FACULTAD DE DERECHO

UNIVERSIDAD DE LEÓN

CURSO 2022/2023

LA HUELLA DIGITAL.

FINGERPRINT.

GRADO EN DERECHO

AUTOR/A: D. EDUARDO REVILLA ALONSO

TUTOR/A: D.JOSE MANUEL ALIJA PÉREZ

Índice

Abreviaturas

- **AEPD:** Agencia Española de Protección de Datos.
- **BOE:** Boletín Oficial del Estado.
- **CDFUE:** Carta de los Derechos Fundamentales de la Unión Europea.
- **DPD:** Delegado de Protección de Datos.
- **IDC:** International Data Corporation.
- **INCIBE:** Instituto Nacional de Ciberseguridad.
- **IP:** Dirección del protocolo de internet.
- **LO:** Ley Orgánica.
- **LOPD:** Ley Orgánica de Protección de Datos de Carácter Personal.
- **LOPDGDD:** Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.
- **LORTAD:** Ley Orgánica de Tratamiento Automatizado de Datos de Carácter Personal.
- **OCDE:** Organización para la Cooperación y el Desarrollo Económicos.
- **RAE:** Real Academia Española.
- **RGPD:** Reglamento de Protección de Datos.
- **SSL:** Secure Sokets Layer
- **STC:** Sentencia del Tribunal Consitucional.
- **TFUE:** Tratado de Funcionamiento de la Unión Europea.
- **TJUE:** Tribunal de Justicia de la Unión Europea.
- **URL:** Uniform Resource Locator.
- **VPN:** Virtual Private network.

Resumen

La huella digital tiene un valor muy importante en lo que respecta a todos los datos que cada persona deja durante el uso de internet. En el presente Trabajo de Fin de Grado se intentará identificar la regulación de la protección de datos en relación con el uso de la huella digital. Para ello, se analizará el concepto de huella digital desde diferentes perspectivas, llevando a cabo el estudio de los diferentes usos que se pueden llevar a cabo de la misma, haciendo referencia a los posibles problemas y recomendaciones, así como el tratamiento de la protección de datos tomando como fundamento el consentimiento. Posteriormente, se llevará a cabo el examen de una sentencia del Tribunal de Justicia de la Unión Europea respecto al derecho de supresión, que es configurado como un derecho fundamental en la legislación europea y finalmente nos centraremos en el régimen jurídico del uso de la huella digital y de la protección de datos a nivel europeo y nacional, así como su evolución a lo largo de los años hasta la configuración actual del mismo.

Palabras clave: Huella digital, protección de datos, consentimiento y derecho de supresión.

Abstract

The fingerpint has a very important value in regards to all the data that each person leaves while using the Internet. In this Final Degree Project, an attempt will be made to identify the regulation of data protection in relation to the use of the fingerpint. For this, the concept of fingerpint will be analyzed from different perspectives, carrying out the study of the different uses that can be carried out of it, referring to possible problems and recommendations, as well as the treatment of data protection. based on consent. Subsequently, the examination of a judgment of the Court of Justice of the European Union will be carried out regarding the right of deletion, which is configured as a fundamental right in European legislation and finally we will focus on the legal regime of the use of the fingerprint and data protection at a European and national level, as well as its evolution over the years up to its current configuration.

Keywords: Fingerprint, data protection, consent, right of deletion,

Objetivos del trabajo

El objetivo general del presente trabajo es identificar la regulación de la protección de datos personales relacionados con el uso de la huella digital.

Para ello, se plantean tres objetivos específicos:

- Fomentar la educción sobre el tema principal dando recomendaciones basadas en la evidencia actual.
- Realizar un estudio detallado de la sentencia que reconoció por primera vez el derecho de supresión o al olvido digital.
- Identificar la evolución de la normativa en esta materia, centrando el tema en el reconocimiento del derecho a la supresión o al olvido digital.

Metodología

Se ha realizado una revisión bibliográfica narrativa de diferentes fuentes bibliográficas y normativas, junto con diversos artículos publicados en revistas de derecho con la finalidad de elaborar el presente Trabajo de Fin de Grado. Tras llevar a cabo una búsqueda detallada y analizar de manera exhaustiva las diferentes fuentes encontradas, se ha conseguido observar la evidencia actual sobre la huella digital y su uso. Han sido numerosas fuentes las que han reflejado la situación actual en la cual hay un déficit de conocimientos sobre este tema en los usuarios.

Se ha seguido el siguiente esquema a la hora de realizarlo:

1. Elección del tema a tratar para la elaboración del presente Trabajo Fin de Grado.
2. Designar el título apropiado para el tema seleccionado.
3. Propuesta de objetivos del trabajo y la estructura del mismo.
4. Recopilación bibliográfica, lectura crítica y realización del trabajo.

Tras la lectura crítica de las diversas fuentes, normativas y artículos seleccionados, se ha realizado un análisis exhaustivo de la información obtenida y se comenzó a elaborar el presente trabajo según la estructura y los objetivos citados anteriormente.

Introducción

La Agencia Española de Protección de Datos (AEPD) define la huella digital de un dispositivo como la forma de recopilar de manera sistemática información sobre un dispositivo remoto específico, con el propósito de identificarlo y distinguirlo, permitiendo así realizar un seguimiento de la actividad del usuario y crear un perfil de este último.

Tradicionalmente, las cookies eran el método de seguimiento empleado a la hora de obtener esta información sobre un dispositivo remoto específico. Actualmente, se ha observado que se están empleando métodos de seguimiento más avanzados que han superado a estas.

Las nuevas técnicas se basan en la recopilación de información específica del navegador web y/o dispositivo de navegación, y su combinación permite crear un identificador único para cada usuario. Sin embargo, la legitimidad de estas técnicas no está claramente establecida.

La huella digital del dispositivo, definida en la lengua española, se conoce como *device fingerprinting*, *browser fingerprinting* o simplemente *fingerprinting* en la terminología anglosajona, la cual usaremos a lo largo del trabajo.

Estos términos, definidos de una manera más sencilla, hacen referencia al conjunto de datos obtenidos del dispositivo del usuario. Estos datos permiten identificarlo de manera única, con ello, las entidades que utilizan técnicas de huella digital recopilan sistemáticamente información de todos los dispositivos que se conectan a sus servidores con el objetivo de distinguirlos y seguir la navegación del usuario para crear un perfil.

Existen diversas técnicas de huella digital; mediante estas se accede a una página web donde el navegador ejecuta una serie de procesos en el dispositivo, sin un conocimiento previo, con la finalidad de recopilar una cantidad suficientemente detallada de datos para que se pueda identificar de forma individual y se transmita al servidor para su posterior uso.

Las cookies, por su parte, son ampliamente reconocidas y aceptadas por el servidor web pudiendo realizar un seguimiento de la navegación de los usuarios con la garantía de

que al eliminarse, se eliminará también el vínculo entre el dispositivo y la información recopilada.

Por el contrario, el uso de la huella digital en el dispositivo permite volver a asignar al mismo usuario la información asociada al identificador de la cookie eliminada; con esto no se perdería la trazabilidad de los datos de navegación del usuario o el seguimiento[1].

1. Capítulo 1: La huella digital del dispositivo.

Las técnicas de identificación mediante el uso de la huella digital del dispositivo son definidas como las *"cookies monsters"*. De esta forma no se requiere instalar ningún tipo de cookie en el dispositivo para poder recopilar dicha información.

Existen diferentes tipos de técnicas que pueden utilizarse para obtener la huella digital de un dispositivo de manera muy precisa como son: canvas fingerprint, el canvas font fingerprint, el web RTC fingerprint o el audio fingerprint.

El uso de estas técnicas es con el propósito de rastrear a los usuarios durante su navegación web y recopilar, a su vez, información sobre sus hábitos e intereses sin que el propio usuario del dispositivo sea consciente de esto. Además, el uso de estas técnicas también puede ser con fines legítimos, pudiendo formar parte de mecanismos de autenticación de múltiples factores.

La obligación de proporcionar información sobre este acto, es común que se encuentre en los sitios web y aplicaciones mediante cláusulas de privacidad específicas que permiten dar el consentimiento para el uso de las cookies. En cuanto a la huella digital, no es tan común encontrar información para el usuario sobre el uso de estas técnicas de seguimiento[1].

1.1 Como dejamos las huellas digitales

Como sabemos, las huellas digitales pueden ser usadas para rastrear las acciones de los usuarios. Estas son la base para que los proveedores de servicios en línea y otras

[1] AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio: Fingerprinting o Huella digital del dispositivo* [En línea] [Consultado el 4 de junio de 2023]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

personas interesadas puedan crear perfiles de usuarios. Es por esto, por lo que las personas que utilicen Internet deben ser conscientes del uso de su privacidad y de las huellas digitales.

A la hora de visitar un sitio web, revelamos información personal al propietario del sitio. Esta información personal puede ser nuestra dirección del protocolo de internet (IP), que puede revelar desde nuestra ubicación geográfica exacta, el tipo de navegador, el último sitio que visitamos online y el sistema operativo que utilizamos.

Esto puede representar un problema para algunas personas, aunque sean datos demasiado superficiales. Muchos servicios en línea u online necesitan vincular múltiples interacciones para determinar si el usuario está realizando una actividad en un momento. Es cierto que varias personas pueden estar usando la misma dirección IP al mismo tiempo, lo cual no resuelve el problema.

El uso de las cookies para abordar este problema sería una solución. Las cookies son una forma de vincular múltiples acciones realizadas por el mismo usuario y poder crear una conexión.

Las decisiones de seguridad de una transacción se basan en una combinación de diferentes factores, en los que por supuesto se incluyen las cookies; pero hay otros mecanismos como la propia dirección IP, o las cadenas que identifican al navegador[2].

Sin embargo, en lugar de las cookies, el uso de la huella digital en el dispositivo permite volver a vincular la información asociada al identificador de la cookie eliminada al mismo usuario. De esta manera, no se pierde la capacidad de rastrear los datos de navegación del usuario ni realizar un seguimiento de sus actividades[1].

[2] BUA. BIBLIOTECA DE LA UIVERSIDAD DE ALICANTE. *La Huella Digital* [En línea] [Consultado el 6 de junio de 2023]. Disponible en: https://rua.ua.es/dspace/bitstream/10045/79601/1/CI2_intermedio_2017-18_Huella-digital.pdf

1.2 Quienes utilizan las huellas digitales

La intensa utilización de las huellas digitales dejadas por los usuarios en Internet con el fin de rastrearlos y personalizar el contenido es una consecuencia de intercambio económico relacionado con Internet.

Las huellas digitales existirían incluso sin tener ningún propósito comercial, pero este aspecto comercial de Internet ha aprovechado la oportunidad que representan estas huellas. Los anunciantes y comerciantes dependen actualmente del poder que les concede las huellas digitales para observar, vigilar y recopilar datos sobre los usuarios de internet.

El marketing, actualmente es quien sostiene al Internet; en casi todos los casos, cada vez que visitamos una página de internet, se nos refleja un anuncio, es decir, los comerciantes salen beneficiados. En el ámbito de la publicidad y el seguimiento en línea, principalmente son los anunciantes, los agregadores y los editores quienes se benefician. ´

En su mayoría, las huellas digitales se utilizan en un contexto comercial por empresas que desean ofrecernos productos y servicios. Sin embargo, también existe el riesgo de que las huellas digitales resulten una pérdida de anonimato a través del intercambio de información entre terceros que tienen poca consideración por la privacidad del consumidor[2].

1.3 Problemas que puedan ocasionar las huellas digitales

Entre los efectos secundarios derivados de las huellas digitales nos encontramos ante la pérdida de privacidad y el anonimato en línea, lo cual atenta contra el valor social de Internet. Cuando se participa en diversas actividades en Internet, no se es consciente de que se dejan evidencias de lo que se ha estado realizando como los lugares visitados, los pensamientos, conexiones con amigos y familiares… Las huellas que se dejan con el tiempo aumentan.

La Declaración Universal de Derechos Humanos garantiza a todos el “derecho a la privacidad”, pero no existe un consenso universal sobre cómo se aplica la privacidad en internet.

Además, las huellas digitales no solo son un riesgo en cuanto a la privacidad, sino también en cuanto a los intereses de las personas en otras áreas, como el anonimato. A la hora de compartir huellas digitales de usuarios entre empresas con fines publicitarios, la violación de la privacidad y la disminución del anonimato pueden aparecer.

Es por todo esto que la pérdida de privacidad y anonimato no solo afecta a nivel individual, sino también disminuye la confianza con los usuarios de internet y perjudica a la comunidad de Internet en su conjunto[2].

1.4 Recomendaciones sobre el uso de la huella digital

El Instituto Nacional de Ciberseguridad (INCIBE), es una entidad creada por el Ministerio de Asuntos Económicos y Transformación Digital de España, que se trata de una sociedad mercantil estatal y medio propio, organizada como sociedad anónima.

A través de esta entidad se sabe que no es posible eliminar por completo nuestra presencia en línea, ya que siempre se dejan rastros en Internet o a la hora de compartir inadvertidamente mediante metadatos. Lo que sí es cierto, es que podemos recudir significativamente la huella digital al adoptar ciertos hábitos y adquiriendo ciertos conocimientos básicos.

Debemos apuntar que hoy en día muchas redes sociales eliminan los mandatos al cargar imágenes en línea. Aún así, sigue siendo no recomendable subir imágenes de lugares fácilmente identificables o de ubicaciones importantes en el entorno del usuario. No se recomienda tomar fotos donde se muestre información sensible.

En cuanto a los datos en documentos, existen diferentes herramientas que permiten eliminar los mandatos antes de subir los propios archivos a la red, evitando así posibles fugas de información.

A su vez, a la hora de utilizar navegadores se ha de usar los que ofrezcan opciones de configuración para minimizar la huella digital. El uso de una *Virtual Private network (VPN),* siendo una red privada virtual, también puede ser útil para mejorar la privacidad en línea y reducir así la huella digital. Al conectarte mediante una VPN, la información

transmitida está protegida, lo que dificulta saber quién está accediendo a un sitio web y desde que dispositivo se está accediendo[3].

Por otra parte, existen cuatro niveles en los que podemos tomar medidas adicionales:

Nivel 1: Mejorar la compresión de los problemas fundamentales: Es importante reflexionar sobre las implicaciones de compartir cualquier tipo de información en Internet, ya que en mayor o menor medida esto pone en riesgo la privacidad.

Nivel 2: Desarrollar hábitos básicos de "higiene": La privacidad es contextual, por lo que utilizar diferentes identidades para diferentes aspectos de la vida en línea, como tener una dirección de correo electrónico para el trabajo y otra para asuntos personales, o utilizar una tarjeta de crédito específica para compras en línea, ayuda a mantener separadas las diferentes partes de la huella digital.

Nivel 3: Es importante familiarizarse con las configuraciones por defecto de navegadores, dispositivos y aplicaciones, ya que a menudo favorecen la divulgación de información personal en lugar de protegerla. Se debe aprender a utilizar estas herramientas de manera efectiva para mejorar la privacidad.

Nivel 4: Encontrar y utilizar herramientas específicas para mejorar la privacidad: Existen numerosas herramientas disponibles, especialmente para navegadores, para mejorar la privacidad. Estas herramientas protegen áreas específicas de nuestra huella digital y también mantiene al usuario informado ayudándole a comprender información buscando los proveedores de servicios.

También se recomienda hacer uso de la gestión de las cookies ajustando las configuraciones del navegador para bloquear cookies de terceros, revisar la configuración de privacidad en servicios públicos como redes sociales y blogs, comprender las implicaciones de compartir datos y buscar las herramientas y la motivación necesarias para tomar decisiones más informadas; aunque como sabemos, esto no exime de todos los datos que quedan grabados por la huella digital[2].

[3] INCIBE. *Como Evitar Que La Huella Digital Afecte Nuestras Empresas* [En línea]. [Consultado el 17 de junio de 2023]. Disponible en: https://www.incibe.es/empresas/blog/como-evitar-que-la-huella-digital-afecte-nuestras-empresas

2. Capítulo 2: La Protección de Datos Personales

La protección de datos personales hace referencia a la garantía o la capacidad de controlar nuestra propia información frente a su procesamiento automatizado o no, abarcando no solo los datos almacenados en sistemas informáticos, sino también en cualquier medio que permita su uso, almacenamiento, organización y acceso.

Este campo de estudio está abarcado en el ámbito del Derecho Informático, el Derecho de la Información, los Derechos Humanos y el Derecho Constitucional. Además, ha de abarcar el Derecho de Supresión.

En algunos países, la protección de datos está reconocida constitucionalmente como un derecho humano, mientras que en otros se establece mediante determinadas leyes. Este derecho es protegido a través del derecho a la privacidad y al respeto de la confidencialidad de las comunicaciones[4].

El tratamiento de los datos puede basarse en el cumplimiento de una misión de interés público, el ejercicio de poderes públicos conferidos al responsable del tratamiento, el cumplimiento de una obligación legal o el consentimiento de las personas interesadas.

Es importante mencionar la figura del Delegado de Protección de Datos (DPD), quien tiene las funciones de atender consultas y reclamaciones, ya que es responsable de los diferentes tratamientos de datos personales. Este actúa en conjunto con la Agencia Española de Protección de Datos (AEPD)[5].

El derecho a la protección de datos personales es un derecho fundamental que permite a las personas tener el control sobre el tratamiento de sus propios datos, ya sea en formatos manuales o automatizados, y respecto a aspectos relacionados con su vida íntima o privada. Este derecho se encuentra estrechamente vinculado con la dignidad

[4] GUAMANZARA TORRES LH. RIOFRÍO, J.C. *El derecho de los secretos.* Bogotá: Temis. Ius Hum Law J [En línea] [Consultado el 7 de junio de 2023];2(2):249–51. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4999992

[5] MINISTERIO DE TRANSPORTES M Y AU. *Protección de datos personales* [En línea] [Consultado el 7 de junio de 2023]. Disponible en: https://www.mitma.gob.es/el-ministerio/buen-gobierno/proteccion-datos-personales

humana, así como con otros derechos como la intimidad, el acceso a la información, la libertad, la autodeterminación informática y la libertad de información.

En el núcleo de este control se encuentra el consentimiento previo, expreso, informado, inequívoco y verificable que otorga el titular de los datos para que estos sean tratados de manera legítima. El consentimiento del individuo constituye el elemento central que le permite ejercer dicho control sobre sus datos personales[6].

2.1 El consentimiento como fundamento del tratamiento de los datos personales

El consentimiento del individuo es considerado una base legal y un factor habilitante que permite el tratamiento íntegro de los datos personales. Este consentimiento ha adquirido un papel fundamental en el ámbito del derecho de protección de datos, ya que en la Carta de los Derecho Fundamentales de la Unión Europea se estable que los datos personales han de ser tratados de manera justa y con un propósito específico, basado en el consentimiento del individuo o en otros fundamentos legales previstos por la ley.

El Tribunal Constitucional destaca que el consentimiento del interesado es el elemento clave del sistema de protección de datos personales, salvo en las situaciones que exista una habilitación legal para el tratamiento de estos datos sin consentimiento.

Por otro lado, el Reglamento de Protección de Datos (RGPD) establece que el tratamiento de datos será lícito cuando el usuario haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

El consentimiento informado debe cumplir una serie de requisitos para poder establecerse; este ha de ser: libre, específico, informado e inequívoco, tal y como es enunciado en el RGDP. Este consentimiento siempre ha de ser otorgado antes del tratamiento de los datos personales y puede ser revocado por el usuario en cualquier momento, sin que esto afecte a la legalidad del tratamiento realizado hasta ese mismo

[6] GÓMEZ-CÓRDOBA AI, ARÉVALO-LEAL S, BERNAL-CAMARGO DR, ROSERO DE LOS RÍOS D. *El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia.* Rev Bioet Derecho [En línea] [Consultado el 11 de junio de 2023];(50):271–94. Disponible en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017

momento. En conclusión, el consentimiento del usuario desempeña un papel esencial en el tratamiento de datos personales y debe ser obtenido de una forma consciente, cumpliendo con los requisitos enumerados en el RGPD[7].

2.2 Principios de Calidad de los Datos Personales

El RGPD establece un conjunto de principios que deben ser seguidos por los responsables del tratamiento de datos personales:

1. *‘‘Principio de "licitud, transparencia y lealtad": Los datos deben ser tratados de manera legal, justa y transparente para el interesado.*
2. *Principio de "finalidad": Los datos deben ser tratados con uno o varios propósitos específicos, explícitos y legítimos. Está prohibido tratar los datos recopilados con un propósito diferente e incompatible con el inicial*
3. *Principio de "minimización de datos": Se deben aplicar medidas técnicas y organizativas para garantizar que solo se traten los datos necesarios para cada finalidad específica. Esto implica limitar la cantidad de datos recopilados, reducir la duración de su almacenamiento y restringir su accesibilidad.*
4. *Principio de "exactitud": Los responsables deben tomar medidas razonables para asegurar que los datos sean precisos, y deben eliminar o corregir sin demora aquellos que sean inexactos o incompletos en relación con los fines del tratamiento.*
5. *Principio de "limitación del plazo de conservación": Los datos deben ser almacenados durante el tiempo necesario para cumplir con los fines establecidos. Una vez que se han logrado dichos fines, los datos deben ser borrados, bloqueados o anonimizados para evitar su identificación.*

[7] EDPB. *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* [En línea] [Consultado el 11 de junio de 2023]. Disponible en:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

6. *Principio de "seguridad": Los responsables del tratamiento deben realizar análisis de riesgos y tomar medidas técnicas y organizativas adecuadas para garantizar la seguridad, integridad y confidencialidad de los datos personales.*

7. *Principio de "responsabilidad activa" o "responsabilidad demostrada": Los responsables deben llevar a cabo una diligencia continua para proteger y garantizar los derechos y libertades de las personas cuyos datos son tratados. Esto implica realizar análisis de riesgos y demostrar que el tratamiento cumple con las disposiciones del RGPD y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (*LOPDGDD).”*[8]

3. Capítulo 3: Derecho de supresión (“Al olvido”)

El derecho de supresión es un derecho fundamental establecido en la legislación europea de protección de datos[9]. Este derecho es definido por el Diccionario de la Real Academia Española (RAE) como *“Derecho del interesado a que el responsable del tratamiento suprima todos o algunos de sus datos personales y se abstenga de darles más difusión, cuando ya no son necesarios para los fines para los que fueron recogidos o tratados”*[10]. El derecho al olvido brinda a las personas la capacidad de solicitar la eliminación de su información personal en situaciones en las que esta información esté desactualizada, no sea deseada o incluso esté incorrecta. Este derecho no es un derecho absoluto. En ciertos casos, es posible que no se pueda eliminar los datos del usuario cuando el tratamiento necesario sea con la finalidad de ejercer la libertad de expresión e información, cumplir con una obligación legal, con una misión de interés público,

[8] AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Principios del Reglamento General de Protección de Datos* [En línea] [Consultado el 17 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

[9] AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Derecho de supresión (“al olvido”)* [En línea][Consultado el 15 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido

[10] RAE. *Diccionario Real Academia Española* (RAE) [En línea] [Consultado el 15 de junio de 2023]. Disponible en: https://dpej.rae.es/lema/derecho-al-olvido-o-derecho-de-supresi%C3%B3n#:~:text=Derecho%20a%20eliminar%2C%20ocultar%20y,2.

ejercer poderes públicos conferidos al usuario, por razones de interés público en el ámbito de la salud pública, fines de archivo de interés público, fines de investigación científica o histórica, fines estadísticos o para el ejercicio o defensa de reclamaciones.

Por lo tanto, este derecho se puede ejercer comunicándose con la persona responsable y solicitando la eliminación de sus datos personales si cumple los siguientes requisitos:

- Un vez que los datos personales del usuario dejan de ser necesarios para los fines para los que fueron recopilados o procesados.
- Cuando el usuario retira el consentimiento del tratamiento de sus datos personales, siempre que no exista otra base legal para dicho tratamiento de datos.
- Si el usuario se opone al tratamiento de sus datos personales ejerciendo el derecho de oposición, y el tratamiento tenía su base en el interés legítimo del usuario o en el cumplimiento de una misión de interés público; no teniendo motivos que justifiquen dicho tratamiento de datos.
- Si el usuario desea que sus datos personales no sean utilizados para actividades marketing directo, incluyendo en dichas actividades la creación de perfiles relacionados.
- Si el usuario considera que sus datos personales han sido tratados de forma ilegal.
- Si el usuario considera necesario eliminar sus datos personales para cumplir con una obligación legal establecida por la legislación de la Unión Europea que sea aplicable al propio usuario del tratamiento.
- Si los datos personales del usuario se obtuvieron en relación con la oferta de servicios de la sociedad de la información a menores [9].

En resumen, este derecho hace referencia a la capacidad de solicitar la eliminación de datos personales en situaciones específicas cuando existe el riesgo de que su existencia en Internet pueda infringir los derechos al honor y a la intimidad personal[11].

Este derecho se fundamenta en el derecho a la protección de datos, reconocido constitucionalmente de manera amplia en la Constitución Española. Según este derecho se garantiza a los usuarios el poder de control y disposición sobre sus datos personales, lo que implica una serie de facultades esenciales, como el consentimiento para la recopilación y uso de los datos, el conocimiento de quién los posee y con qué propósito, así como el derecho a oponerse a esa posesión y uso, exigiendo que se ponga fin a la posesión y utilización de dichos datos[12].

Por lo tanto, la justificación de este derecho se fundamenta en la creencia en la capacidad de reinserción, cambio y mejora del individuo, lo cual pone en duda si este tipo de información personal debe ser publicada por los motores de búsqueda y, por lo tanto, estar accesible al público en general; surgiendo así el derecho al olvido, con la finalidad de evitar que el pasado se convierta en un presente continuo[13].

Dependiendo de la tradición jurídica del país que regule dicho derecho se establecen unos límites. En nuestro país, el Tribunal Constitucional destaca la configuración y protección del bien jurídico de la privacidad, de la cual se derivan facultades de control

[11] FERNÁNDEZ JPM. *La protección de datos y los motores de búsqueda en Internet: Cuestiones actuales y perspectivas de futuro acerca del derecho al olvido / Data protection and Internet search engines: current issues and future perspectives about the right to be forgotten.* Rev Derecho Civ [En línea] [Consultado el 17 de junio de 2023] Disponible en: https://www.nreg.es/ojs/index.php/RDC/article/view/280

[12] SENTENCIA DEL TRIBUNAL CONSITUCIONAL DE 30 NOVIEMBRE DEL 2000 [RTC\2000\290]. *La aplicación judicial del derecho comunitario ne España durante 2000 Y 2001* [En línea] [Consultado el 7 de junio de 2023]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/266015.pdf

[13] DE LA CUEVA CONZÁLEZ-COTERA J. *Relato del VII Congreso Internacional sobre Internet, Derecho y Política: neutralidad de la red y derecho al olvido. IDP Rev Internet Derecho Política* [En línea] [Consultado el 11 de junio de 2023];(13):84–90. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3865410

sobre los datos e información del individuo. Como se menciona en algunas sentencias sobre la privacidad electrónica, nos encontramos en una situación de falta de protección para los usuarios de Internet, lo cual impacta directamente en el ámbito de la dignidad individual[14].

3.1 El caso de Google con respecto al Derecho de Olvido.

El 13 de Mayo del 2014, El Tribunal de Justicia de la Unión Europea (TJUE) respaldó el "Derecho al Olvido", como un reciente fallo con profundas consecuencias para los motores de búsqueda en Europa, como es Google[15]. El tribunal declaró que los motores de búsqueda debían eliminar los enlaces de la información publicada en el pasado que perjudicasen al usuario y ya no fueran pertinentes, es decir, cuando los resultados se consideren inadecuados, irrelevantes, ya no relevantes o excesivos. Se ha considerado que los gestores de motores de búsqueda son responsables del tratamiento de los datos personales que aparecen en las páginas web publicadas por terceros. En caso de que estos gestores se negaran a acceder a la solicitud, el usuario puede acudir a las autoridades competentes para que se eliminen los enlaces de la lista de resultados, bajo ciertas condiciones establecidas por el tribunal.

Esta sentencia fue emitida por la consulta de un ciudadano español llamado Mario Costeja González, quien solicitó la eliminación de los enlaces a información perjudicial tal y como se cita en su "Derecho de Olvido". La consulta paso a mano de las autoridades judiciales españolas en relación con el litigio entre la Agencia Española de Protección de datos y Google[16].

---

[14] LÓPEZ PORTAS MB. *La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE.* Rev derecho político [En línea] [Consultado el 17 de junio de 2023];1(93):143–75. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5169233

[15] GOOGLE. *Preguntas frecuentes – Privacidad y Condiciones – Google* [En línea] [Consultado el 15 de junio de 2023]. Disponible en: https://policies.google.com/faq?hl=es

[16] INFOCURIA JURISPRUDENCIA I. *Sentencia del Tribunal de Justicia.* [En línea] [Consultado el 15 de junio de 2023]. Disponible en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&amppageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=276332

Desde que esta sentencia fue emitida, Google ha estado trabajando arduamente para cumplirla. Este proceso es complejo, ya que cada solicitud debe ser evaluada de forma individual, equilibrando el derecho de la persona a controlar sus datos personales con el derecho del público a acceder y difundir información por parte del gestor.

La sentencia del tribunal representa un cambio significativo para los motores de búsqueda, con lo cual se encuentran trabajando en un diseño de un proceso que cumpla con la ley. Google ha actualizado su versión con un aviso que indica que los resultados pueden haber sido modificados de acuerdo con la legislación europea de la protección de datos a la hora de realizar una búsqueda de un nombre.

Los resultados de búsqueda de Google muestran el contenido que está disponible públicamente en Internet para todos los usuarios. El hecho de eliminar resultados de búsqueda de Google no implica eliminar el contenido en sí ya que los motores de búsqueda no tienen la capacidad de eliminar directamente el contenido de los sitios web.

Google avisa en su política que si se desea eliminar contenido específico de Internet, se debe comunicar con el administrador del sitio web donde aparece ese contenido y solicitarle que lo modifique o elimine. Cuándo el contenido haya sido eliminado y Google detecte la actualización, dejará de aparecer en los resultados de búsqueda.

Google propone usar la búsqueda cifrada conocida como la búsqueda SSL (Secure Sockets Layer), ya que en la mayoría de casos, los términos de búsqueda no se mostrarán en la URL (Uniform Resource Locator) de referencia. Aunque este motor de búsqueda también expone que existen algunas excepciones a esto, como cuando se utilizan navegadores menos populares. Además, los anunciantes pueden recibir información sobre las palabras clave exactas que llevaron a hacer clic en un anuncio[15].

3.2 Derecho de información

El derecho de información es un derecho fundamental establecido en la legislación europea de protección de datos que hace referencia a la obligación del responsable del tratamiento de proporcionar información cuando se recopilan los datos personales del usuario.

A la hora de cumplir con este derecho, la Agencia Española de Protección de Datos recomienda proporcionar la información por distintos niveles, de la siguiente manera:

Primer nivel o capa: información básica.

- Identidad del responsable del tratamiento.
- Breve descripción de los fines del tratamiento, incluyendo la elaboración de perfiles si corresponde.
- Base legal del tratamiento.
- Posibilidad de cesión de datos a terceros o transferencias a países fuera de la Unión Europea.
- Referencia al ejercicio de derechos.

Segundo nivel o capa: Información adicional.

- Datos de contacto del responsable del tratamiento, representante (si corresponde) y delegado de protección de datos (si corresponde).
- Descripción ampliada de los fines del tratamiento, plazos de conservación de los datos, decisiones automatizadas, perfiles y lógica aplicada.
- Detalles sobre la base legal del tratamiento en casos de obligación legal, interés público o interés legítimo, y la obligación o no de proporcionar datos y las consecuencias de no hacerlo.
- Destinatarios de los datos, decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.
- Instrucciones sobre cómo ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento, retirada del consentimiento y derecho a presentar una reclamación ante la Autoridad de Control.
- Información sobre datos obtenidos de fuentes distintas al propio interesado, incluyendo la fuente y, en la información adicional, el origen detallado de los datos y la categoría de datos tratados.

En caso de que tus datos personales no hayan sido obtenidos directamente del usuario, se proporcionará información adicional sobre la fuente y el origen de los datos. Esta

información debe ser proporcionada en un plazo razonable; es decir, no ha de exceder un mes, a menos que existan circunstancias específicas en las que se deba proporcionar antes, como en el caso de una comunicación directa con el interesado o si se van a divulgar los datos a otro interesado[17].

3.3 Derecho a la intimidad y privacidad

El derecho a la intimidad y a la privacidad son derechos esenciales de la persona, sobre todo para los valiosos bienes personales que surgen de la propia personalidad del usuario. Éste tiene derecho de exigir protección para ejercer el derecho a la vida.

Estos derechos pertenecen a los derechos íntimos, los cuales deben ser respetados ya que son valores fundamentales que sirven como base para el ejercicio de otros derechos. Estos derechos se caracterizan por ser: fundamentales, originarios, innatos, no relacionados con el patrimonio, opinables a todos, imprescindibles y los cuales no pueden renunciarse y no son transferibles.

A principios de época, este derecho no era reconocido de manera autónoma ya que se fundamentaba en el derecho de propiedad o en la violación de lealtad. El hecho de que no se reconociera como un derecho independiente no daba pie a que no se existiera.

Estos derechos se basan fundamentalmente en que solo el usuario es capaz de hacer públicas cuestiones relacionadas con su intimidad.

Actualmente, la intimidad y privacidad del usuario se ve constantemente amenazada por el rápido avance de la tecnología y el desarrollo de los medios de comunicación. No existe la posibilidad de establecer límites precisos de antemano para determinar cuándo se invade la intimidad o privacidad del usuario; corresponde a la jurisprudencia determinar el alcance exacto de este ámbito teniendo en cuenta cada caso y circunstancias[18].

---

[17] AEPD. *Derecho de información* [En línea] [Consultado el 15 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-informacion

[18] URQUIAGA EP. *Los Derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información.* [En línea] [Consultado el 17 de junio de 2023]. Disponible en: https://www.redalyc.org/pdf/197/19760123.pdf

4. Capítulo 4: Régimen jurídico de la huella digital

El derecho a la protección de datos trata de un derecho a la autodeterminación informativa ya que la persona decide qué contar y cómo contarlo. Asimismo, decide no divulgar sus datos personales y que los datos que ya no son necesarios según los fines que se emplearon para los mismos, sean suprimidos.

Es importante determinar cuándo existe interés objetivo en que determinados datos personales sean mantenidos o tratados en el tiempo y para ello es preceptivo el correspondiente análisis estudiando los aspectos subjetivos de los datos personales y los aspectos subjetivos que se encuentren relacionados con las circunstancias del afectado. Tras lo cual, podemos decir que es necesario llevar a cabo un juicio de proporcionalidad para que podamos valorar si la conservación o la difusión de dichos datos personales se llevan a cabo con o sin el consentimiento de su titular o en contra del mismo.

Dicho esto, se debe tener en cuenta el factor tiempo ya que se debe ponderar la permanencia de ese interés en el tiempo dado que el transcurso del mismo puede hacer desaparecer los datos que ya no son necesarios para los fines que fueron tratados. Estos datos pueden convertirse en irrelevantes y el deseo del afectado puede ser que determinados datos personales dejen de ser accesibles al conocimiento público surgiendo así un derecho de protección de los datos personales y un derecho al olvido. Las notas más importantes en lo que a protección de privacidad se refiere son: la limitación de la finalidad, el consentimiento, la confidencialidad y la calidad[19].

El factor tiempo es de trascendental importancia para evaluar si se ha lesionado o no el derecho a la protección de datos personales y más en los tiempos que corren con la nueva sociedad digital ya que puede suponer un peligro que afecte de forma grave a la privacidad de las personas[20].

Respecto al tratamiento jurídico que regula la huella digital y más concretamente en lo que se refiere a la protección de datos y derechos digitales, existe una amplia normativa

[19] RAÚL FERNÁNDEZ J. *Los principios relativos al tratamiento de datos personales en el RGPD - J. Raul Fernández. Abogado* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.jraulfernandez.es/los-principios-relativos-al-tratamiento-de-datos-en-el-rgpd/

[20] GRUPO ATICO 34. *Plazo de Conservación datos personales Rgpd* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/conservacion-datos-plazo/

al respecto. En lo expuesto en el anterior epígrafe respecto a la protección de datos hemos dado unas nociones generales y para ello se necesita como sustento tanto la LO 3/2018 como el Reglamento 2016/679.

A nivel nacional tenemos la Ley Orgánica 3/2018, del 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales y a nivel europeo el Reglamento 2016/679 del Parlamento Europeo y del Consejo del 27 de Abril del 2016. Podemos decir que ambas regulaciones van de la mano y llevaremos a cabo un tratamiento más pormenorizado de la legislación nacional anterior y posterior a dicho reglamento.

Es de trascendental importancia mencionar también los derechos ARCO que se encuentran regulados en la Ley Orgánica 15/1999 de protección de datos de carácter personal.

4.1 Nivel Unión Europea

Un hito normativo significativo en el tema que estamos abordando fue la aprobación de la Directiva 95/46/CE por el Parlamento Europeo y el Consejo el 24 de octubre de 1995. Esta Directiva tenía como objetivo principal garantizar una protección sólida en el tratamiento de datos personales dentro del territorio de la Unión Europea. Su propósito era establecer medidas para evitar obstáculos que limitaran la libre circulación de información, al tiempo que se reconocía el derecho de oposición en casos legítimos[21]. Más de dos décadas después de la aprobación de la Directiva 95/46/CE, la Unión Europea ha promulgado el Reglamento (UE) 2016/679, también conocido como Reglamento General de Protección de Datos (RGPD), el cual entró en vigor en 2018 y reemplaza y anula la mencionada Directiva.

La Directiva de 1995 se creó con el propósito de salvaguardar el derecho fundamental a la protección de datos y garantizar la libre circulación de los mismos. Sin embargo, el contexto en el que se aprobó era muy diferente al actual, marcado por los avances tecnológicos, Internet y la globalización. Por esta razón, la Comisión presentó varias

[21] MORENO BOBADILLA A. *Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital. Estud Const (Impresa)* [En línea] [Consultado el 24 de junio de 2023];18(2):121–50. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002020000200121

propuestas sobre protección de datos, incluida la sustitución de la Directiva 95/46/CE por el actual RGPD. Se llegó a la conclusión de que la Directiva no abordaba los problemas, ni se adaptaba a las nuevas realidades, ni estaba a la altura de los desafíos tecnológicos de ese momento.

En consecuencia, el 5 de octubre de 2010 tuvo lugar una reunión de gran importancia en la que se tomó una decisión y se solicitó la opinión del Grupo de Trabajo sobre Protección de Datos del artículo 29[22]. Era evidente que la Directiva no era adecuada tanto para abordar las necesidades actuales como para salvaguardar el derecho fundamental a la protección de datos. Durante esa reunión, se subrayó la necesidad de establecer un marco legal unificado, es decir, lograr la armonización de las regulaciones en los diversos Estados miembros de la Unión Europea[23].
En este período, la libertad de información y, especialmente, la llegada de nuevas tecnologías han generado cambios en la sociedad y planteado nuevas realidades, lo que requiere que la legislación se adapte a estas circunstancias. Un elemento clave ha sido el cambio en la percepción del habeas data, que pasó de considerarse como una protección de otros derechos, principalmente la intimidad, a ser reconocido como un derecho autónomo e independiente con su propia estructura y lógica interna.

Podemos afirmar que el derecho a la libertad informática ha adquirido autonomía respecto al derecho a la intimidad, convirtiéndose ahora en un derecho fundamental independiente. En este sentido, el legislador comunitario y los tribunales de los Estados miembros han desempeñado un papel fundamental[24]. El reconocimiento del derecho a

[22] *Legado: Grupo de Trabajo del art. 29* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://edpb.europa.eu/about-edpb/more-about-edpb/legacy-art-29-working-party_es

[23] Inglés MCC. *El "derecho al olvido digital". Una exigencia de las nuevas tecnologías, recogida en el futuro reglamento general de protección de datos. Actualidad jurídica iberoamericana* [En línea] [Consultado el 4 de junio de 2023];(5):255–71. Disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=5723770

[24] BOE-T-2001-332 Pleno. *Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica* [En línea] [Consultado el 12 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

la protección de los datos personales no solo se encuentra presente en las Directivas y Reglamentos de la Unión Europea, sino que adquiere una especial importancia en la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), específicamente en su artículo 8.1, y en el Tratado de Funcionamiento de la Unión Europea (TFUE), en su artículo 16.1. Ambos artículos establecen lo mismo; toda persona tiene derecho a la protección de los datos personales que le conciernen.

La legislación necesitaba adaptarse a las nuevas realidades, ya que el objetivo del Reglamento General de Protección de Datos (RGPD) es el mismo que el de la Directiva anterior, pero se produce un cambio significativo en la protección debido a la aparición de nuevas tecnologías, el Big Data y el alto nivel de filtración y exposición de nuestra vida privada, entre otros aspectos. La economía digital parece haberse convertido en un objetivo prioritario para la Unión Europea.

En términos de protección de las personas, los desafíos y riesgos han aumentado debido a las significativas diferencias en el uso de datos personales en comparación con años atrás. Prueba de ello es un estudio publicado por la IDC (International Data Corporation), que lleva a cabo un estudio del consumo de productos digitales con el paso de los años. Podemos llegar a la conclusión de que el universo digital crecerá en un factor 10 duplicando su tamaño cada dos años tras llevar a cabo varios análisis al respecto[25].

La legislación de protección de datos se ha convertido en un símbolo de los elevados estándares del Derecho europeo. En la actualidad, el tratamiento de datos personales por parte de las empresas tiene principalmente fines comerciales, mientras que para los usuarios, proporcionar sus datos a terceros, como en una página web, es simplemente necesario para acceder a los servicios ofrecidos. En muchos casos, incluso se puede negar el uso de un servicio si no se proporcionan los datos, lo que implica una obligación impuesta al usuario. Esta divergencia de intereses puede generar dificultades para salvaguardar los derechos de ambas partes. Como resultado, los legisladores europeos y nacionales buscan proporcionar a los consumidores herramientas para tener cierto control sobre sus datos personales

[25] MESA AR *Big Data: La evolución de los datos* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://openwebinars.net/blog/big-data-la-evolucion-de-los-datos/

El nuevo Reglamento establece precisamente eso, ya que pasar de una Directiva a un Reglamento implica una regulación más uniforme y sólida en toda la Unión Europea, en lugar de una regulación más flexible y abierta para los Estados miembros. Se buscaba superar los obstáculos planteados por los avances tecnológicos y la globalización, y para ello se ha destacado la importancia de una "ejecución estricta" que garantice una mayor seguridad jurídica en toda la Unión Europea. Esta preocupación se refleja claramente en el Documento de Trabajo de la Comisión que sirvió de base para la elaboración del Reglamento y otras disposiciones relacionadas con la protección de datos. En dicho documento se resaltan las barreras que surgen de la fragmentación normativa en materia de protección de datos, la inseguridad jurídica y la falta de coherencia en la supervisión del cumplimiento. Si bien se ha buscado establecer un marco normativo común para realizar acciones conjuntas en todo el territorio europeo, la Directiva dejaba cierto margen de acción a los Estados en la implementación de dichas acciones, lo que condujo a una amplia disparidad en la interpretación y en los planes de acción en cada Estado miembro.

En consecuencia, la Comisión identificó diversas discrepancias en este sentido, dado que la Directiva ofrece una mayor apertura y flexibilidad a los Estados miembros desde el punto de vista legislativo. En contraste, el Reglamento representa una herramienta legislativa más coherente, sólida y restrictiva, con una aplicación más amplia en todo el territorio europeo[26].

El objetivo del nuevo Reglamento es abordar de manera más rigurosa y completa los diferentes aspectos del tratamiento de datos personales, buscando así superar los inconvenientes mencionados. Por primera vez, todos los países de la Unión Europea se encuentran sujetos a una regulación común en materia de protección de datos personales.

El Reglamento General de Protección de Datos ha introducido importantes novedades en cuanto a los derechos de las personas afectadas, estableciendo como principio fundamental que nuestra información personal debe estar bajo nuestro propio control, al

[26] BOE. *Reglamento n V, del Consejo 1234/2007, De octubre de de 22, De mercados agrícolas y se establecen disposiciones específicas para determinados Productos Agrícolas*. [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/doue/2012/012/L00014-00021.pdf

igual que lo hacía la Directiva. Se han proporcionado herramientas de control al individuo para que pueda ejercer sus derechos de manera efectiva.

Esta nueva normativa ha provocado un cambio radical en el ámbito de la protección de datos, ya que ahora se concede al titular de los datos la capacidad de gestionar su propia información personal de acuerdo con sus preferencias. Además, tanto las empresas privadas como las administraciones públicas están obligadas a cumplir con el interés del ciudadano y adoptar políticas activas de protección de datos, lo que ha modificado las reglas del juego existentes hasta ahora. Por lo tanto, el enfoque central se ha centrado en el consumidor y en su protección en caso de violación del derecho a la protección de datos.

Otro aspecto relevante a considerar es el consentimiento. El Reglamento establece en su artículo 7 las condiciones que deben cumplirse para que el consentimiento sea válido, y exige que el responsable del tratamiento de datos pueda demostrar que el interesado ha dado su consentimiento. Aunque el consentimiento puede seguir siendo implícito en algunos casos, cuando se trata de categorías especiales de datos se requiere que sea explícito.

Además, el creciente acceso de los menores a los servicios de la sociedad de la información ha llevado a regular su consentimiento mediante condiciones especiales, las cuales se encuentran establecidas en el artículo 8 del Reglamento[27].

En la nueva normativa se establece una especie de edad mínima para el consentimiento informado, en la que se considera válido el consentimiento otorgado por personas mayores de dieciséis años (aunque los Estados miembros pueden reducirlo hasta los trece años). En el caso de los menores por debajo de esta edad, el uso de servicios de la sociedad de la información queda sujeto a la autorización de quien ejerza la patria potestad o tutela.

[27]BOE. *Artículo 7. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Otro derecho que se ve afectado y está estrechamente relacionado con los mencionados anteriormente es el derecho recogido en el artículo 22, el derecho a no ser objeto de decisiones automatizadas.

Los tradicionales derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) también son objeto de importantes modificaciones en la nueva normativa. Estos derechos se transforman en los derechos de Transparencia, Información, Acceso, Rectificación, Cancelación, Oposición, Limitación del Tratamiento y Portabilidad. Detallaremos estos derechos en el siguiente apartado.

Entre los nuevos derechos incorporados, destaca el derecho recogido en el artículo 17, conocido como derecho de supresión o derecho al olvido, que constituye una de las principales novedades introducidas por el RGPD. Este derecho permite a las personas solicitar al responsable del tratamiento la eliminación de sus datos personales, en determinadas circunstancias. El responsable del tratamiento está obligado a eliminar los datos personales sin demora indebida cuando se cumplan ciertos criterios.

El derecho al olvido digital establece un límite a la memoria de Internet, donde el tiempo es lineal y no distingue entre pasado, presente y futuro. Esto puede provocar, en muchos casos, una vulneración de los derechos fundamentales del individuo al descontextualizar la información, perjudicando su integridad y dignidad personal. La naturaleza jurídica de este derecho se basa en el derecho a la intimidad, a la vida privada y, especialmente, a la protección de datos.

Los ciudadanos tienen la facultad de solicitar la eliminación de sus datos o información personal de Internet cuando pueda afectar a su intimidad o al libre desarrollo de sus derechos fundamentales. Esto se lleva a cabo mediante la presentación de una solicitud a los responsables de los registros, quienes están obligados a eliminar los datos. Nombraremos alguna circunstancias que obliga a la eliminación de los datos; que los datos personales ya no sean necesarios en relación a los fines recogidos, que el interesado retire el consentimiento, que los datos hayan sido tratados ilícitamente etc. Estas condiciones se encuentran recogidas en el artículo 17 del RGPD.

Toda la legislación y la doctrina en este ámbito se han ajustado a las nuevas realidades tecnológicas y al contexto social actual[28].

En este sentido, el Reglamento actual introduce diversos mecanismos, como el cifrado y la seudonimización de los datos personales (según se establece en el artículo 32). Entre las novedades más destacadas, cabe resaltar la promoción del uso de datos personales seudonimizados, con el objetivo de prevenir de manera irreversible la identificación de los individuos y salvaguardar la confidencialidad e integridad de sus datos personales[29]. De igual manera, se establece la exigencia de llevar a cabo una evaluación de impacto, también denominada Privacy Impact Assessment, en casos de tratamiento de datos que puedan implicar riesgos para los derechos y libertades de las personas físicas. Esta evaluación se realiza mediante la aplicación de diversas operaciones destinadas a determinar la magnitud de los riesgos asociados al tratamiento de los datos personales y garantizar su adecuada protección.

Es importante resaltar también el concepto de "responsabilidad activa" (accountability), el cual implica la obligación de tomar las medidas necesarias para cumplir con los principios, derechos y garantías establecidos en el RGPD (Reglamento General de Protección de Datos). Además, se establecen responsabilidades por el incumplimiento de estas medidas, según lo regulado en el artículo 24 del RGPD. El Reglamento requiere una responsabilidad proactiva tanto en el cumplimiento como en la demostración del cumplimiento. En este sentido, el responsable del tratamiento de los datos debe establecer procedimientos que aseguren la aplicación de la normativa de

[28]SANCHO LÓPEZ, M. *GARANTÍAS LEGALES DEL CONCEPTO DE PRIVACIDAD: ENTRE EL DERECHO AL OLVIDO Y EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS [En LÍNEA]* [Consultado el 24 de junio de 2023]. Disponible en: https://revista-aji.com/articulos/2018/9/176-201.pdf

[29] BOE. *Artículo 8. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

protección de datos y que puedan demostrar a terceros la efectividad de su aplicación y cumplimiento. Este concepto se menciona en el artículo 5, apartado 2, del RGPD[30].

Además, se presenta una novedad relacionada con el principio de territorialidad, un aspecto que puede resultar complejo de definir debido a que el ciberespacio es un entorno virtual en el que los límites territoriales tienen poca relevancia o incluso carecen de existencia. Además, las jurisdicciones y competencias territoriales de los tribunales no son efectivas en este contexto[31] .

Es importante destacar que los litigios que surgen en el ámbito de la protección de datos deben ser resueltos por tribunales con base territorial. Sin embargo, los problemas principales que surgen están relacionados con la protección de datos en un entorno global, donde empresas con sedes en terceros países brindan servicios a ciudadanos de todo el mundo a través de Internet.

La clave reside en determinar qué normativa se aplica a las reclamaciones presentadas por los usuarios y qué tribunales son competentes para resolver dichas reclamaciones. Anteriormente, se solía utilizar como referencia el lugar donde la empresa tenía su centro de operaciones. Sin embargo, esta solución no es efectiva en la actualidad, ya que las empresas que operan en Internet pueden tener infraestructuras técnicas centralizadas en diferentes países y sus servidores pueden estar ubicados en lugares remotos o incluso secretos, lo que les permite prescindir de un establecimiento físico tradicional.

Es evidente que lograr una protección efectiva de los datos personales de los ciudadanos no puede depender únicamente de la ubicación del centro de medios técnicos de una

---

[30] BOE. *Artículo 5. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[31]CÓRDOBA CARTROVERDE D. *Los retos de la protección de datos en Internet. Caso Google Spain y Derecho al olvido. ANUARIO DE LA FACULTAD DE DERECHO DE LA UNIVERSIDAD AUTÓNOMA DE MADRID* [En línea]. [Consultado el 14 de junio de 2023];221–48. Disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-A-2017-10022100248

empresa. Aquí es donde surge el principal problema para garantizar una protección efectiva de los datos cuando se producen posibles violaciones en el ciberespacio. Además, muchas empresas emplean estratagemas para eludir la aplicación de la normativa europea o nacional, como eliminar establecimientos y recursos, e incluso cambiar el centro de gestión de recursos y ubicarlo en países con una normativa más permisiva.

Por lo tanto, el Reglamento aborda esta cuestión de manera sensata y eficaz al establecer un criterio de conexión más amplio y mejorado, reconociendo que la protección efectiva de los datos personales no puede depender únicamente de la ubicación física de los recursos técnicos de una empresa.

En su artículo 3.2 establece lo siguiente: El presente Reglamento 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 de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Este criterio de conexión es acertado y se ajusta a la realidad tecnológica y a los desafíos planteados por la ubicación de los medios y establecimientos en el tratamiento de datos personales.

El artículo 3.2 del RGPD resuelve el problema de la territorialidad al extender la aplicabilidad del Reglamento a los responsables que no están establecidos en la Unión Europea cuando las actividades de tratamiento de datos personales están relacionadas con la oferta de bienes y servicios a personas residentes en suelo europeo o que llevan a cabo su actividad en la Unión[32].

El derecho a la tutela judicial de la privacidad garantiza que cualquier persona interesada pueda presentar una reclamación ante la autoridad de control de cualquier

[32] BOE. *Artículo 3.2. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Estado miembro en el que resida, trabaje o donde se haya producido la presunta infracción.

Además, es importante mencionar la regulación establecida para el derecho a recurrir a los tribunales contra el responsable o encargado del tratamiento de datos. Este derecho puede ejercerse ante los órganos jurisdiccionales del Estado miembro donde el responsable o encargado tenga su establecimiento o donde la persona interesada tenga su residencia habitual. Existe una excepción a esta regla, que es cuando el responsable del tratamiento es una autoridad pública que actúa en el ejercicio de sus poderes, en cuyo caso se entiende que el recurso debe presentarse en el Estado miembro donde se encuentre dicha autoridad[33]

De esta manera, se pone fin a la diversidad de criterios entre diferentes tribunales en relación a cuestiones fundamentales, como la legitimidad de los actores involucrados, lo que soluciona los obstáculos para la acción de los poderes legislativo y judicial. Además, se pone fin a la práctica común de las corporaciones de Internet de establecer sus sedes en países con legislaciones permisivas que permiten la comercialización de información personal, ignorando las leyes nacionales y europeas en esta materia y dificultando el ejercicio efectivo de los derechos de los ciudadanos, quienes se encontraban en una situación de indefensión legal.

Por último, es importante hacer una breve mención al artículo 68 y siguientes del Reglamento General de Protección de Datos (RGPD), que se dedican al Comité Europeo de Protección de Datos (CEPD)[34].

---

[33] BOE. *Artículo 3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[34] BOE. *Artículo 68. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

El Comité Europeo de Protección de Datos (CEPD) es una entidad independiente a nivel europeo que garantiza la aplicación coherente de las regulaciones de protección de datos en toda la Unión Europea. Fue establecido en virtud del Reglamento General de Protección de Datos (RGPD). Su composición incluye representantes de las autoridades nacionales de protección de datos de los países de la UE/EEE, así como del Supervisor Europeo de Protección de Datos.

En las actividades y sesiones del Comité, la Comisión Europea participa sin derecho a voto. Las principales responsabilidades del CEPD son proporcionar orientación sobre los conceptos fundamentales del RGPD y la Directiva sobre protección de datos en el ámbito penal, asesorar a la Comisión Europea en asuntos relacionados con la protección de datos personales y futuras legislaciones propuestas en la Unión Europea, y tomar decisiones vinculantes en caso de conflictos entre las autoridades nacionales de control.

4.2 Nivel Nacional

El primer desarrollo legislativo que se realizó sobre el derecho fundamental a la protección de datos se llevó a cabo a través de Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Para su aprobación, se tuvo en cuenta el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981. Este Convenio supuso un hito en la regulación de la materia de protección de datos en el ámbito europeo y determinó la aprobación sucesiva de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, ya citada anteriormente en el epígrafe anterior. Estas normativas y, adicionalmente otras dos Directivas europeas, se incorporaron al Derecho nacional con la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que derogó la citada LO 5/1992.

La regulación anterior de 1999 ha sido reemplazada por el Reglamento General de Protección de Datos (RGPD) 2016/679, que entró en vigencia el 25 de mayo de 2018. En España, esta normativa se adecuó mediante la Ley Orgánica 3/2018, de 5 de

diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que se convierte en la ley vigente en nuestro país[35].

A principios de los años 90, los avances tecnológicos requerían una respuesta legal para abordar el vacío existente en la protección de datos. El Derecho no podía ignorar este nuevo fenómeno y, como resultado, surgieron las primeras iniciativas legislativas para establecer un sistema de garantías de los derechos y libertades de las personas. Estas iniciativas dieron lugar a las diferentes generaciones de leyes de protección de datos personales[36].

Para comprender el contexto histórico, es necesario retroceder en el tiempo hasta la Ley Orgánica 5/1992, de 29 de octubre, conocida como LORTAD (Ley Orgánica de tratamiento automatizado de los datos de carácter personal). Esta ley representó el final de un proceso de desarrollo doctrinal y normativo que se remonta a 1976. Además, con esta ley, el Reino de España cumplió con el compromiso adquirido al ratificar el Convenio 108 del Consejo de Europa cuyo artículo 4 obligaba a los Estados parte a dotarse de una ley interna de protección de datos dentro del plazo que el propio Convenio preveía para su entrada en vigor[37].

La implementación de esta Ley también se justificó por las demandas derivadas de los Acuerdos de Schengen de 1985, donde el artículo 117 establecía la obligación para los Estados miembros de contar con una legislación interna de protección de datos que cumpliera al menos con el nivel establecido en el Convenio 108 y la Recomendación

[35] BOE. *DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=SL

[36] LUÑO AEP. Derechos *humanos, estado de derecho y Constitución. Tecnos;*[En línea] [Consultado el 17 de junio de 2023] Disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=160138

[37] BOE. BOE-A-1985-23447 *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981* [En línea]. [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

(87) 15 del 17 de septiembre[38]. La LORTAD se complementó con dos regulaciones adicionales: el Real Decreto 1332/1994, del 20 de junio, que desarrolla ciertos aspectos de la Ley Orgánica 5/1992, del 29 de octubre, sobre el tratamiento automatizado de datos personales, y el Real Decreto 428/1993, del 26 de marzo, que aprueba el Estatuto de la Agencia de Protección de Datos. Además, en 1999 se promulgó otro Real Decreto para el desarrollo legislativo de la LO 5/1992, con el propósito de establecer medidas técnicas y organizativas para garantizar la seguridad de los archivos automatizados, los centros de tratamiento, los equipos, los sistemas, los programas y las personas involucradas en el tratamiento automatizado de datos personales.

La Exposición de Motivos de la Ley Orgánica 5/1992 revela la llegada de tecnologías completamente desconocidas hasta entonces. En su contenido, particularmente en el artículo 3, la Ley ofrece definiciones que nos permiten comprender el significado de los términos utilizados, los cuales aún utilizamos en la actualidad con diferencias sustanciales.

El objetivo de la Ley era regular el tratamiento automatizado de datos personales, y como se expresa en su artículo 1, buscaba limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de la información para salvaguardar los derechos de la personalidad. Sin embargo, el término "intimidad" se usaba siguiendo el concepto anglosajón de "privacy", no se refería a la intimidad de las personas, sino a la facultad de disponer de información personal o datos que revelen circunstancias o características de la persona. El núcleo del problema que la Ley intentaba resolver era la recopilación, acumulación y procesamiento informático de los datos de una persona.

La Ley establecía un sistema preventivo o cautelar para evitar que el uso descontrolado de los datos cause perjuicios a las personas, en lugar de reparar dichos perjuicios posteriormente. El objeto de protección se determinaba en base a los conceptos de datos personales, fichero y tratamiento.

[38] BOE. BOE-A-1985-23447 *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981* [En línea]. [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

Es importante destacar que el término "datos" se entendía como cualquier información relacionada con personas físicas identificadas o identificables, abarcando cualquier forma de información. Por lo tanto, la recopilación de imágenes y su procesamiento debían cumplir con los principios establecidos en la ley, siempre que fueran susceptibles de ser tratadas de forma informatizada[39].

En relación al principio de proporcionalidad, se refiere a que los datos recopilados deben ser adecuados, relevantes y no excesivos, y su obtención debe realizarse de manera lícita, sin fraudes ni acciones desleales. Por otro lado, el principio de transparencia se refiere a la necesidad de que se informe sobre la existencia de los archivos, sus propósitos y la identidad del responsable. Estos principios fueron inicialmente establecidos en las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[40].

Otro principio relevante es el de la veracidad y exactitud de la información personal. Es necesario que los datos sean precisos y estén actualizados para reflejar de manera veraz la situación actual del individuo afectado.

El consentimiento del individuo, regulado en el artículo 7, fue y sigue siendo un elemento fundamental en la protección de datos, que fue incorporado como principio en la LORTAD. La norma del consentimiento, como se estableció en el artículo 6, se aplicaba de manera general al tratamiento de datos, no solo a su recopilación. Sin embargo, el consentimiento era especialmente necesario cuando se trataba de datos sensibles o de naturaleza específica[41].

---

[39] *Ley LLORTADL, Heredero Higueras M. La L.O.R.T.A.D. y su fututo. La Ley Orgánica 5/1992, de de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/248235.pdf

[40] De D, SOBRE LO, et al. *ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf

[41] BOE. *BOE-A-1992-24189 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Entre todos los derechos y garantías que se establecen en el texto legal, el más importante y fundamental en el sistema de protección es el derecho de acceso, tanto en sentido amplio (artículo 13) como en sentido estricto (artículo 14), que implica el derecho a conocer la existencia de un archivo de datos personales y a tener acceso a esos datos. Este derecho es de gran relevancia en la actualidad, ya que es un requisito previo para ejercer los derechos de cancelación y rectificación, ambos regulados en el artículo 15.

Con la aprobación de esta Ley, también se establece en España el primer organismo encargado de la protección de datos personales: la Agencia Española de Protección de Datos. Los primeros indicios para su creación se encuentran en la Resolución del Parlamento Europeo de 1979 y, especialmente, en la primera propuesta de la Directiva comunitaria, que imponía a los Estados miembros la obligación de establecer una autoridad encargada de supervisar la aplicación de las disposiciones de transposición de la Directiva en su territorio. El objetivo era crear un organismo concreto y especializado capaz de controlar la implementación del sistema de protección establecido por la ley[42]. Como ya hemos apuntado en epígrafes anteriores, la labor principal de la Agencia se ha centrado en el control y vigilancia de los responsables de los archivos de datos, en lograr una notificación exhaustiva de los archivos existentes y en ejercer el poder sancionador. La Agencia se configura como una de las denominadas "Administraciones independientes" y se define como una entidad de derecho público que actúa con total independencia de las Administraciones Públicas en el desempeño de sus funciones.

Siete años después de la entrada en vigor de la LO 5/1992, esta ley fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que entró en vigor el 14 de enero de 2000. Esta nueva ley estableció un marco regulatorio destinado a lograr un equilibrio entre un alto nivel de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE), estableciendo límites estrictos para la recopilación y uso de datos personales.

[42] OFICIAL D. EUROPA EU. *Comunicaciones e informaciones*. [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2023:214:FULL

La LOPD introduce nuevas definiciones relacionadas con el responsable del archivo o tratamiento, el encargado del tratamiento, el consentimiento del interesado, la transferencia o comunicación de datos y las fuentes accesibles al público.

En cuanto a los principios de protección de datos, hay novedades para los casos en que se recopilan datos por parte de una persona distinta al interesado, ya que se obliga al responsable del archivo o su representante a informar al afectado de manera expresa, precisa e inequívoca, dentro de los tres meses siguientes al registro de sus datos, sobre el contenido del tratamiento y el origen de los datos. En cuanto al consentimiento, esta nueva ley establece que debe ser inequívoco, claro e indudable, y declara la invalidez del consentimiento del afectado si no ha sido informado previamente sobre la finalidad de dicha transferencia y el tipo de actividad realizada por el receptor de dichos datos.

También es importante destacar la obligación de regular, en un contrato por escrito, la realización de tratamientos en nombre de terceros, estableciendo expresamente que el encargado del tratamiento solo tratará los datos siguiendo las instrucciones del responsable y no los utilizará con un propósito diferente al establecido en dicho contrato, ni los comunicará a otras personas, incluso para su conservación, sin cumplir con las medidas de seguridad exigibles para el responsable del tratamiento.

En cuanto a los derechos de los afectados, la LOPD introduce dos innovaciones que benefician a las empresas responsables de los datos personales, ya que se amplía el plazo a diez días (anteriormente eran 5 días en la LORTAD) para ejercer los derechos de rectificación o cancelación solicitados por los afectados, y también se establece la obligación de conservar los datos personales durante los plazos establecidos en las disposiciones aplicables[43].

Por último, la LOPD estableció uno de los regímenes sancionadores más severos. A pesar de ello, se hace evidente la necesidad de una normativa más equilibrada en cuanto al monto de las multas, que se ajuste a la realidad actual. El régimen jurídico de protección de datos personales es muy complejo y requiere herramientas reglamentarias que especifiquen las disposiciones legislativas. El 6 de diciembre de 2018,

[43] ROCKETLAYWER *Derecho de rectificación y cancelación de datos personales* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.rocketlawyer.com/es/es/guia-rapida/derecho-rectificacion-cancelacion-datos-personales

conmemorando los 40 años de la Constitución de 1978, se publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Esta ley se deriva directamente del mencionado Reglamento (UE) 2016/679, conocido como el Reglamento General de Protección de Datos (RGPD), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas.

En cuanto al objetivo de la Ley, se pretendía adaptar nuestra legislación al RGPD y regular el derecho fundamental a la protección de datos, además de ser una norma más flexible y adaptada a la realidad actual, desarrollando y ajustando en lo necesario el Derecho español al RGPD.

Una de las novedades introducidas por esta Ley es el concepto de "testamento digital" aplicado a las personas fallecidas (artículo 3). Esto permite que las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, puedan solicitar el acceso, rectificación o eliminación de los datos personales del fallecido, a menos que el fallecido lo haya prohibido expresamente, aunque dicha prohibición no se aplica a los datos de carácter patrimonial.

En cuanto a los principios de protección de datos, la LOPDGDD mantiene la edad de 14 años, que ya estaba establecida en la normativa nacional, como la edad a partir de la cual el tratamiento de los datos personales de un menor de edad puede basarse en su consentimiento.

En relación a los derechos de las personas, se incluye una nueva modalidad denominada "información por capas"[44].

Además, se establecen regulaciones sobre ciertos aspectos del ejercicio de los derechos, especialmente el derecho de acceso, pero no se incorporan regulaciones adicionales para los demás derechos. Sin embargo, se brinda una explicación más detallada sobre el tratamiento de cierta información y el tratamiento de información con fines públicos.

Es importante destacar la introducción de una figura completamente nueva en comparación con la regulación anterior, que es la del delegado de protección de datos

[44] ALONSO N. *La información por capas en el RGPD* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/informacion-por-capas-rgpd/

(DPD), regulado en los artículos 34 y siguientes de esta ley. El DPD tiene la responsabilidad de resolver conflictos en materia de protección de datos.

Una de las principales novedades es el reconocimiento de una serie de derechos digitales para los ciudadanos. Entre estos, se encuentran el derecho a la neutralidad de Internet (artículo 80), el derecho al acceso universal a Internet (artículo 81), el derecho a la seguridad y educación digital (artículos 82 y 83), la protección de los menores en Internet (artículo 84), el derecho de rectificación en Internet (artículo 85), el derecho a la actualización de información en medios de comunicación digitales (artículo 86) y el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (artículo 87), entre otros. Esto demuestra que se trata de una normativa mucho más moderna y adaptada a la sociedad actual.

Por último, es importante mencionar los derechos ARCO, que son de gran importancia, como se evidencia en las sentencias 290/2000 y 292/2000, en las que se define el derecho fundamental a la protección de datos[45].

Estos derechos ARCO son el derechos de acceso, rectificación, cancelación y oposición, que permiten conocer qué información personal nuestra está siendo tratada por un responsable, de quién o de dónde han obtenido esos datos y a quién se los ha cedido. A su vez, permiten modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos a tratamientos de datos realizados sin nuestro consentimiento[46].

Se encuentran regulados tanto en la Ley Orgánica 15/1999 de protección de datos de carácter personal, como en el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de dicha ley, y también en el Reglamento (UE) 2016/679.

---

[45]BOE. *BOE-T-2001-332 Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

[46] AGPD. *Agencia Española de Protección de Datos* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-ides-idphp.php

El derecho de acceso otorga a los individuos la capacidad de controlar de forma individual si sus datos han sido tratados, así como conocer el origen y las comunicaciones realizadas con respecto a ellos. Es decir, tienen el derecho de acceder a información específica o a la totalidad de los datos sometidos a tratamiento, tal como se establece en el artículo 27.2 [47].

El derecho de rectificación y cancelación permite modificar los datos que sean incompletos o inexactos, o en su caso, eliminar aquellos datos personales que sean inadecuados o excesivos, según se establece en el artículo 16.

En relación al principio de finalidad, se establece que una vez que los datos personales dejan de ser utilizados para los fines con los que fueron recopilados y ya no existe justificación para su tratamiento, deben ser anonimizados o eliminados. Sin embargo, es importante destacar que esta eliminación no ocurre de manera inmediata. En su lugar, los datos personales se bloquean y se conservan únicamente para ser utilizados por las Administraciones Públicas, Jueces y Tribunales en caso de posibles responsabilidades derivadas del tratamiento, durante el plazo de prescripción correspondiente. Una vez que este plazo ha transcurrido, se debe proceder a la eliminación de los datos[48].

El derecho de supresión, también conocido como derecho al olvido, está incluido en el nuevo Reglamento (UE) 2016/679, como ya se explicó anteriormente. Este derecho permite a una persona solicitar que se eliminen sus datos personales de un fichero.

El último de los derechos ARCO es el derecho a la oposición, que consiste en la facultad que tiene un individuo de comunicar al responsable del fichero que desea que se detenga el tratamiento de sus datos.

---

[47] BOE. *BOE-T-2001-332 Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

[48] RAMÍREZ H. *¿Cómo eliminar datos de empresas aplicando la LOPD?* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/eliminar-datos/

En cuanto a las características, los cuatro derechos comparten las mismas características. Son derechos personalísimos que solo pueden ser ejercidos por el titular de los datos. Además, son derechos independientes entre sí, lo que significa que no es necesario ejercer uno antes de poder ejercer otro. Por último, estos derechos deben ser reclamados ante el responsable que esté tratando los datos, siendo la Agencia Española de Protección de Datos un recurso subsidiario en caso de que las solicitudes del individuo no sean atendidas.

En cuanto a los plazos, cada uno de estos derechos tiene un plazo máximo diferente. El derecho de acceso tiene un plazo máximo de 1 mes, mientras que los derechos de rectificación, cancelación y oposición tienen un plazo máximo de 10 días.

4.3 Regulación en la Constitución Española.

En todo lo relativo a la protección de datos, la Constitución Española (CE) de 1978 en su artículo 18.1 establece que: *"se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen",* así en el apartado cuarto del mismo artículo señala que: *"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"*[49].

El Tribunal Constitucional en la Sentencia del Tribunal Constitucional (STC) 134/1999, de 15 de julio, llevo a cabo un pronunciamiento en el que señalaba que: *"lo que el artículo 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio"*[50].

[49] BOE. *BOE-A-1978-31229 Constitución Española* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

[50] BOE. *Sumario del día 18/08/1999* [En línea]. [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/1999/08/18/

Debemos plantearnos que sucede con la noción de “intimidad en público”[51] porqué el alcance del derecho a la intimidad no se limita únicamente al ámbito privado. La STC 12/2012 de 30 de enero de 2012, se menciona la presencia de un "círculo íntimo" en el cual el individuo puede llevar su vida personal de acuerdo a su propia forma y excluir completamente al mundo exterior que desea mantener alejado de dicho círculo. También se hace alusión a la expectativa razonable de privacidad, es decir, la posibilidad de que los demás no violen nuestra intimidad, expresada en evitar acciones como escucharnos u observarnos[52]. Al pertenecer el derecho al honor a los derechos de la personalidad y tratarse de un concepto jurídicamente indeterminado, el Tribunal Constitucional en la STC 223/1992 señaló que el alcance y contenido del derecho al honor son variables y están sujetos a cambios constantes, siendo en definitiva: *"dependiente de las normas, valores e ideas sociales vigentes en cada momento"*[53]. La doctrina ha decidido diferenciar entre el significado objetivo del concepto de honor, que se refiere a la reputación de una persona o la evaluación que otros hacen de ella; y el sentido subjetivo, que se refiere a la valoración que cada individuo hace de sí mismo.

En cuanto al derecho a la propia imagen, la STC 117/1994, de 25 de abril: “*garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona”*[54]. Respecto a lo contenido en el artículo 18.4 de la Constitución Española (CE), se encuentra desarrollado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

---

51 JAVIRED. Derecho A La Intimidad Y La Protección De Datos Personales [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://mundojuridico.net/derecho-a-la-intimidad-y-la-proteccion-de-datos-personales/

52 CCCLII A. *BOLETÍN OFICIAL DEL ESTADO* [En línea]. [Consultado el 11de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/2012/02/24/pdfs/BOE-S-2012-47.pdf

53SISTEMA HJ. *Resolución: SENTENCIA 223/1992* [En línea] [Consultado el 11 de junio de 2023]. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2110

54 BOE. *Sumario 129 Martes 31 mayo 1994 17011* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/1994/05/31/pdfs/A17011-17011.pdf

El derecho del artículo 18.4 CE ha sido perfilado por el Tribunal Constitucional en la sentencia 292/2000, de 30 de noviembre, relatando que: *"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"*[55]. Por primera vez se refiere a un derecho a la autodeterminación informativa en virtud del artículo 18.4 CE y se declara inconstitucional una parte de los artículos 21.1, como el 24.1 y 24.2 de la LO 15/1999. Estos actos violaban el derecho a la intimidad al permitir que se compartieran datos personales entre las administraciones públicas para fines distintos a los de su recopilación inicial.

Con el derecho a la autodeterminación informativa al titular se le asigna: *"un conjunto de poderes jurídicos cuyo ejercicio se impone como deberes ante terceros con un carácter instrumental ya que pretende garantizar a los ciudadanos el pleno ejercicio de sus derechos, todos ellos"*[56]. Tanto el derecho al honor, intimidad y propia imagen como el derecho a la protección de datos del artículo 18 CE, tienen por objeto: *"ofrecer una eficaz protección constitucional de la vida privada personal y familiar".* El Tribunal Constitucional afirma que las funciones de los dos artículos difieren de manera significativa, la finalidad del artículo 18.1 CE es: *"proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad"* (STC 144/1999, de 22 de julio). Por otro lado, el derecho fundamental a la protección de datos es: "*garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. El derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno"* (STC

[55] BOE. *Sumario del día 04/01/2001* [En línea] [Consultado el 17 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/2001/01/04/

[56] UNED. *Vista de La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/15140/13298

292/2000) siendo este derecho más abarcador, se extiende a todos los tipos de información de carácter personal.

4.4 Regulación en el ámbito penal.

En el contexto con el derecho penal, se debe hacer una referencia al delito tipificado en el artículo 197.2 del código penal como delito contra la libertad informática o "habeas data"; este delito establece que se castigará a aquella persona que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro usuario que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. De igual manera, se impondrá la misma pena a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular usuario de los datos o de un tercero.

Este delito afecta directamente al derecho de intimidad y privacidad de los usuarios, entendiendo que engloba toda información personas que se encuentre en programas informáticos, electrónicos o telemáticos. Estos tratos de carácter reservado pertenecen al usuario titular, pero no se encuentran en su ámbito de protección directo. Esos datos se encuentran en archivos o bases de datos cuya custodia aparece especialmente protegida en orden a la autorización de su inclusión, supresión, fijación de plazos, cesión de información, etc, de acuerdo a la legislación de protección de datos, delimitando claramente la titularidad y manejo y cesión de la información contenida de los mismos.

Las conductas expuestas anteriormente en el artículo mencionado, afectan a datos que no tienen posesión por el usuario titular, sino que se encuentran a libre disposición, en banco de datos; estos datos pueden causar perjuicios a terceros.

A tenor de lo anteriormente expuesto en dicho artículo 197 del código penal, existe una doctrina que se decanta más sobre la protección de la intimidad del sujeto pasivo, mientras que otra parte de la doctrina se decanta por la integridad de los datos.

Conclusiones

En base a lo descrito anteriormente, se han podido extraer ciertas conclusiones. En primer lugar, la huella digital de un dispositivo es utilizada para recopilar información sistemática sobre un dispositivo remoto específico con el propósito de identificarlo y realizar un seguimiento de la actividad del usuario. Mientras que las cookies, tradicionalmente fueron el método principal utilizado para obtener esta información, se han desarrollado técnicas más avanzadas de seguimiento que las han superado. Estas nuevas técnicas se basan en la recopilación de datos específicos del navegador web y/o dispositivo de navegación para crear un identificador único para cada usuario. Sin embargo, la legitimidad de estas técnicas no está claramente establecida.

A diferencia de las cookies, que son reconocidas y aceptadas por el servidor web y pueden ser eliminadas para eliminar el vínculo entre el dispositivo y la información recopilada, el uso de la huella digital permite volver a asignar la información asociada a un identificador de cookie eliminado, lo que evita perder la trazabilidad de los datos de navegación o seguimiento del usuario.

El uso intensivo de las huellas digitales dejadas por los usuarios en Internet está impulsado por el intercambio económico relacionado con Internet. Su uso puede suponer una pérdida de privacidad y anonimato en línea, lo cual atenta contra el valor social de Internet y puede afectar la confianza de los usuarios. Aunque existen riesgos asociados al intercambio de información entre terceros sin consideración por la privacidad del consumidor, también se reconoce que las huellas digitales pueden tener usos legítimos, como parte de mecanismos de autenticación de múltiples factores. Se recomienda adoptar hábitos y conocimientos básicos, como tener cuidado con la información personal compartida, utilizar herramientas de configuración y privacidad en navegadores y dispositivos, y considerar el uso de una red privada virtual (VPN).

A pesar de estas medidas, se reconoce que algunos datos quedan grabados por la huella digital, por lo que es importante seguir revisando y ajustando la configuración de privacidad y buscar herramientas y motivación para tomar decisiones más informadas.

Por otro lado, la protección de datos personales es un derecho fundamental que permite a las personas tener el control sobre el tratamiento de su información, tanto en formatos manuales como automatizados, y en relación con su vida privada. Este derecho está

respaldado por el derecho a la privacidad y al respeto de la confidencialidad de las comunicaciones, y está reconocido constitucionalmente en algunos países y a través de leyes específicas en otros.

No debemos olvidarnos del consentimiento del individuo, el cuál es un elemento clave en el tratamiento de datos personales. Debe ser previo, expreso, informado, inequívoco y verificable, y constituye la base legal para el tratamiento de los datos, a menos que exista una habilitación legal específica para el tratamiento sin consentimiento.

Como foco de concentración, nos centramos en el derecho de supresión, también conocido como derecho al olvido, es un derecho fundamental establecido en la legislación europea de protección de datos. Permite a las personas solicitar la eliminación de su información personal en situaciones específicas, como cuando los datos son desactualizados, no deseados o incorrectos. Para ejercer el derecho de supresión, es necesario cumplir ciertos requisitos, como el cese de la necesidad de los datos, la retirada del consentimiento, la oposición justificada al tratamiento, la no utilización de los datos para marketing directo, la consideración de tratamiento ilegal o el cumplimiento de una obligación legal.

El derecho de supresión se fundamenta en el derecho a la protección de datos y en el control y disposición que los usuarios deben tener sobre sus datos personales. Esto implica conocer quién posee los datos, con qué propósito se utilizan y tener la facultad de oponerse a su posesión y uso.

El Tribunal de Justicia de la Unión Europea respaldó el derecho al olvido en un fallo que afectó a los motores de búsqueda como Google. Estos motores deben eliminar enlaces a información perjudicial que ya no sea pertinente para el usuario. Google ha estado trabajando para cumplir con esta sentencia, evaluando cada solicitud individualmente.

Por último, no debemos olvidarnos de dos derechos que van muy estrechamente anexionados con el derecho al olvido, el derecho de información y el derecho a la intimida y privacidad.

El derecho de información es otro derecho fundamental establecido en la legislación europea de protección de datos. Obliga al responsable del tratamiento de datos a proporcionar información básica y adicional al recopilar datos personales del usuario.

El derecho a la intimidad y privacidad son derechos fundamentales e imprescindibles de la persona. Estos derechos se ven amenazados por el avance tecnológico y los medios de comunicación, y su alcance debe determinarse en base a la jurisprudencia y las circunstancias de cada caso.

En resumen, el derecho de supresión o derecho al olvido, junto con el derecho de información y el derecho a la intimidad y privacidad, son aspectos fundamentales en la protección de datos y la garantía de los derechos individuales en el ámbito digital.

En lo que respecta al tratamiento jurídico de la huella digital, es importante determinar cuándo existe interés en que determinados datos personales sean mantenidos o tratados en el tiempo. Para ello, se debe tener en cuenta el factor tiempo y se debe ponderar la permanencia de ese interés en el tiempo para evaluar si se ha lesionado o no el derecho a la protección de datos personales.

Resulta de trascendental importancia el nuevo tratamiento jurídico que se está dando en torno al derecho de protección de datos ya que la normativa debe adaptarse a los nuevos tiempos en el que el uso de la tecnología es cada día mayor. A tenor de esto, con la aprobación de la Directiva 95/46/CE, se creó el Reglamento General de Protección de Datos (RGPD).

Resaltar, que la principal misión de este Reglamento es instaurar una regulación más uniforme y sólida en toda la Unión Europea en un intento de superar los nuevos obstáculos generados a causa de las nuevas tecnologías. El enfoque central de este Reglamento ha sido el consumidor y su protección en caso de violación del derecho a la protección de datos.

Es de destacar la inclusión del derecho al olvido en el Reglamento, permitiendo a los afectados pedir la eliminación de sus datos personales en determinadas circunstancias cuando pueda afectar a su intimidad o al libre desarrollo de sus derechos fundamentales.

Otra conclusión que podemos sacar de la redacción del nuevo Reglamento es que se ha acabado el problema relacionado con la territorialidad gracias a su nueva regulación, al extender la aplicabilidad del Reglamento a los responsables que no están establecidos en la Unión Europea cuando las actividades de tratamiento de datos personales están relacionadas con la oferta de bienes y servicios a personas residentes en suelo europeo o que llevan a cabo su actividad en la Unión.

En lo que a regulación nacional se refiere, debemos destacar el hecho de la implantación de la nueva ley con el objetivo de dar una respuesta legal al vacío existente en la protección de datos con motivo de los avances tecnológicos para establecer un sistema de garantías de los derechos y libertades de las personas. Fruto de todo ello se creó la Agencia Española de Protección de Datos para el control y vigilancia de los responsables de los archivos de datos.

Destacar que nuestra actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) deriva de forma directa del Reglamento (UE) 2016/679, de ahí la gran importancia de dicho reglamento, ya que nuestra ley pretendía adaptar nuestra legislación a dicho reglamento.

De igual modo, no podemos olvidarnos de los derechos ARCO, que han permitido conocer qué información personal nuestra, está siendo tratada por un responsable, de quién o de dónde han obtenido esos datos y a quién se los ha cedido.

Por último, y a modo de conclusión, el tema de la protección de datos es muy amplio y necesita de un estudio detallado de cada caso para que su tratamiento se lleve a cabo de la forma más correcta y menos perjudicial para el individuo. Los avances tecnológicos nos están sobrepasando hoy en día y prueba de ello es, que son el principal motor de desarrollo legislativo de la materia por la velocidad a la que se están produciendo dichos avances. A mi modo de ver, siempre iremos por detrás de la evolución tecnológica en lo que a protección jurídica se refiere.

Bibliografía

1. AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Estudio: Fingerprinting o Huella digital del dispositivo* [En línea]. Aepd.es. 2019 [Consultado el 4 de junio de 2023]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

2. BUA. BIBLIOTECA DE LA UIVERSIDAD DE ALICANTE. *La Huella Digital* [En línea]. Rua.ua.es. [Consultado el 6 de junio de 2023]. Disponible en: https://rua.ua.es/dspace/bitstream/10045/79601/1/CI2_intermedio_2017-18_Huella-digital.pdf

3. INCIBE. *Como Evitar Que La Huella Digital Afecte Nuestras Empresas* [En línea]. Incibe.es. 2023 [Consultado el 17 de junio de 2023]. Disponible en: https://www.incibe.es/empresas/blog/como-evitar-que-la-huella-digital-afecte-nuestras-empresas

4. GUAMANZARA TORRES LH. RIOFRÍO, J.C. *El derecho de los secretos.* Bogotá: Temis. Ius Hum Law J [En línea]. 2011 [Consultado el 7 de junio de 2023];2(2):249–51. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4999992

5. MINISTERIO DE TRANSPORTES M Y AU. *Protección de datos personales* [En línea]. Gob.es. [Consultado el 7 de junio de 2023]. Disponible en: https://www.mitma.gob.es/el-ministerio/buen-gobierno/proteccion-datos-personales

6. GÓMEZ-CÓRDOBA AI, ARÉVALO-LEAL S, BERNAL-CAMARGO DR, ROSERO DE LOS RÍOS D. *El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia.* Rev Bioet Derecho [En línea]. 2020 [Consultado el 11 de junio de 2023];(50):271–94. Disponible en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017

7. EDPB. *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* [En línea]. Europa.eu. 2020 [Consultado el 11 de junio de 2023].

Disponible en:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

8. AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Principios del Reglamento General de Protección de Datos* [En línea]. AEPD. 2022 [Consultado el 17 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

9. AEPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Derecho de supresión ("al olvido")* [En línea]. Aepd.es. 2019 [Consultado el 15 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido

10. RAE. *Diccionario Real Academia Española* (RAE) [En línea]. Rae.es. [Consultado el 15 de junio de 2023]. Disponible en: https://dpej.rae.es/lema/derecho-al-olvido-o-derecho-de-supresi%C3%B3n#:~:text=Derecho%20a%20eliminar%2C%20ocultar%20y,2.

11. FERNÁNDEZ JPM. *La protección de datos y los motores de búsqueda en Internet: Cuestiones actuales y perspectivas de futuro acerca del derecho al olvido / Data protection and Internet search engines: current issues and future perspectives about the right to be forgotten.* Rev Derecho Civ [En línea]. 2017 [Consultado el 17 de junio de 2023];4(4):181–209. Disponible en: https://www.nreg.es/ojs/index.php/RDC/article/view/280

12. SENTENCIA DEL TRIBUNAL CONSITUCIONAL DE 30 NOVIEMBRE DEL 2000 [RTC\2000\290]. *La aplicación judicial del derecho comunitario ne España durante 2000 Y 2001* [En línea]. Unirioja.es. [Consultado el 7 de junio de 2023]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/266015.pdf

13. DE LA CUEVA CONZÁLEZ-COTERA J. *Relato del VII Congreso Internacional sobre Internet, Derecho y Política: neutralidad de la red y derecho al olvido. IDP Rev Internet Derecho Política* [En línea]. 2012 [Consultado el 11 de junio de 2023];(13):84–90. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3865410

14. LÓPEZ PORTAS MB. *La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE.* Rev derecho político [En línea]. 2015 [Consultado el 17 de junio de 2023];1(93):143–75. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5169233

15. GOOGLE. *Preguntas frecuentes – Privacidad y Condiciones – Google* [En línea]. Google.com. [Consultado el 15 de junio de 2023]. Disponible en: https://policies.google.com/faq?hl=es

16. INFOCURIA JURISPRUDENCIA I. *Sentencia del Tribunal de Justicia.* [En línea]. Europa.eu. 2014 [Consultado el 15 de junio de 2023]. Disponible en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&amp pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=276332

17. AEPD. *Derecho de información* [En línea]. Aepd.es. 2022 [Consultado el 15 de junio de 2023]. Disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-informacion

18. URQUIAGA EP. *Los Derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información.* [En línea]. Redalyc.org. 2000 [Consultado el 17 de junio de 2023]. Disponible en: https://www.redalyc.org/pdf/197/19760123.pdf

19. RAÚL FERNÁNDEZ J. *Los principios relativos al tratamiento de datos personales en el RGPD - J. Raul Fernández. Abogado* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.jraulfernandez.es/los-principios-relativos-al-tratamiento-de-datos-en-el-rgpd/

20. GRUPO ATICO 34. *Plazo de Conservación datos personales Rgpd* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/conservacion-datos-plazo/

21. MORENO BOBADILLA A. *Los derechos digitales en Europa tras la entrada en vigor del Reglamento de Protección de Datos Personales: Un antes y un después para el derecho al olvido digital. Estud Const (Impresa)* [En línea] [Consultado el 24 de junio de 2023];18(2):121–50. Disponible en:

https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002020000200121

22. *Legado: Grupo de Trabajo del art. 29* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://edpb.europa.eu/about-edpb/more-about-edpb/legacy-art-29-working-party_es

23. Inglés MCC. *El "derecho al olvido digital". Una exigencia de las nuevas tecnologías, recogida en el futuro reglamento general de protección de datos. Actualidad jurídica iberoamericana* [En línea] [Consultado el 4 de junio de 2023];(5):255–71. Disponible en: http://dialnet.unirioja.es/servlet/articulo?codigo=5723770

24. BOE-T-2001-332 Pleno. *Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica* [En línea] [Consultado el 12 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

25. MESA AR *Big Data: La evolución de los datos* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://openwebinars.net/blog/big-data-la-evolucion-de-los-datos/

26. BOE. *Reglamento n V, del Consejo 1234/2007, De octubre de de 22, De mercados agrícolas y se establecen disposiciones específicas para determinados Productos Agrícolas*. [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/doue/2012/012/L00014-00021.pdf

27. BOE. *Artículo 7. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

28. SANCHO LÓPEZ, M. *GARANTÍAS LEGALES DEL CONCEPTO DE PRIVACIDAD: ENTRE EL DERECHO AL OLVIDO Y EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS [En LÍNEA]* [Consultado el 24 de junio de 2023]. Disponible en: https://revista-aji.com/articulos/2018/9/176-201.pdf

29. BOE. *Artículo 8. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

30. BOE. *Artículo 5. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

31. CÓRDOBA CARTROVERDE D. *Los retos de la protección de datos en Internet. Caso Google Spain y Derecho al olvido. ANUARIO DE LA FACULTAD DE DERECHO DE LA UNIVERSIDAD AUTÓNOMA DE MADRID* [En línea]. [Consultado el 14 de junio de 2023];221–48. Disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-A-2017-10022100248

32. BOE. *Artículo 3.2. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de

junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

33. BOE. *Artículo 3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

34. BOE. *Artículo 68. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

35. BOE. *DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=SL

36. LUÑO AEP. Derechos *humanos, estado de derecho y Constitución. Tecnos;*[En línea] [Consultado el 17 de junio de 2023] Disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=160138

37. BOE. BOE-A-1985-23447 *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981* [En línea]. [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

38. BOE. BOE-A-1985-23447 *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en*

Estrasburgo el 28 de enero de 1981 [En línea]. [Consultado el 14 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

39. *Ley LLORTADL, Heredero Higueras M. La L.O.R.T.A.D. y su fututo. La Ley Orgánica 5/1992, de de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/248235.pdf

40. De D, SOBRE LO, et al. *ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf

41. BOE. *BOE-A-1992-24189 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

42. OFICIAL D. EUROPA EU. *Comunicaciones e informaciones*. [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2023:214:FULL

43. ROCKETLAYWER *Derecho de rectificación y cancelación de datos personales* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.rocketlawyer.com/es/es/guia-rapida/derecho-rectificacion-cancelacion-datos-personales

44. ALONSO N. *La información por capas en el RGPD* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/informacion-por-capas-rgpd/

45. BOE. *BOE-T-2001-332 Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de*

varios preceptos de la Ley Orgánica [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

46. AGPD. *Agencia Española de Protección de Datos* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/ejercicio_derechos/index-ides-idphp.php

47. BOE. *BOE-T-2001-332 Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

48. RAMÍREZ H. *¿Cómo eliminar datos de empresas aplicando la LOPD?* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/eliminar-datos/

49. BOE. *BOE-A-1978-31229 Constitución Española* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

50. BOE. *Sumario del día 18/08/1999* [En línea]. [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/1999/08/18/

51. JAVIRED. Derecho A La Intimidad Y La Protección De Datos Personales [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://mundojuridico.net/derecho-a-la-intimidad-y-la-proteccion-de-datos-personales/

52. CCCLII A. *BOLETÍN OFICIAL DEL ESTADO* [En línea]. [Consultado el 11de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/2012/02/24/pdfs/BOE-S-2012-47.pdf

53. SISTEMA HJ. *Resolución: SENTENCIA 223/1992* [En línea] [Consultado el 11 de junio de 2023]. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2110

54. BOE. *Sumario 129 Martes 31 mayo 1994 17011* [En línea] [Consultado el 24 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/1994/05/31/pdfs/A17011-17011.pdf

55. BOE. *Sumario del día 04/01/2001* [En línea] [Consultado el 17 de junio de 2023]. Disponible en: https://www.boe.es/boe/dias/2001/01/04/

56. UNED. *Vista de La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE* [En línea] [Consultado el 14 de junio de 2023]. Disponible en: https://revistas.uned.es/index.php/derechopolitico/article/view/15140/13298

Anexos

ANEXO 1: FORMULARIO DE SOLICITUD DE DERECHO DE ELIMINACIÓN (PDF)

EJERCICIO DEL DERECHO DE SUPRESIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ....., Comunidad Autónoma ..... con D.N.I....., con correo electrónico.....por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada.

Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta supresión.

Se recomienda que acompañe al presente formulario un escrito en el que exponga de manera detallada todos los datos que permitan identificar el objeto de su pretensión.

En .....a.....de.....de 20.....

Firmado:

INSTRUCCIONES

1. Este modelo se utilizará por el afectado cuando desee la supresión de los datos cuando concurra alguno de los supuestos contemplados en el Reglamento General de Protección de Datos. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida.
No obstante, se prevén ciertas excepciones en las que no procederá acceder a este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.

2. El solicitante deberá estar suficientemente identificado en la solicitud, que habrá de estar firmada. Si la solicitud la formula un tercero, deberá acreditarse oportunamente la representación otorgada para ello. Debe saber que, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar su identidad.

3. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

4. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

5. Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de supresión, resulta necesario que el responsable no haya hecho efectivo el derecho, y aporte alguno de los siguientes documentos:

- la negativa del responsable del tratamiento a la supresión de los datos solicitados.
- copia sellada por el responsable del tratamiento del modelo de petición de supresión.
- copia del modelo de solicitud de supresión sellada por la oficina de correos o copia del resguardo del envío por correo certificado.
- cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.