de edad o una persona con discapacidad necesitada de especial protección. (Artículo 197.5 CP)

-Por el fin perseguido, si este tiene finalidad lucrativa con la información obtenida (Artículo 197.6 CP)

### **Régimen Jurídico del Derecho de Protección de Datos: Desarrollo Normativo**

Nos hemos centrado hasta ahora en el derecho a la protección de datos desde un punto de vista constitucional del mismo, siendo la hora de adentrarnos en las normas que lo desarrollan y lo regulan. Cabe destacar que la propia Constitución no conforma este derecho fundamental desde una perspectiva única del ordenamiento jurídico español, sino que ha de tenerse en cuenta, a la hora de interpretar los mismos la posible existencia de convenios, tratados y reglamentos de la UE que contengan preceptos que lo regulen. Es por ello que el Art 10.2 de la CE obliga a que sean interpretados conforme aquellas disposiciones de derecho internacional público que hayan sido ratificadas por España<sup>14</sup>.

### **Reglamento UE Reglamento (UE) 2016/679**

---

<sup>14</sup>CE

En un primer lugar y dado que nos encontramos inmersos en la Unión Europea, ha de acudir, según el orden de prelación de fuentes conforme al Derecho internacional, al Reglamento 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). Éste regula, como se establece en su artículo 1 relativo al objeto del reglamento, “lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos”; estableciéndose con el objetivo de proteger, en particular los derechos de las personas físicas en relación con el derecho a la protección de datos (Art 1.2 del Reglamento).

En cuanto a su ámbito de aplicación material, este Reglamento europeo -como tal, de aplicación directa en los Estados miembros de la UE se aplica en los casos de tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (Art 2 del Reglamento). En cuanto a su ámbito de aplicación territorial, el Art 3 del Reglamento establece que se aplica “en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.” También establece que “se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión”, cuando las actividades se encuentren relacionadas con la oferta de bienes y servicios a interesados en la Unión, independientemente de si se les requiere pago o no<sup>15</sup>.

### **Adaptación al Ordenamiento Jurídico español: LO 3/2018**

A pesar de la aplicabilidad y eficacia directa del propio reglamento europeo mencionado, no se excluye la intervención de los Estados a la hora de regular dicha materia. Esto se justifica por medio del principio de seguridad jurídica, por lo que el legislador español, al integrar el propio reglamento, ha de revisar y hacer una adaptación al ordenamiento jurídico español, a fin de una mejor aplicación en el mismo, así como desarrollando aquellas disposiciones del reglamento que crea conveniente el poder legislativo, dado que existen disposiciones que requieren de un complemento normativo para que produzcan

---

<sup>15</sup> 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 adelante Reglamento (UE) 2016/679) (En adelante RGPD)

eficacia. Es por ello que conviene, y así se lleva a cabo, la elaboración de una norma “complementaria” al reglamento europeo.

Como vimos, al ser un derecho fundamental es necesario que venga regulado por una Ley Orgánica, siendo en nuestro ordenamiento jurídico actual la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta ley tiene como objeto dos aspectos principales, los cuales vienen contenidos en el artículo 1 del texto normativo: adaptar el ordenamiento jurídico español al reglamento europeo de protección de datos y la libre circulación de los mismos, así como desarrollar las disposiciones normativas que así lo requieran.

También se hace especial énfasis, como objeto de esta ley orgánica que se establece en la letra b) del artículo 1 de la misma, en la garantía que brinda la propia norma acerca los derechos digitales, por el que se desarrolla el mandato contenido en el artículo 18.4 CE.

En cuanto a su ámbito de aplicación establece en su artículo 2.1 se establece que “se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero”<sup>16</sup>.

Para concluir y en síntesis en cuanto al régimen jurídico aplicable, el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esa ley orgánica (Art 1.a).2 párrafo LO 3/2018).

### **Derechos en favor del interesado**

En el marco de las normas reguladoras del tratamiento de los datos de carácter personal se establecen una serie de garantías en favor de los interesados que ostentan el control sobre los mismos. Esta serie de derechos abarcan facultades que van desde el conocimiento de qué datos se encuentran en poder del responsable, así como solicitar su cambio o rectificación, terminando incluso por suprimir la propia información que fue otorgada. Los iremos considerando conforme son tratados tanto por el Reglamento como por la Ley Orgánica.

---

<sup>16</sup> LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (En adelante LOPDGDD)

Cabe destacar que estos Derechos serán ejercitado a título gratuito para el interesado titular de la información por lo previsto en el Art 12.5 del Reglamento 2016/679, estando previstas circunstancias de penalización en caso de que existan solicitudes infundadas o excesivas que no debieran soportar los responsables.

### **Derecho de información y transparencia**

En primer lugar, se encuentra el **Derecho de información y transparencia** en favor del afectado que cumple con la facultad establecida por el derecho fundamental en la medida en que ha de conocer el interesado la finalidad del tratamiento de sus datos, quién los trata y demás que especifican las normas. Éstas contienen tratamientos diferenciados, cuyo fundamento se sustenta en el origen de la obtención de los datos, siendo distintos los deberes y garantías en función de si han sido otorgados o no directamente por los interesados.

De esta manera, el Art 11.1 de la LOPDGDD en relación con los Art 13 y siguientes del Reglamento establece de forma imperativa que, de ser obtenidos los datos de carácter personal a razón del interesado, han de informarlo, en el momento en que se otorguen, de una información determinada básica para el cumplimiento pleno de las garantías establecidas, así como facilitarle un medio electrónico con el que tenga la posibilidad de acceder de forma sencilla e inmediata a la información restante que pudiera necesitar el interesado. En este caso, según el Art 11.2 de la LOPDGDD este deber de información se entiende cumplido con facilitar:

- a) identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.
- c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 (Derechos a los que haremos referencia más adelante)

Sin embargo, el Reglamento no establece una relación tan escueta acerca de los deberes de información del responsable del tratamiento estableciendo, en su art. 13, una relación más amplia acerca de la información que han de facilitar. Descartando las similitudes de conformidad con la LOPDGDD el reglamento exige, en su artículo 13.2 para cumplir con

las exigencias de un tratamiento leal y transparente inherente al Derecho de transparencia, además:

a) **el plazo** durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho **a solicitar** al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el consentimiento (en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a)), la **existencia del derecho a retirar el consentimiento en cualquier momento**<sup>17</sup>, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos. Así, ambos textos recogen, tanto en el Art 11.2 2º párrafo de la LOPDGDD como en el Art 13.2.f) la peculiaridad que existe en caso de tratamiento y realización de perfiles de manera automatizada estableciendo, en ese caso, la obligatoriedad de así informarlo.

En último lugar, en caso de que durante el transcurso del tiempo sea modificada la finalidad para la cual fue concebida la recogida de datos, habrá de ser informado el afectado con anterioridad a dicho tratamiento, para que pueda ejercer sus derechos con todas las garantías, respondiendo al imperativo establecido por el Art 13.3 del Reglamento.

En el caso en que la información no haya sido recogida del interesado se establecen unas exigencias de información diferentes. En la LOPDGDD se encuentra contemplado en el Art 11.3 en el que se establece que se entenderá cumplido el deber de información facilitando la información correspondiente al apartado anterior (la contemplada para el caso en que se recojan a razón del interesado) indicando con ello una dirección electrónica para el fácil acceso a la información restante. A su vez, se exige un añadido a la información básica anteriormente citada, siendo esta información relativa a las categorías

---

<sup>17</sup> RGPD

de datos objeto de tratamiento (Art 11.3.a)) e información relativa acerca de la fuente de la que proceda la información (Art 11.3.b))<sup>18</sup>.

En el Reglamento se encuentran reguladas las mismas disposiciones, exigiendo lo nombrado anteriormente, estableciendo, además, unas condiciones en las que se desarrollará el deber. Estas condiciones son, según el Art 14.3 del Reglamento, que la información que hemos indicado en los apartados anteriores ha de ser facilitada:

- a) una vez obtenidos, ha de ser en un plazo razonable, siendo el máximo por tardar, un mes, dependiendo de las circunstancias en que se traten estos datos.
- b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el **momento de la primera comunicación** a dicho interesado
- c) de estar prevista la comunicación a otro destinatario, como muy tarde ha de informarse en el momento en que los datos personales se comuniquen por primera vez.

Conocida la información a la que ha de tener acceso el interesado independientemente de cómo se obtuviesen los datos, ha de constar que la misma ha de ser, según lo dispuesto en el Art 12 .1 del Reglamento, “concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”<sup>19</sup>. Es decir, que ha de asegurarse la comprensión por parte del interesado, sin utilizar artimañas que induzcan a error en los términos.

## **Derecho de acceso**

En segundo lugar, se encuentra el **Derecho de acceso** el cual se encuentra recogido en el Art 15 del Reglamento europeo, así como en el Art 13 de la LOPDGDD. El mismo es posible entenderlo como un derecho de garantía al derecho de información y transparencia anteriormente abarcado, puesto que habilita al interesado a acceder al conocimiento de si un determinado responsable ostenta datos personales, así como a los datos de los que disponga, según lo dispuesto en el Art 15.1 del Reglamento. Además, este habilita para que sea informado el afectado acerca de los fines del tratamiento, el plazo en el que tratarán sus datos, cualquier información sobre la fuente de los datos personales de no haber sido obtenidos directamente desde el interesado y toda información relacionada (Art 15.1 Reglamento). Además, se incluye en Art 15.1.e) la

---

<sup>18</sup> LOPDGDD

<sup>19</sup> RGPD

posibilidad de ser informado acerca de los derechos de rectificación y supresión de los que ostenta.

En resumen, se trata de acceder a aquella información de la cual tengan conocimiento además de la información que debieran haber obtenido conforme al mandato de los Art 13 y 14 del Reglamento 2016/679 ya estudiado.

Se dará por cumplido este derecho, como bien establece la LOPDGDD en su Art 13.2 cuando “el responsable del tratamiento facilitará al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad”<sup>20</sup>. Sin embargo, debido al carácter de gratuito del ejercicio de dichos derechos salvo cuando se considere excesivo el ejercicio del mismo, en caso de que el interesado solicite un medio distinto que eleve el coste de manera desproporcionada, correrá a cuenta del propio interesado (Art 13.4 de la LOPDGDD).

### **Derecho de rectificación<sup>21</sup>**

En tercer lugar, para los casos en que el responsable del tratamiento de los datos refleje inexactitud en los mismos, el interesado tendrá derecho, en virtud del Art 16 del Reglamento 2016/679 y el Art 14 de la LOPDGDD, a solicitar la modificación de los datos que considere inexactos, es decir, **a la rectificación**. El propio interesado ha de acreditar cuando sea necesario mediante documentación que justifique la inexactitud resaltada, acompañando la solicitud con la corrección sugerida. Como podemos observar, no se trata de un derecho absoluto en el cual la persona solicite su rectificación y se conceda, debiendo aportar la correspondiente justificación.

En la LOPDGDD se hace especial referencia a la rectificación tanto en internet como en redes sociales y servicios similares que, sin embargo, trataremos de manera independiente en el punto final de nuestro estudio, dada la relación que ostenta en lo relativo a las “Fake News”.

### **Derecho “al olvido”**

---

<sup>20</sup> LOPDGDD

<sup>21</sup> RGPD

En cuarto lugar, nos encontramos con el **derecho de supresión**, también llamado **Derecho al olvido**, el cual se encuentra regulado en el Art 15 de la LOPDGDD, así como en el Art 17 del Reglamento 1016/679. El contenido de éste viene a dar lugar a la facultad por parte del interesado a instar y obtener la realización efectiva, sin dilaciones indebidas, de la supresión de los datos personales por parte del responsable del tratamiento.

Especial énfasis ha de hacerse al ejercicio del derecho al olvido **en el ámbito de internet** y, más concretamente, en el de los motores de búsqueda. Esto nos remonta a la sentencia dictada por el TJUE en el asunto C-131/12 cuyos intervinientes lo conforman la Agencia Española de Protección de Datos [AEPD] y Google. La misma surge al suscitarse una cuestión prejudicial acerca de la interpretación de determinados preceptos normativos contenidos en la anterior directiva europea relativa a la protección de la persona física en lo referido al tratamiento de sus datos personales.

En ella se declara que, dada la función realizada por los motores de búsqueda en la red, siendo ésta la de almacenar la información y acceder a ella mostrándola a los usuarios, es considerado “*tratamiento de datos*” estableciéndose, por tanto, como responsable del tratamiento a la propia empresa. Por ello, el TJUE estimaba que *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 obtenida tras una búsqueda efectuada a partir de su nombre. 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.*<sup>22</sup>

Declarándose así en su momento, a falta de una normativa sólida relativa con la protección de datos, se reafirma este “derecho al olvido”, ejercitable por los interesados en cualquier ámbito reconocido por el tratamiento de datos.

Haciendo hincapié acerca de los motores de búsqueda empleados en Internet, lo principal es evitar la relación entre el propio nombre de la persona con la información que se considere en el caso concreto. Además de establecerse en la sentencia del TJUE anteriormente analizada, lo encontramos en nuestro Ordenamiento Jurídico en el Art 93 de la LOPDGDD, el cual abarca la misma problemática dotando de solución al conflicto

---

<sup>22</sup> STJUE (Gran Sala) de 13 de mayo de 2014 (asunto C-131/12)

en el mismo sentido. Si alguien realiza la búsqueda expresa del nombre del interesado, no ha de encontrarse determinada información afectada por este derecho de supresión<sup>23</sup>. Es decir, se pretende limitar el alcance de la información que muestra el motor de búsqueda relacionada con información que no cumpla con los requisitos establecidos en las normas a las que nos hemos referido, teniendo en cuenta “cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información” (Art 93.1 LOPDGDD). Resaltar también, en el sentido de la Sentencia TJUE anteriormente citada, la posibilidad de que los propios datos sobre los que se ejerce el derecho de supresión, según lo establecido en el Art 93.3 de la LOPDGDD, sean encontrados a través de otros métodos de búsqueda alternativos al relacionado directamente con la identidad de la persona<sup>24</sup>.

Asimismo, el auge de las redes sociales se hace notar, por lo que el legislador le dedica un precepto único para el ejercicio de este Derecho al olvido en el ámbito de las redes y sus equivalentes. La LOPDGDD en su Art 94 regula dicha figura, otorgando a los interesados la posibilidad de suprimir, mediando simple solicitud, aquellos datos personales que hubiesen sido otorgados por el afectado para la publicación de contenido relacionado con su persona en dichos portales (Art 94.1 LOPDGDD). Además, cuando fuesen facilitados en virtud de terceros ajenos al interesado podrán pedir su supresión en caso de que “fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información” (Art 94.2 LOPDGDD).

En el momento actual con la vigencia del Reglamento aplicable para los ficheros que contengan datos personales encontramos un marco jurídico expreso para el ejercicio de éste. Se establecen por ello las causas que han de concurrir para ejercitar el propio derecho siendo, en virtud del Art 17.1 Reglamento 2016/679:

---

<sup>23</sup> LOPDGDD

<sup>24</sup> STJUE (Gran Sala) de 13 de mayo de 2014 (asunto C-131/12)

- a) *Que los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos, pudiendo entender que el consentimiento no se extienda a los fines por los que ahora se ostentan*
- b) *Que el interesado retire el consentimiento en que se basa el tratamiento, siendo este el factor determinante a la hora de disponer los datos, como analizaremos en profundidad.*
- c) *Que el interesado se oponga al tratamiento, ejerciendo por tanto su Derecho de oposición (art 21.1 del Reglamento 2016/679), siempre que no prevalezcan otros motivos legítimos para el tratamiento por los que exista fundamento para mantenerlos.*
- d) *Que los datos personales hayan sido tratados ilícitamente, en ausencia de los requisitos contenidos en dichas normas, así como ser tratados sin consentimiento.*
- e) *Que los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;*
- f) *Que los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información. Esto significa, según la propia definición que nos brinda el Reglamento 2016/679 en su Art 4 apartado 25 en relación con el artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, que los datos deriven de la prestación de aquel “servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios”<sup>25</sup>.*

Sin embargo, volvemos a resaltar que no se trata de un derecho absoluto, no ejercitable ante determinadas situaciones y circunstancias. Retomando la sentencia del TJUE y la visión de los jueces, establecía circunstancias en las que preponderaba el “derecho a la información” al derecho de supresión *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>26</sup>.

---

<sup>25</sup> Directiva (UE) 2015/1535

<sup>26</sup> STJUE (Gran Sala) de 13 de mayo de 2014 (asunto C-131/12)

Sigue la doctrina el Reglamento 2016/679 y establece una relación de circunstancias donde se limita el ejercicio del derecho, contempladas en su Art 17.3. Por ello, se establecen causas de inaplicación de las disposiciones normativas anteriormente descritas reguladoras del ejercicio al derecho de supresión. No sería aplicable, por tanto, de ser necesario para *ejercer el derecho a la libertad de expresión e información, para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos*, en la medida en que el derecho de oposición *podiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento o para la formulación, el ejercicio o la defensa de reclamaciones*<sup>27</sup>.

### **Derecho a la limitación del tratamiento**

En quinto lugar, analizaremos el **derecho de limitación del tratamiento**, el cual se encuentra regulado en el Art 16 de la LOPDGDD que nos remite al Art 18 del Reglamento 2016/679. Este Derecho habilita al interesado titular a establecer una serie de limitaciones en el tratamiento de sus datos al responsable, ya sea limitando la finalidad para la que son tratados o establecer límites con el objetivo de evitar que se modifiquen o supriman.

En el Reglamento se establece un listado que se incluye en el Art 18.1 donde se establecen determinadas condiciones, de las cuales ha de cumplirse alguna de ellas para poder ejercitar por parte del interesado el derecho a la limitación del tratamiento.

Así, la AEPD establece que se trata de un derecho el cual se ejercita en una doble vertiente<sup>28</sup>. Por un lado, establece que es posible solicitar la suspensión de los datos personales en caso de que concurran las condiciones establecidas en el Art 18.1.a) y en el Art 18.1.d):

- En caso de que se impugne por parte del interesado la exactitud de los datos personales, en un plazo en que el responsable tenga la posibilidad de verificar la exactitud de la información.
- En caso de que el interesado se haya opuesto al tratamiento en virtud del derecho de oposición por motivos relacionados con su situación particular, **mientras** se

---

<sup>27</sup> RGPD

<sup>28</sup> Disponible en <https://www.aepd.es/es/preguntas-frecuentes/1-tus-derechos/FAQ-0112-que-es-el-derecho-a-la-limitacion-del-tratamiento-de-datos> (fecha de consulta: 30 de agosto de 2022)

verifica si los motivos legítimos del responsable prevalecen sobre los derechos del interesado.

Por otro lado, establece, la AEPD, que es posible solicitar la conservación de los datos personales en caso de que concurran las condiciones establecidas en el Art 18.1.b) y en el Art 18.1.c):

- En caso de ilicitud del tratamiento y el interesado se haya opuesto a la supresión de la información.
- En caso de no necesitar, el responsable del tratamiento, los datos personales para la finalidad inicialmente convenida, pero sea necesaria para que el interesado pueda formular y ejercer reclamaciones.

Así, ejercida la potestad otorgada por la ley y habiendo limitado el tratamiento de los datos, solo podrán ser tratados habiendo otorgado el interesado su consentimiento, así como para formular alegaciones acerca del tratamiento o por razones de interés público (Art 18.2 Reglamento 2016/679).

### **Derecho a la portabilidad de los datos**

En sexto lugar, nos encontramos con el **derecho a la portabilidad** de los datos cuya regulación la encontramos en el Art 17 de la LOPDGDD la cual nos remite al Art 20 del Reglamento 2016/679. Se trata de un derecho el cual atribuye un control y conocimiento acerca de la información tratada por el responsable del tratamiento, que posibilita al interesado a recibir los datos personales que le incumban y haya facilitado, así como a transmitirlo a otro responsable, siempre en un formato estructurado y de uso común (Art 20.1 Reglamento 2016/679). Esto siempre y cuando se encuentre fundado en el consentimiento del afectado o exista un contrato de por medio (Art 20.1.a) del Reglamento 2016/679), así como cuando se encuentre el tratamiento llevado a cabo por medios automatizados (Art 20.1.b) del Reglamento 2016/679).

Como ocurría con el derecho al olvido, la LOPDGDD dedica su Art 95 al derecho a la portabilidad de los datos en Internet, más concretamente a los servicios de redes sociales y similares. El mismo en su apartado primero establece la opción para los usuarios de solicitar y con ello recibir y transmitir aquellos contenidos que han sido facilitados a los prestadores del propio servicio, así como de habilitar la opción a favor de los prestadores

para que, en caso de que sea posible, puedan transmitir dicha información con otro prestador que haya sido previamente designado por el usuario.

Como último inciso contenido en el apartado segundo del precepto mencionado, se habilita también al prestador de dicho servicio a que, en caso de existir la necesidad por imperativo legal, puedan conservar dicha información, siempre sin difundirla a través de internet.

### **Derecho de oposición**

En último lugar, nos encontramos con el **derecho de oposición** cuya regulación se encuentra en el Art 19 de la LOPDGDD que nos remite al Art 21 del Reglamento 2016/679. Este Derecho brinda la facultad al interesado de la posibilidad de oponerse a que el responsable trate sus datos personales, alegando motivos particulares que crea conveniente por su situación personal, pudiendo hacerlo efectivo en cualquier momento, debiendo el responsable poner fin al tratamiento de los mismo, siempre teniendo en cuenta que el responsable no alegue motivos legítimos que se antepongan a los intereses del afectado.

Por ello, ha de tenerse en cuenta que es posible, de tener el tratamiento de los datos una finalidad de interés público, así como la investigación científica, histórica o estadística, que no finalice el tratamiento de estos debido a la justificación que le brinda el Art 21.6 del Reglamento 2016/679. No ocurre lo mismo en el caso de que el tratamiento de los datos esté orientado a la mercadotecnia directa, ya que el Art 21.2 del Reglamento 2016/679 deja claro que “el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan”<sup>29</sup>, sin establecer excepciones, dejando de ser tratados de manera definitiva (Art 21.3 del Reglamento 2016/679).

### **Órganos ante los que ejercitar los derechos:**

Una vez analizados los derechos que ostentan los interesados que se encuentran con sus datos personales bajo tratamiento de un responsable, ha de determinarse como se ejercitan y ante qué órgano o mecanismo se ejercitan, pues un derecho que no pueda hacerse efectivo carecería de sentido.

---

<sup>29</sup> RGPD

Para el ejercicio de estos contamos, en virtud del del Reglamento 2016/679, con las autoridades de control públicas que han de establecer, de manera imperativa, los Estados Miembros. Se crea con una función única y específica, establecida en el Art 51.1: “supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento”<sup>30</sup>.

Para ello, nuestro Estado miembro ha creado la Agencia Española de Protección de Datos (AEPD). Figura en el Art 44 de la LOPDGDD en cuyo precepto se establece que “es una autoridad administrativa independiente de ámbito estatal”<sup>31</sup> que, cumpliendo con lo designado por el reglamento, ostenta “personalidad jurídica y plena capacidad pública y privada, que actúa con **plena independencia** de los poderes públicos en el ejercicio de sus funciones”. Como vimos, su función principal es la de supervisar la aplicación del Reglamento 2016/679 en virtud del Art 57.1.a) del Reglamento 2016/679 así como en el Art 47 de la LOPDGDD. Además, se prevén otras, que son análogas o consecutivas a la primera, como lo puede ser facilitar información, previa solicitud, a cualquier interesado en relación con el ejercicio de sus derechos (Art 57.1.e) del Reglamento 2016/679) o tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con **el artículo 80**, e investigar, en la medida oportuna, el motivo de la reclamación (Art 57.1.f) del Reglamento 2016/679).

El Artículo 80 del Reglamento 2016/679 mencionado en el párrafo anterior relativo a las funciones de la AEPD habilita al interesado perjudicado a dar mandato a aquella entidad, considerada como autoridad de control, con el objetivo de que presente en su nombre la reclamación en el caso de que un tratamiento de datos en el que se encuentre perjudicado infrinja el Reglamento 2016/679 (Art 77.1 del Reglamento 2016/679).

También vincula la posibilidad, en virtud del mismo precepto, de ejercitar el “derecho a la tutela judicial efectiva”, cuando el interesado “considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales”<sup>32</sup>.

Como síntesis, podemos afirmar que la AEPD se encarga de promover y hacer efectivo el cumplimiento del reglamento, así como velar por los derechos de los interesados.

---

<sup>30</sup> Reglamento (UE) 2016/679

<sup>31</sup> LOPDGDD

<sup>32</sup> Reglamento (UE) 2016/679

Ha de tenerse en cuenta que, en el caso de redes sociales como en páginas de gran relevancia solemos encontrar un apartado específico establecido concretamente para facilitar el ejercicio de nuestros derechos por medio de una relación privada entre el afectado y el responsable del tratamiento. En primer lugar, habría de intentar conciliar la situación con el actor principal que comparte el contenido sin las observaciones correspondientes<sup>33</sup>.

En segundo lugar, y como dejamos claro, páginas como *Facebook* o *Google* prestan un servicio específico con un apartado dedicado a la revisión de contenido, pudiendo denunciar directamente violaciones de privacidad o ilicitudes en lo que a protección de datos se refiere<sup>34</sup>.

En última instancia, de no responder sin dilaciones indebidas (según lo requerido en el Art 17.1 del Reglamento 2016/679) y en plazo máximo de un mes, entra en juego la AEPD. Ha de acompañarse a la solicitud con la prueba que acredite ese primer contacto con la empresa para ejercitar dicho derecho. Acreditando, se interpondrá la reclamación acorde a lo expuesto en los párrafos anteriores, debiendo hacerse efectivo, en el caso de que corresponda, por ejemplo, la supresión de los datos<sup>35</sup>.

A todo esto, debemos de resaltar el **pilar fundamental** para que este mismo tratamiento sea llevado a cabo conforme la legalidad que ofrecen las normas reguladoras.

### **El consentimiento como pilar fundamental**

Encontramos múltiples ramas del Derecho en la cual se establece una definición o requisitos para otorgar el consentimiento, siendo cada rama la encargada de establecer lo necesario para establecer su validez. En este caso, y muy similar a las demás ramas del Derecho, el Art 4.11 del Reglamento 2016/679 así como el Art 6.1 de la LOPDGDD entienden el consentimiento del interesado como aquella “manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta”<sup>36</sup>. Así mismo,

---

<sup>33</sup> Disponible en <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido>

<sup>34</sup> Disponible en <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido> (fecha de última consulta: 25 de agosto del 2022)

<sup>35</sup> Disponible en <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/eliminar-fotos-y-videos-de-internet> (fecha de última consulta: 25 de agosto del 2022)

<sup>36</sup> Reglamento (UE) 2016/679

en la LOPDGDD viene establecido como un principio fundamental en la protección de datos, de ahí la relevancia que hemos de darle.

Como establece el Reglamento 2016/679 además de otros supuestos contenido en el mismo precepto, en su Art 6.1.a) se establece la necesidad de que el interesado otorgue su consentimiento para el tratamiento de sus datos orientados a un determinado fin. De ello extraemos que, en determinados supuestos, siendo la mayoría de los casos en que el tratamiento sea para un fin privado, se trata de un requisito de licitud de tratamiento de datos la necesidad de obtener el consentimiento por parte del afectado.

### **Requisitos**

Para que el consentimiento sea otorgado de manera válida ha de cumplir una serie de **requisitos**, los cuales analizaremos a raíz de la definición legal de este concepto jurídico:

En primer lugar, éste ha de ser otorgado libremente, significando que ha de ser una manifestación de voluntad carente de todo vicio, como puede ser dolo.

En segundo lugar y para evitar los vicios del consentimiento relacionados con la libertad de la declaración de voluntad, la información ha de ser presentada de manera clara y entendible, habiendo informado correctamente al interesado, utilizando para ello un lenguaje y sencillez comprensible para el afectado. Así, en el contexto de páginas web, han de evitarse artimañas engañosas tanto del lenguaje como de la ubicación donde se muestre la información que puedan llegar a inducir error a la hora de prestar el mismo y aceptar el tratamiento.

En tercer lugar, se hace mención a la especificidad de la manifestación de voluntad, dado que ha de estar directamente relacionada con el tratamiento de los datos para el fin concreto que se le presenta. Es más, en los casos en que concurra la necesidad de manifestar el consentimiento al tratamiento de datos, así como para otros asuntos, han de quedar claramente diferenciadas las disposiciones ante las cuales el afectado aceptará, quedando específicamente la manifestación de voluntad vinculada con la voluntad de que sus datos sean tratados, a fin de cumplir con el principio de especificidad e información. (Art 7.2 Reglamento 2016/679)

En último lugar, se hace mención acerca de la necesidad de que la manifestación del consentimiento para el tratamiento de datos ha de ser inequívoca, debiendo estar expresamente otorgado, excluyendo la manifestación tácita del consentimiento.

Cabe destacar, por lo mencionado acerca de la manifestación expresa del consentimiento que, en materia de internet, no puede considerarse la mera inactividad del navegante en consideración a la aceptación de los términos y las *cookies*<sup>37</sup> (sobre las que trataremos en breve) con un otorgamiento tácito del consentimiento, pues el propio reglamento exige que se lleve a cabo de manera inequívoca. Aún más se desprende de la propia definición contenida en los preceptos la necesidad de que el consentimiento derive de una “*declaración o una clara acción afirmativa*”<sup>38</sup>, quedando plasmado lo dispuesto en este párrafo, en un sentido en el que la inactividad o pasividad del afectado no pueda considerarse como consentimiento en ningún caso.

Para matizar acerca de la posición del responsable del tratamiento de los datos, de tratarse de un tratamiento de datos en virtud de consentimiento, el responsable tiene la obligación de poder demostrar que el interesado otorgó su consentimiento (Art 7.1 Reglamento 2016/679).

### **Tratamiento de datos sin consentimiento: interés legítimo, interés público y obligación legal**

Sin embargo, existen casos en que el consentimiento puede no ser otorgado y no obstante el tratamiento no deja de tener un carácter lícito. Se trata de situaciones determinadas y concretas en los cuales prevalece un interés distinto al del propio afectado, por el que no se requiere su autorización para el tratamiento de éstos. Como ejemplo de ello con lo tratado hasta aquí, tenemos los casos en que se ejercitaban determinados derechos como el de supresión u oposición y no se llevaban a cabo, dado que concurrían determinadas circunstancias prevaleciendo un interés distinto frente al derecho del propio interesado. Por ello, se encuentran contemplados en el Art 6, junto con el tratamiento de datos bajo consentimiento del interesado, determinados escenarios en los que se entiende como lícito el tratamiento de datos personales que:

- sea necesario en virtud de una relación contractual en que el interesado es parte (Art 6.1.b) del Reglamento 2016/679);
- el tratamiento de los datos derivada de una *obligación legal en el que se vea inmerso el responsable* del tratamiento (Art 6.1.c) del Reglamento 2016/679), el

---

<sup>37</sup> STJUE (Gran Sala) de 1 de octubre de 2019 (Asunto C-673/17)

<sup>38</sup> Reglamento (UE) 2016/679

cual ha de entenderse complementado con una disposición tanto del Derecho de la Unión como de los Estados Miembros (Art 6.3 del Reglamento 2016/679);

- exista un interés que responda al aseguramiento de intereses vitales para el interesado (Art 6.1.d) del Reglamento 2016/679);
- sea necesario para el cumplimiento de una misión cuya finalidad responda al interés público o en el ejercicio de un poder público del responsable del tratamiento de datos (Art 6.1.e) del Reglamento 2016/679), debiendo ser complementada con una disposición tanto del Derecho de la Unión como de los Estados Miembros (Art 6.3 del Reglamento);
- exista un interés legítimo perseguido siempre que no prevalezcan los derechos y libertades del afectado sobre el propio interés alegado por el responsable o un tercero, haciendo especial énfasis de ser el interesado un menor (Art 6.1.f) del Reglamento 2016/679).

### **Especial consideración del consentimiento del niño: la Protección del menor en internet**

Notoria importancia cobra el auge del uso de las propias tecnologías en el sector más joven de la población, es decir, **los menores de edad**. El legislador es consciente de la relevancia, por lo que implementa determinados preceptos que regulan de otra forma el tratamiento de datos de los menores de edad.

Como analizamos en los párrafos anteriores y quedando claro la suma importancia que cobra, dado que se considera necesario en la mayoría de las circunstancias, ha de tener en consideración que los menores de edad, es decir, aquellos que no ha adquirido plena capacidad de obrar, tienen limitada su capacidad para prestar el consentimiento, dependiendo del negocio jurídico en el que se encuentren inmersos para considerar la validez de este.

El reglamento 2016/679 dedica expresamente su Art 8 a regular el tratamiento de los datos relativos a “niños” en relación con el tratamiento derivado de la oferta de servicios de la sociedad de la información. Éste limita la capacidad para otorgar el consentimiento, estableciendo un mínimo de dieciséis años para otorgar un consentimiento válido y sea

considerado como lícito el tratamiento de los datos basado en el consentimiento del interesado, en este caso el menor de edad<sup>39</sup>.

En los casos en los que el interesado tenga una edad inferior a los dieciséis años establecidos como edad mínima, será necesario que el consentimiento sea otorgado por aquellas personas que ostenten la titularidad de la patria potestad o los tutores legales, aplicándose única y exclusivamente el tratamiento de los datos en la medida en que se otorgó el consentimiento.

Así mismo, como último inciso en cuanto a lo relativo de la edad mínima para otorgar el consentimiento, el Reglamento deja la puerta abierta a la posibilidad de que sean los Estados Miembros los que regulen una edad distinta para otorgar el consentimiento, siempre y cuando no sea, bajo ningún concepto, inferior a los trece años (Art 8.1 segundo apartado del Reglamento 2016/679). En este sentido, en el ordenamiento jurídico español, a través de la LOPDGDD, se establece una edad distinta a la de dieciséis años establecida en el reglamento, siendo de catorce años la edad mínima para otorgar el consentimiento como regla general, sin perjuicio de las excepciones contenidas en la ley<sup>40</sup>, en virtud del Art 7.1 de dicha ley orgánica.

No obstante, deja a cargo del responsable del tratamiento, en la medida de lo posible, la capacidad y necesidad de verificar los requisitos del propio consentimiento, así como la posible existencia de consentimiento otorgado por parte de los titulares de la patria potestad o tutela<sup>41</sup>.

En cuanto a la protección relativa al uso de internet, hemos de tener en cuenta la existencia del Art 84 de la LOPDGDD relativo a la protección de los menores en Internet. En él encontramos en el primer apartado una obligación destinada a los responsables de los menores en el que han de procurar unas buenas prácticas acerca del uso de internet y tecnologías análogas cumpliendo con el pleno respeto a su dignidad y Derechos Fundamentales.

En un segundo apartado se establece una protección reforzada a favor de los menores por parte del Ministerio Fiscal donde se habilita su participación en el caso en que se entiendan como vulneradas las garantías contenidas por los Derechos Fundamentales debido a la utilización o difusión de imágenes o datos personales en el ámbito relativo a las redes sociales, así como las sociedades de la información que presten servicios

---

<sup>39</sup> RGPD

<sup>40</sup> LOPDGDD

<sup>41</sup> ídem

análogos (Art 84.2 de la LOPDGDD). Este segundo apartado ha de interpretarse en relación con el Art 92 de la misma ley relativo a la protección de datos en internet. En él se contiene el mandato hacia centros educativos o cualquier persona física o jurídica responsable del tratamiento de los datos de un menor a proteger, con especial consideración, el interés superior del mismo relativo con la protección de datos. En cuanto a la difusión de imágenes o cualesquiera otros datos de los que tuvieren posesión, es necesario contar con el consentimiento debido, en las condiciones que hemos mencionado en los párrafos anteriores, siendo otorgado por el menor o por los que ostenten su representación<sup>42</sup>.

Una vez realizado un análisis jurídico de los derechos y facultades que nos brindan las nuevas normativas a fin de salvaguardar nuestro Derecho a la protección de datos, así como los requisitos contenidos en él para que, siendo inevitable, se traten con el mayor respeto posible, entramos en contacto con la realidad y afrontamos una de las formas más comunes que, en lo que al uso de internet se refiere, se llevan a cabo para recabar nuestros datos.

## **Internet y las famosas “Cookies”**

### **Qué son y qué aceptamos**

Para poder analizar el marco jurídico de esta figura hemos de conocer, en primer lugar, qué son las cookies y qué función tienen. Sin entrar en tecnicismos informáticos, puesto que lo que nos interesa es el análisis jurídico de esta figura, se trata de un fichero informático que contiene información que es solicitada a tu ordenador por la página web a la que pretendemos acceder.

Existen numerosos tipos de *cookies* dependiendo de la función que vayan a desempeñar, así como la información que almacenan sus ficheros. Podemos encontrar las llamadas cookies “técnicas”, encargadas de recabar la información suficiente y necesaria para el buen funcionamiento de la página web; de personalización, que almacenan información acerca de cómo queremos que nos sea mostrada la página web así como, por ejemplo, el idioma de nuestra preferencia; de análisis, encaminada a almacenar información con el

---

<sup>42</sup> LOPDGDD

objetivo de registrar el tráfico que recibe una página web; así como las publicitarias, siendo estas las encargadas de recopilar información personal necesaria para mostrar los anuncios más relevantes dependiendo del usuario que se encuentre interactuando con el servidor.<sup>43</sup>

### **Problemática desde una perspectiva jurídica**

Como vemos, el factor sobre el que actúa este fichero informático es la información personal, con el que puede llegar a saber nuestro correo electrónico, nuestras búsquedas realizadas y vídeos que hemos visto, aplicaciones que utilicemos o nuestra ubicación en tiempo real tal y como podemos ver, por ejemplo, en las políticas y condiciones que nos brinda *Google*, siendo todas ellas objeto de protección por el derecho a la protección de datos y por lo que deben establecerse acorde a las leyes aplicables.

Es por ello por lo que se encuentran, de igual manera que otros ejemplos que hemos puesto a lo largo de nuestro trabajo, sometidas al derecho de protección de datos. Tanto es así que, a pesar de no ser mencionadas de manera directa en el articulado del Reglamento 2016/679, en el considerando donde encontramos la contextualización de la norma, vemos reflejado la tendencia del legislador a dotar de protección a dicha figura: *“las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas”*<sup>44</sup>.

En nuestro Derecho interno, además, encontramos referencias a dicho concepto informático, entre otros, en la Ley de Servicios de la Sociedad de la Información y la Comunicación, teniendo en cuenta que se trata de una ley anterior al RGPD y a la LO, pero que nos sitúa el concepto de *cookies* en el ordenamiento jurídico. En cuyo Art 22.2 se establece una condición, ya familiar para nosotros a estas alturas, a los prestadores de servicio, estableciendo que “podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los

---

<sup>43</sup> AEPD: “Guía sobre el uso de las cookies”, Disponible en <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies> (fecha de consulta: 28 de agosto de 2022)

<sup>44</sup> RGPD

mismos hayan **dado su consentimiento** después de que se les haya facilitado información clara y completa sobre su utilización”<sup>45</sup>.

Ha de dejarse claro que esta disposición no es aplicable en sí mismo para el ámbito de protección de datos, puesto que la continuación al mismo precepto ya lo establece, redirigiendo a las normas reguladoras de este Derecho fundamental en lo que tenga relación directa con la protección de datos.

Por tanto, nos referiremos a las *cookies* que, en aplicación del reglamento realicen un tratamiento de datos personales, siendo estos, siguiendo la definición legal establecida en el Art 4.1 del Reglamento 2016/679 como “toda información sobre una persona física identificada o identificable ... como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea”; así como la contenida en el Art 4.2 Reglamento 2016/679 en cuanto a considerar tratamiento a “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales”<sup>46</sup>.

La licitud del tratamiento descansa fundamentalmente en la figura del consentimiento, debiendo ser prestado, como bien analizamos en puntos anteriores, de forma “libre, específica, informada e inequívoca”. Esta es la razón por la cual, de querer optar a tener una página web que respete los Derechos Fundamentales, ha de quedar muy claro el mecanismo por el que se presta o deniega el consentimiento.

Así, las fórmulas más utilizadas y que se repiten en las páginas y buscadores más importantes de nuestro tiempo es la de abrir una “pestaña” con un mensaje de aviso con la información detallada que se va a solicitar a nuestro equipo y la finalidad de la recogida de dicha información, así como la posibilidad de prestar consentimiento específico de determinados datos y descartar otros, a elección del interesado. Éstas no han de estar marcadas, puesto que significaría que la pasividad del interesado equivaldría a otorgar un consentimiento tácito, cosa que se excluye expresamente en virtud del Art 4.11 del Reglamento al exigir una clara acción afirmativa.

En este mismo sentido se pronuncia el TJUE en el asunto C-673/17 en el que declaran como no válido el establecimiento de casillas marcadas que signifiquen la prestación del consentimiento, pues de llevar a cabo una actitud pasiva determinaría que no se entiende prestado en ningún caso. Con otras palabras, concretamente las del Tribunal: “no se presta

---

<sup>45</sup> Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

<sup>46</sup> RGPD (UE)

de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de *cookies* se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento”<sup>47</sup>.

También es necesario poder habilitar un sistema sencillo y práctico para los casos en los que, una vez otorgado el consentimiento, el interesado pueda retirarlo en cualquier momento y desactivar las cookies que hubieran actuado, cumpliendo con el mandato establecido en virtud del Art 7.3 del Reglamento 2016/679.

### **La desinformación en línea o las *Fake News***

Apartando la mirada hacia una rama diferente del mismo árbol encontramos uno de los problemas más grandes que supone la facilidad de compartir contenido en internet, sobre todo y concretamente por la sencillez que se hacen virales determinadas informaciones sobre las cuales los ciudadanos menos avisados no someten a ningún filtro. Es decir, nos encontramos en la era de la información y, paradójicamente, de la desinformación. Cada vez es mayor el número de personas que creen todo lo que se les cruza por una pantalla y lo más probable es que no tengan conocimientos, o no se empeñen en contrastar un mínimo.

Donde mayor hemos visto esta problemática ha sido durante los últimos años con la pandemia sufrida, puesto que cada día surgía un bulo diferente compartido a la ligera por toda red social posible. Es un problema que, en los días que corren y el interés de los ciudadanos por la veracidad en horas bajas, tiene difícil solución a corto plazo. Esta dificultad no es ajena al Derecho, puesto que muchas de las soluciones pueden estar vulnerando los Derechos fundamentales.

Volviendo a la CE, encontramos en el Art 20.1.d) con el Derecho “a comunicar o recibir libremente **información veraz** por cualquier medio de difusión”<sup>48</sup>. Además, en el Art 20.2 de la CE se establece como protección de estos la interdicción de no ser restringido “mediante ningún tipo de censura previa”. Por tanto, se trata de un Derecho fundamental,

---

<sup>47</sup> STJUE (Gran Sala) de 1 de octubre de 2019 (Asunto C-673/17)

<sup>48</sup> CE

adoptando el Estado un papel activo para garantizar que la función de los medios de comunicación pertinentes sea ejercida conforme estos principios y Derechos.

En la LOPDGDD en su Art 85 se hace referencia al Derecho de todo ciudadano a la libertad de expresión en Internet. Sin embargo, en el apartado segundo del mismo artículo establece un mandato hacia los responsables de los servicios de redes sociales para que adopten los protocolos necesarios para ejercer el Derecho de rectificación, cuyo objetivo es hacer efectivo el Derecho a divulgar y recibir información veraz<sup>49</sup>.

Se establece, el precepto anterior, en conexión con la Ley Orgánica 2/1984 reguladora del Derecho de rectificación, el cual aborda su contenido en el Art 1 por el cual “toda persona, natural o jurídica, tiene derecho a rectificar la información difundida”<sup>50</sup>, estableciendo en su desarrollo normativo como ha de ejercerse dicho Derecho.

Introducido el mecanismo para ejercitar ese Derecho de rectificación de la información, el legislador, para advertir acerca de las *Fake News* a los ciudadanos, impone la necesidad a las plataformas de “proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo”<sup>51</sup>, debiendo aparecer dicho aviso en un lugar visible junto con la publicación original, quedando constancia de la posible alteración de la verdad.

Además, entre otras medidas, en la Ley General de Comunicación Audiovisual (LGCA) aprobada recientemente, el 7 de julio de 2022, establece -entre muchas otras novedades aplicables- tanto a cadenas de televisión como a simples creadores de contenido en las distintas redes, contempla una figura para paliar y evitar los efectos de estas *Fake News*.

En el Art 10 de la LGCA se establece un objetivo claro: conseguir una mayor sensibilización en la población y criterio propio. En su apartado 1 se establece, para los prestadores de servicios de comunicación, que “adoptarán medidas para la adquisición y el desarrollo de las capacidades de alfabetización mediática en todos los sectores de la sociedad, para los ciudadanos de todas las edades y para todos los medios”<sup>52</sup>. Estas medidas se encuentran en su apartado 2, las cuales consistirán en “desarrollar competencias, conocimientos, destrezas y actitudes de comprensión y valoración crítica

---

<sup>49</sup> LOPDGDD

<sup>50</sup> Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

<sup>51</sup> LOPDGDD

<sup>52</sup> Ley General de Comunicación Audiovisual (LGCA) de 7 de julio de 2022

que permitan a los ciudadanos de todas las edades utilizar con eficacia y seguridad los medios, acceder y analizar críticamente la información, discernir entre hechos y opiniones, reconocer las noticias falsas y los procesos de desinformación y crear contenidos audiovisuales de un modo responsable y seguro”.

Se establece una gran importancia en la educación en línea, por lo que se estipula en el Art 83 de la LOPDGDD el Derecho a la educación digital dentro del sistema educativo, entendiéndose así la educación como el principal disipador de las *fake news*.

Para terminar, en cuanto a aquellas *fake news* que afecten a los ciudadanos, es decir, a interesados particulares causándoles un perjuicio real, se establece el derecho de aquéllos, en virtud del Art 86 de la LOPDGDD, “a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan”<sup>53</sup>. Esto es aplicable para los casos en que la “información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación”, requiriendo, para ello que exista un perjuicio en el afectado.

## **Conclusión**

Hemos podido comprobar lo que posiblemente sea uno de los Derechos Fundamentales más relevantes en la actualidad con un crecimiento exponencial para un futuro próximo. Además de la cantidad de áreas que abarca, se torna imprescindible para la difícil tarea que es la defensa de nuestros datos en internet, donde cualquier información personal es más que valiosa, así como difícil de interrumpir su difusión.

Gracias a una legislación actualizada y con unos valores de protección altamente a favor del interesado se nos brindan una serie de garantías que en el internet primitivo no eran imaginables, otorgándole la capacidad de disposición a los usuarios, así como los medios para lograrlo.

En cuanto a las *fake news* no queda más remedio que la solución por excelencia: dotar a los ciudadanos de herramientas y conocimientos para que puedan discernir acerca de la información y realizar por ellos mismos un juicio en compromiso con la verdad. Todo

---

<sup>53</sup> LOPDGDD

ello con el objetivo de no incurrir en una censura y control por parte de una tercera parte como desgraciadamente sucede en Estados autocráticos donde la única voz válida es la del poder y no fruto de la libertad como ciudadanos.

## **Bibliografía**

- LÓPEZ SÁEZ, M: *Una revisión del derecho fundamental a la protección de datos de carácter personal*, Ed. Tirant lo Blanch, 2018
- VILLAVERDE MENENDEZ, I: “Protección de Datos Personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993, *Revista española de Derecho Constitucional*, núm 41, pág 187-224
- Garriga Domínguez, A: “Nuevos Retos para la Protección de Datos Personales en la Era Del Big Data y de la Computación Ubicua: El derecho a la intimidad personal y familiar”, disponible en <https://vlex.es/vid/derecho-intimidad-personal-familiar-642494381> (fecha última de consulta: 1 de septiembre de 2022)
- STC de 20 de julio de 1993 (rec. núm 254/1993) (<https://www.boe.es/buscar/doc.php?id=BOE-T-1993-21425>)
- STC de 30 de noviembre del 2000 (rec. Núm 292/2000) (<https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332>)
- STS (sala de lo penal) de 29 de abril del 2019 (rec. núm 1383/2019) (<https://www.poderjudicial.es/search/openDocument/223bdb1d5d682b47>)
- STJUE (Gran Sala) de 13 de mayo de 2014 (asunto C-131/12) (<https://curia.europa.eu/juris/document/document.jsf?jsessionid=D5664FBF0AFB6C6CD68A48F4AF54324B?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=12346325>)
- STJUE (Gran Sala) de 1 de octubre de 2019 (Asunto C-673/17) (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=12361979>)
- Derecho de supresión ("al olvido"): buscadores de internet (AEPD): disponible en <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido>

- AEPD: “Guía sobre el uso de las cookies”, Disponible en <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies> (fecha de consulta: 28 de agosto de 2022)
- AEPD: “Según el RGPD ¿Cómo debe solicitarse el consentimiento de los interesados para tratar sus datos personales?”, Disponible en <https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/4-consentimiento-de-los-interesados/FAQ-0211-segun-el-rgpd-como-debe-solicitarse-el-consentimiento-de-los-interesados-para-tratar-sus-datos-personales> (fecha de consulta: 30 de agosto de 2022)
- AEPD: “Guía sobre la seguridad y privacidad en internet”, disponible en <https://www.aepd.es/es/documento/guia-privacidad-y-seguridad-en-internet.pdf> (fecha de consulta: 30 de agosto de 2022)
- AEPD: “Qué es el derecho a la limitación de datos”, disponible en <https://www.aepd.es/es/preguntas-frecuentes/1-tus-derechos/FAQ-0112-que-es-el-derecho-a-la-limitacion-del-tratamiento-de-datos> (fecha de consulta: 30 de agosto de 2022)

