TESIS

Universidad de Jaén

Escuela de Doctorado

PROTECCIÓN DE DATOS PERSONALES Y SU PROYECCIÓN EN ÁREAS DE CONVERGENCIA CON OTROS DERECHOS FUNDAMENTALES

Autor: Carolina López Medina

Directores de la tesis: Gerardo Ruiz-Rico Ruiz y Joaquín Delgado Martín
Departamento: Derecho Público. Derecho Constitucional

Fecha: 10/04/2024

PROTECCIÓN DE DATOS PERSONALES Y SU PROYECCIÓN EN ÁREAS DE CONVERGENCIA CON OTROS DERECHOS FUNDAMENTALES

"(…) Es fundamental que el desarrollo de las nuevas tecnologías se rija por valores y principios democráticos (…). Nada puede haber más importante que la defensa de los derechos fundamentales de nuestros ciudadanos, en Europa y en cualquier otra región del mundo, en la actualidad y para las generaciones venideras. (…)".

S.M. Rey Felipe IV de España, en la 40ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad. Bruselas, 2018.

Publicaciones

La presente Tesis Doctoral por Compendio de Publicaciones se sustenta en un total de cuatro publicaciones de conformidad con el artículo 25.2 del Reglamento de los Estudios de Doctorado de la Universidad de Jaén[1]. En particular, se compone por dos artículos publicados en revistas en formato digital y por dos capítulos de libro publicados en editoriales de reconocido prestigio en el ámbito jurídico y de alto impacto a nivel nacional e internacional. A continuación, se relacionan las citadas publicaciones que conforman el Compendio de la Tesis:

- López Medina, C., "Aproximación a los nuevos derechos y garantías digitales reconocidos en la LOPDGDD 3/2018", en *Revista Asuntos Constitucionales, número monográfico. Retos Actuales del Derecho Constitucional.* Centro de Estudios Sociales y Jurídicos Sur de Europa (CESJ), núm. 0, 2021, págs.141-150. Recuperado de: https://www.asuntosconstitucionales.com/pdf/0-CLopez.pdf.

- López Medina, C., "Protección de datos personales en la Administración de Justicia española. Protocolo de Comunicación de la Justicia 2018", en *Revista Internacional Online Derecho de la Comunicación de la Universidad Complutense de Madrid (Derecom),* núm. 26, 2019, págs. 115-130. Recuperado de: http://www.derecom.com/secciones/articulos-de-fondo/item/374-personal-data-protection-in-the-spanish-judiciary-the-2018-protocol-on-the-judiciary-communications.

- López Medina, C., "El derecho fundamental a la protección de datos personales en el ámbito penal", en Ruiz Rico-Ruiz, G.; Pomares Cintas, E.; Revenga Sánchez, M.; Vergara Galaz, D. (coords.), *Derecho Penal y Garantías Constitucionales. Una perspectiva iberoamericana*, Tirant lo Blanch. Valencia, 2020, págs.113-133.

[1]Disponible en el siguiente enlace: https://www.ujaen.es/departamentos/psicol/sites/departamento_psicol/files/uploads/node_seccion_de_micrositio/2020-03/Reglamento%20doctorado%202019.pdf.

- López Medina, C., “Protección de datos personales en el sector sanitario, en el contexto del derecho a la salud y de la digitalización impulsada por la pandemia Covid-19”, en *La Protección de los derechos humanos por las defensorías del pueblo en situaciones de emergencia constitucional*, Tirant Lo Blanch, aceptada y pendiente de publicación en el año 2024.

Agradecimientos

A la Universidad de Jaén, donde comenzó mi camino universitario formando parte de la primera generación de Grado en Derecho en el año académico 2009/2010-2014, por abrirme sus puertas y hacer este sueño posible.

A mis codirectores de tesis, Joaquín Delgado Martín y Gerardo Ruiz Rico-Ruiz. Su impulso, confianza, orientación, sabiduría y guía en el proceso de elaboración de la Tesis han sido esenciales para que llegue a su fin.

A mi querida familia y mi marido, a quienes dedico todos mis éxitos por todo su apoyo, amor e inspiración.

A mí, por mi trabajo constante, duro y con gran ilusión por perseguir mis retos y sueños.

A todas las personas maravillosas que me han acompañado y apoyado desde el inicio de mi formación jurídica y durante todas las etapas que se han sucedido hasta la presentación de este proyecto investigador en torno al derecho fundamental a la protección de datos, que comenzó en el año 2018 y con el que opto al título de Doctor en Derecho.

"Forja una vida libre de miedos, abierta a la aventura"

(Santandreu Lorite)

A lo que me gustaría añadir: eso sí, controla y protege al máximo tu información y tus datos de carácter personal y tu privacidad, pues su valor es incalculable y pudiendo ser irreparables los perjuicios derivados de su vulneración, ya sea de forma voluntaria como involuntaria.

Índice

Introducción y justificación

Introducción y justificación

En las últimas décadas, y especialmente a partir de la entrada en vigor y aplicación hace casi seis años, el pasado 25 de mayo del año 2018, de la vigente normativa europea sobre protección de datos personales relativos a la persona física, el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (RGPD, en adelante), resulta notoria la evolución y el desarrollo que se ha producido en torno al derecho a la protección de datos y a la privacidad. Ello, junto al aumento de la preocupación, la cultura y la conciencia social sobre la importancia de proteger la intimidad, la privacidad y los datos personales de las personas en todos los ámbitos y a todos los niveles.

En la actualidad, nos encontramos en un mundo en el que el derecho a la protección de datos parece estar más presente que nunca. Sin embargo, fruto de los avances de la digitalización y las herramientas tecnológicas (entre las que destacan los avances de la Inteligencia Artificial o "IA"), la realidad demuestra que se siguen generando grandes retos y desafíos para la tutela de los derechos fundamentales, y en particular, de los derechos a la intimidad y a la protección de datos, así como en el ámbito de la seguridad de la información y la ciberseguridad[2]. Aunque los avances de la globalización y de la digitalización - especialmente en el marco de las denominadas sociedades tecnológicas y en desarrollo[3] - van de forma inevitable por delante de la normativa y de las regulaciones vigentes en cada momento, la tendencia actual a que continúen sin cesar los citados retos y desafíos.

[2] La seguridad de la información es entendida como la adopción de medidas que preservan la confidencialidad, integridad y disponibilidad de los datos que se manejan en la vida cotidiana, así como de los sistemas implicados en su tratamiento.

[3] "Informe sobre Medición de la Sociedad de la Información", *Resumen ejecutivo elaborado por la Unión Internacional de Telecomunicaciones*, Ginebra, 2018, págs. 2-3. Recuperado de: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-S.pdf (fecha de consulta: 2018).

En este contexto, se revela el presente proyecto investigador y original mediante Tesis por Compendio de Publicaciones, algo que en sí mismo podría considerarse como innovador en la Facultad de Ciencias Sociales y jurídicas, al ser más común de tesis doctorales en otras ramas más tecnológicas o de Ciencias, como es sabido. Dicho esto, la tesis presenta un doble objetivo, en primer lugar, pretende i) poner de relieve la actualidad y relevancia del derecho fundamental sobre el que versa, el derecho a la protección de datos, así como su carácter transnacional y transversal mediante su proyección en las principales áreas de convergencia con otros derechos y libertades fundamentales en el ordenamiento jurídico español consagrados en la Constitución Española de 1978; ii) así como hacer referencia a la opción del juicio de ponderación de derechos necesaria en caso de conflicto o convergencia de derechos.

En particular, se centra en su relación con los derechos a la intimidad personal y familiar, a la libertad de información veraz y a la comunicación, a la tutela judicial efectiva en la Administración de Justicia española y sus implicaciones en el orden penal, al ser considerado el de mayor interés mediático y calado social. También, pone el foco en las particularidades de la protección de datos en el derecho a la salud o ámbito sanitario, en el que la mayoría de los datos que se tratan son de carácter sensible, y, por ende, requieren una protección adicional y el establecimiento de garantías agregadas.

En segundo lugar, la tesis procura evidenciar que, aunque se han producido grandes avances y esfuerzos sociales (y normativos) en la tutela de este derecho fundamental, aún queda gran trabajo para conseguir un cumplimiento real e implementado, una conciencia y una cultura global sobre protección de datos, armonizada y con homogeneidad regulatoria – esto es lo que se pretendía, al menos en el ámbito europeo, con el RGPD -.

Por tanto, se pretende realizar una aproximación a este derecho fundamental desde un punto de vista diferente, en el siglo XXI denominado siglo de la internacionalización de los derechos[4] y con un enfoque que no se ha realizado hasta ahora.

[4] Gómez Montero, A., "Exposición sobre obsolescencia de los derechos", en Congreso de la Asociación de Constitucionalistas Españoles*,* 2018.

En línea con lo anterior, se pone de manifiesto en este apartado introductorio que las Tecnologías de la Información y de la Comunicación (TIC, en adelante), los medios digitales en general, el *Cloud* o la nube y la red de internet[5] configuran auténticas armas de doble filo. Así, además de múltiples ventajas (como el incremento de la productividad mediante la automatización de procesos, la mejora las relaciones sociales, la agilización de las comunicaciones *online*, la creación de nuevos modelos de negocio o el acceso inmediato e ilimitado a información), su utilización también conlleva graves riesgos para los derechos fundamentales y libertades de las personas que es preciso considerar y garantizar, en particular en relación con el derecho sobre el que gira la presente tesis.

En este punto, se considera procedente precisar que, aunque existen diversas definiciones del "derecho a la protección de datos personales", a los efectos de la presente tesis se entiende como la facultad de toda persona física de decidir o controlar qué datos personales facilitar, a quién, para qué finalidad. Datos personales entendidos como cualquier información referente a una persona física viva, identificada o identificable. Además, es un derecho que en sí mismo comprende otras facultades ejercitables por los interesados, como el derecho a solicitar el acceso a la información la rectificación o cancelación, oponerse a su tratamiento, limitar su tratamiento o solicitar su portabilidad. Dicho control de la información personal se realiza por su titular, principalmente, con la finalidad de impedir su tráfico o tratamiento ilícito o lesivo para la dignidad y los derechos de su titular, así como para impedir su tratamiento al margen de la ética[6].

En relación, con eso último, a consecuencia del uso generalizado de los medios digitales y de la red de internet, existe una gran cantidad de información sobre personas físicas que circula, fluye y está en movimiento o que, en otros casos,

[5] En este punto, se señala que, en la actualidad, persisten las denominadas brechas digitales entre las personas que utilizan los medios digitales y las que no tienen acceso o teniéndolo no saben utilizarlos por distintos motivos: geográficos, de edad o por pertenecer a denominados grupos denominados "meta-excluidos". García Almeida, A. y Medina Sánchez, N. y Castillo, Singh, C., *"La brecha entre el primer y el tercer mundo en la actualidad",* en *Revista Información Científica*, núm. 50.2, 2006, pág. 3; y Caridad Sebastián, M. y Ayuso García, M.D., "Situación de la brecha digital de género y medidas de inclusión en España", Investig. Bibliog, vol. 25, núm. 55, México, 2011, págs. 227-252. No obstante, se toman medidas para su inclusión y reducción, como se refleja en la vigente legislación española sobre protección de datos, que reconoce expresamente el derecho universal de acceso a internet.

[6] Al final del Capítulo I se delimita el concepto y sus principales diferencias con el derecho fundamental a la intimidad personal y familiar en el ordenamiento jurídico español.

permanece almacenada, siendo susceptible de ser tratada por terceros distintos de su titular con finalidades lícitas. Nos referimos tanto a datos personales ordinarios (como pueden ser los datos identificativos o de contacto) como a los considerados de carácter sensible, entre los que se consideran los datos de salud, aquellos que revelen origen racial, las opiniones políticas o las convicciones religiosas. En ambos casos se trata de información personal que en unas ocasiones es cedida por su titular tanto de forma consciente (como puede ocurrir al suscribirse a una aplicación móvil o al contratar un producto o servicio online o de forma presencial, cediéndose datos básicos identificativos, bancarios, de salud, profesionales o relativos a preferencias) como inconsciente[7].

Además, a dicha información se sumarían los denominados rastros o "huellas digitales" generadas en todos los ámbitos, también generados en unos casos de forma informada e consciente pero en otros de forma no consciente, como puede ocurrir al comprar un periódico, suscribirse a un boletín de noticias de un determinado canal, visitar un sitio web determinado, la descarga y uso de una aplicación o *app* en la que se incluye información personal o la publicación de fotografías o vídeos en redes sociales.

Como se indicaba, el conjunto de dicha esta información personal tiene el riesgo inherente de ser objeto de tratamiento y ser almacenada por terceros, lo que conlleva un riesgo de vulneración de los derechos fundamentales y libertades de las personas, en especial en el derecho a la intimidad y a la protección de datos personales. Así, un tratamiento de datos al margen de la normativa, de los principios sobre protección de datos y de la ética, puede conllevar efectos perjudiciales de difícil reparación e incluso puede lesionar derechos y libertades, con la gravedad que ello supone.

Al respecto, y teniendo en cuenta que la presente tesis se presenta en el ámbito del Derecho Constitucional, se considera de interés traer a colación la reflexión de MURILLO DE LA CUEVA sobre que los verdaderos peligros a los que nos enfrentamos en la actualidad son: primero, el gran volumen de información personal, irrelevante en

[7] En concreto, se puede afirmar que: "el flujo de datos procedentes del gran volumen de objetos conectados existentes se ha incrementado cuarenta y cinco veces en los últimos diez años. Toda esa información, gestionada de forma eficiente gracias a las tecnologías como la inteligencia artificial, permite obtener conocimientos clave para pasar a las empresas o a los gobiernos". Álvarez-Pallete, J.M. "Informe Sociedad Digital en España", Fundación Telefónica, 2019, pág. 8.

principio, manejada por terceros; segundo, que a través de su tratamiento se pueden obtener datos adicionales con los que lograr conocimientos de todo tipo de la vida privada; y tercero, que a partir de la información obtenida se pueden generar perfiles de la personalidad y con ellos, condicionar o limitar los derechos y libertades personales[8]. Añadía el citado autor la advertencia de que se trata de una cadena que, aunque pueda parecer irrelevante o inofensiva, puede generar graves perjuicios de difícil reparación.

Por todo ello, se evidencia que uno de los mayores riesgos de la digitalización y el uso generalizado de las TIC y los medios digitales es la pérdida de privacidad y la recopilación de datos del usuario y su posible distribución a terceros, con el peligro de caer en manos de agentes maliciosos o ser utilizados con fines ilícitos (como pueden ser la comisión de un fraude, un ciberataque, una extorsión, su venta ilícita de los mismos o una sustracción económica). Otros riesgos podrían ser la desinformación a raíz de la divulgación de noticias falsas o *fake news* en medios de comunicación y redes sociales, la propensión al aislamiento social o los problemas de dependencia digital o falta de "desconexión digital".

En este sentido, es necesario partir de la premisa de que los avances tecnológicos como el metaverso, el Internet de las Cosas (IOT, en adelante), el *ChatGPT*, la citada Inteligencia Artificial (IA, en adelante) o los denominados *Chatbots*, conllevan grandes riesgos en materia de privacidad y protección de datos que son necesarios tener en cuenta y abordar garantizando el cumplimiento de la normativa aplicable, junto a mecanismos, medidas de tutela y control periódicos. Como se ha indicado anteriormente, frente a dichos riesgos y tratamientos ilícitos de datos se han ido articulando y desarrollando mecanismos legales a nivel internacional, europeo y nacional; a lo que se une el aumento de la consciencia social del valor de su información personal (aumentando el interés y preocupación en proteger y controlar sus datos personales).

[8] Murillo De la Cueva, L., "La confidencialidad de los datos personales: garantías el proceso judicial. La protección del derecho de intimidad de las personas (fichero de datos)", *Cuadernos de Derecho Judicial (XIII),* CGPJ, Madrid, 1998, pág. 232; Colmenero Guerra, J.A., "La protección de datos en la Administración de Justicia", *Portal Iberoamericano de Ciencias Penales, Instituto de Derecho Penal Europeo e Internacional, Universidad de Castilla- La Mancha*. Recuperado de: http://www.cienciaspenales.net (fecha de consulta: 2018).

No obstante, desde el punto de vista de protección de datos, y será uno de los principales resultados de la presente investigación, casi seis años tras la entrada en vigor y aplicación de la normativa europea reguladora, siguen incrementando los tratamientos ilícitos de datos, reiterándose los sectores, los tipos de infracción y las modalidades. Al mismo tiempo, se pondrá de manifiesto el aumento de las cifras de cibercriminalidad o ciberdelincuencia, habiéndose sofisticado tanto las amenazas como los ciberataques y variado sus agentes[9] (ciberestafas, ciberacoso, ciberbullying, *phishing-car*, *phishing bancario, vishing, smising, spoofing, baiting*[10]).

En virtud de lo anterior, se considera que la actualidad del tema elegido es notoria, encontrándose la protección de datos, junto a la cibercriminalidad, entre las principales preocupaciones en la época actual en todos los ámbitos, configurando además un factor esencial de negocio en todas las empresas independientemente de su tamaño. De ahí, la relevancia y pertinencia de su estudio, así como también su carácter innovador pues, aunque existen diversos estudios y publicaciones sobre protección de datos, ninguno lo realiza con el mismo enfoque y con la vocación general de contribuir modestamente a la cultura global de cumplimiento[11] y al principio de responsabilidad proactiva o *accountability*.

De otro lado, en cuanto a los interrogantes iniciales a los que se pretendía dar respuesta al comenzar la tesis en el año 2018 fueron, principalmente, los siguientes: ¿qué significa exactamente la "protección de datos personales" ala que se hace referencia en múltiples ocasiones y por diversos agentes? ¿cuáles son sus características y sus implicaciones? ¿cuál es el marco normativo de protección de datos a nivel internacional, europeo y español vigente? ¿cómo ha sido su evolución? ¿es un derecho tan novedoso como parece ser? ¿cuáles han sido los principales hitos jurídicos en torno a la evolución de la protección de datos en los citados ámbitos?

[9] Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html (fecha de consulta: 2018).

[10] Ciberataque conocido como "cebo", ataque informático que utiliza la ingeniería social para lograr el objetivo malicioso. Para más información, véase la Guía de ciberataques del Instituto Nacional de Ciberseguridad (INCIBE). Recuperado de: https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf (fecha de consulta 2024)

[11] Schneier, B. *"*Data Is a Toxic Asset, So Why Not Throw It Out*?",* 2016. Recuperado de: https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html (fecha de consulta: 2018).

Entre otros interrogantes iniciales, destacan los siguientes: ¿Protección de datos e intimidad se refieren a lo mismo? ¿qué convergencias entre protección de datos y otros derechos fundamentales pueden darse en el marco del ordenamiento jurídico español y qué hacer ante situaciones de convergencia de derechos? ¿cómo se realizaría un juicio de ponderación y con qué finalidad?

Además, durante los años de desarrollo de investigación, se fueron ampliando otras cuestiones (al mismo tiempo que se fue ampliando el objeto de la Tesis y las publicaciones que la compendian), entre las que cabe resaltar las siguientes: ¿El RGPD ha cumplido con el objetivo de armonización para el que fue creado? ¿se está cumpliendo el RGPD tras varios años después su entrada en vigor y aplicación? ¿cuál es el nivel de cumplimiento o madurez? ¿cuáles serían las principales particularidades de la protección de datos en su aplicación en el ámbito judicial, el ámbito penal y el sector sanitario? ¿cuál fue el principal impacto de la pandemia sanitaria COVID-19 en la digitalización y en el derecho a la protección de datos? ¿cuáles son las tendencias actuales en torno a la protección de datos?

A modo de corolario del presente capítulo introductorio, interesa señalar que el presente trabajo se compone de un total de cinco capítulos, siendo el primero de carácter más teórico al reflejar la aproximación al derecho a la protección de datos y a los principales hitos normativos a nivel internacional europeo y español, previa noción de los derechos humanos y su proceso de reconocimiento. Ello, junto al concepto de protección de datos y su delimitación del derecho a la intimidad personal y familiar; así como las nociones básicas sobre el juicio de ponderación de derechos en caso de conflicto de derechos fundamentales en el ordenamiento jurídico español (como puede ocurrir en la práctica entre protección de datos vs. libertad de información veraz).

Los cuatro capítulos siguientes se consideran de carácter más innovador toda vez que contienen las cuatro publicaciones que conforman el compendio (la última de ellas aceptada y pendiente de publicación en el año 2024). En las publicaciones que lo conforman se reflejan las proyecciones del derecho a la protección de datos en áreas de convergencia con otros derechos fundamentales seleccionadas en el ordenamiento jurídico español, tal y como se ha expuesto.

Finalmente, se expondrán y discutirán los resultados evidenciados en el apartado sobre Resumen global y Discusión de resultados; seguido de las principales Conclusiones y las Referencias.

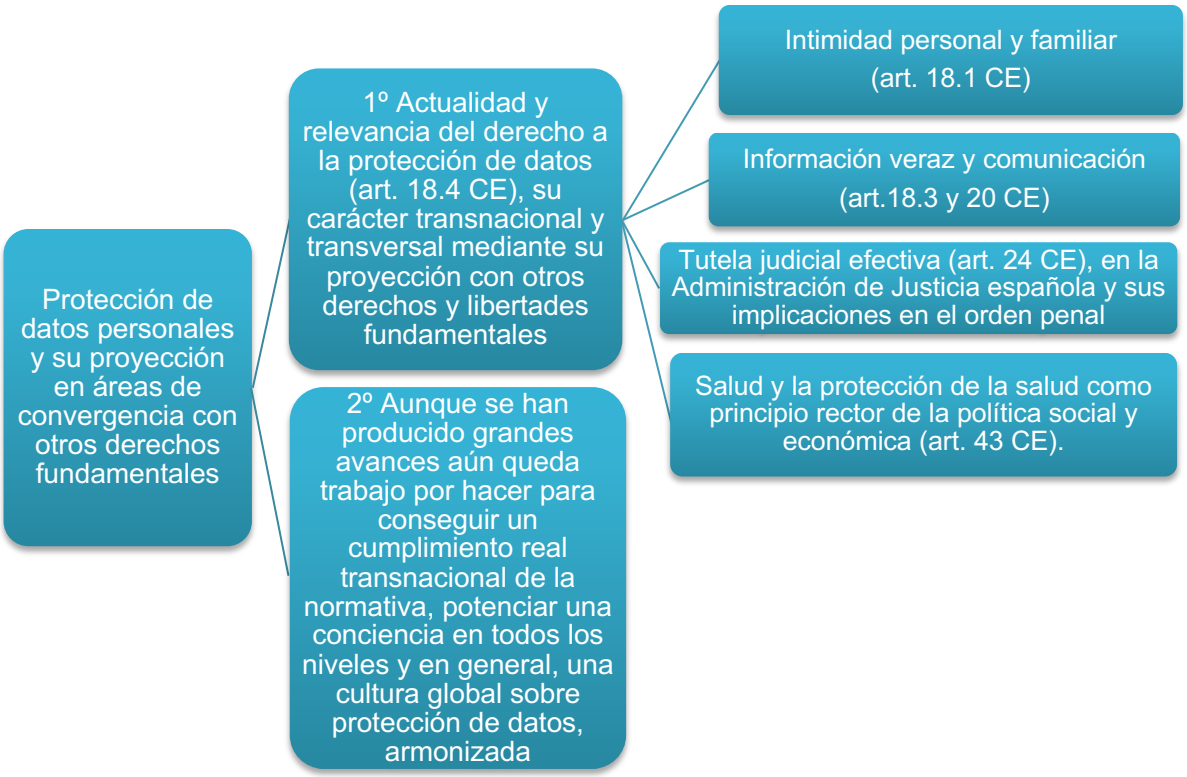
Objetivos, estructura y metodología

Objetivos, estructura y metodología

I. Objetivos

Los objetivos de la presente tesis, que lleva por título “Protección de datos personales y su proyección en áreas de convergencia con otros derechos fundamentales”, son, como se ha mencionado con anterioridad, en primer lugar, poner de relieve la actualidad y relevancia del derecho fundamental de las personas físicas a la protección de datos personales (consagrado en el artículo 18.4 de la Constitución Española de 1978, CE en adelante), así como su carácter transnacional y transversal mediante su proyección y confluencia con otros derechos y libertades fundamentales seleccionados. En línea con lo anterior, se pretende analizar las cuestiones básicas sobre el juicio de ponderación de derechos en casos de convergencia. Centrándonos en los derechos a la intimidad personal y familiar (consagrado en artículo 18.1 de la CE), a la información veraz y a la comunicación (consagrado en el artículo 18.3 de la CE, en conexión con el artículo 20 de la CE); a la tutela judicial efectiva (consagrado en el artículo 24 de la CE) en la Administración de Justicia española y sus implicaciones en el orden penal, al ser el orden de mayor calado social e interés mediático. Por último, en relación con el derecho a la salud, por el carácter sensible de los datos que en él son tratados, así como por el reconocimiento en el texto constitucional de la protección de la salud como principio rector de la política social y económica (según el artículo 43 de la CE).

En segundo lugar, se pretende evidenciar con la presente tesis que, aunque se han producido grandes avances normativos a nivel internacional, europeo y español, así como grandes progresos sociales en la tutela y garantía del derecho a la privacidad y protección de datos, aún queda un gran trabajo por hacer para conseguir un cumplimiento real y transnacional de la normativa, potenciar una conciencia en todos los niveles y en general, una cultura global sobre protección de datos, armonizada y con homogeneidad regulatoria.



Además, la vocación general que preside el presente trabajo investigador es evidenciar la relevancia de la información personal, tratando de contribuir modestamente a una cultura de cumplimiento[12], siguiendo el principio de responsabilidad proactiva o *accountability* en aras de potenciar la concienciación social en el respeto de los derechos de protección de datos y los derechos digitales. Lo anterior, con la finalidad de que dichos derechos sean respetados y percibidos por la sociedad como una necesidad inherente a la identidad y dignidad humana, como uno de los fundamentos del orden y de la paz social.

[12] Schneier, B. "Data Is…" (op. Cit. Nota 11), pág.22.

II. Estructura

En cuanto a la estructura de la presente tesis, además de los preceptivos apartados de “Introducción y justificación” acompañado del apartado sobre “Objetivos, Estructura y Metodología”, se compone de un total de cinco capítulos en relación con los objetivos perseguidos descritos en el punto I sobre Objetivos. A continuación, se desglosa su estructura de forma ordenada por capítulos:

- El **Capítulo I** contiene una aproximación al derecho de protección de datos de carácter personal, precedida por una aproximación a la noción de derechos humanos y su proceso de reconocimiento, lo que se considera relevante dado que el presente trabajo se presenta en el seno de la investigación en el Departamento del Derecho Constitucional. Así, se reflejan los principales hitos jurídicos a nivel internacional, europeo y español relacionados con el mismo. También, contiene referencia al concepto y la delimitación del derecho a la intimidad; y finalmente, unas nociones sobre el juicio de ponderación de derechos en caso de conflicto de derechos.

  Tal y como se ha indicado anteriormente, se trata de un Capítulo de carácter más teórico, compuesto a su vez de cinco apartados versando los cuatro primeros sobre las principales particularidades respecto a la protección de datos, su evolución y los hitos jurídicos más relevantes en esta materia a nivel internacional (en el seno de la Organización para la Cooperación y el Desarrollo Económicos, OCDE en adelante, y el Consejo de Europa), europeo y español. Como hitos jurídicos, se destacan las Directrices de la OCDE, sobre Privacidad y Protección de datos publicadas en 1980, el Convenio Europeo de los Derechos Humanos de 1950, y más recientemente, el RGPD y su reflejo en el ordenamiento jurídico español mediante la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD 3/18 en adelante).

  Adicionalmente, en su apartado quinto se concreta el concepto de “protección de datos”, junto a su delimitación del derecho a la intimidad personal y familiar, con el que en ocasiones se confunde, lo que configura la primera de las proyecciones de convergencia del derecho a la protección de datos con otro derecho. Por último, se

realizan las principales nociones fundamentales sobre el juicio de ponderación de derechos que sería necesario en casos de convergencia de derechos fundamentales.

Este primer capítulo no constituye ninguna publicación, sino que es de carácter más introductorio, de contexto y de estado de la cuestión. Sin perjuicio de la reserva de realizarse una publicación en el futuro con mayor profundidad sobre el mismo. Al final de cada apartado se incluyen los resultados o las evidencias principales a las que se ha llegado en el seno de la investigación.

- Los **Capítulos II a V** comprenden las cuatro publicaciones en Revistas y Libros a nivel nacional e internacional, de reconocido prestigio en el ámbito jurídico, que recopilan los resultados obtenidos en los diferentes focos de investigación y compendian la tesis. Se trata de publicaciones directamente relacionadas con el "Plan de Investigación" académico inicial y según se ha ampliado y evolucionado durante los años de investigación (2018/2024), cumpliendo con los requisitos de ser de calidad acreditada y publicadas después del inicio de la tesis.

  Contienen otras proyecciones relevantes del derecho a la protección de datos con otros derechos fundamentales, además de la contenida en el mencionado Capítulo I, por lo que se considera de los capítulos de carácter más innovador. A continuación, se desglosan las publicaciones y la estructura de su contenido:

  - El **Capítulo II** contiene la primera publicación: López Medina, C., "Aproximación a los nuevos derechos y garantías digitales reconocidos en la LOPDGDD 3/2018", en *Revista Asuntos Constitucionales, número monográfico. Retos Actuales del Derecho Constitucional.* Centro de Estudios Sociales y Jurídicos Sur de Europa *(CESJ)*, núm. 0, 2021, págs.141-150. Recuperado de: https://www.asuntosconstitucionales.com/pdf/0-CLopez.pdf.

    Este Capítulo puede considerarse un complemento al apartado del Capítulo I sobre los hitos jurídicos en el marco del ordenamiento jurídico español, pues aborda una aproximación a los principales derechos y garantías digitales que se reconocieron en el Título X de la LOPDGDD 3/2018 (como el derecho a la educación digital, la seguridad de las comunicaciones, al testamento digital y a

la desconexión digital de los trabajadores). Dichos derechos, para su análisis en la publicación, fueron dividieron en tres bloques: i) los derechos en el entorno digital, ii) los derechos digitales en relación con los menores de edad, al considerarse sujetos a un mayor riesgo; y iii) los derechos digitales en el ámbito laboral. También, en esta publicación se analiza la significación jurídica de su reconocimiento en el ordenamiento jurídico español.

- El **Capítulo III** contiene la segunda publicación: López Medina, C., "Protección de datos personales en la Administración de Justicia española. Protocolo de Comunicación de la Justicia 2018", en *Revista Internacional Online Derecho de la Comunicación de la Universidad Complutense de Madrid* (Derecom), núm. 26, 2019, págs. 115-130. Recuperado de: http://www.derecom.com/secciones/articulos-de-fondo/item/374-personal-data-protection-in-the-spanish-judiciary-the-2018-protocol-on-the-judiciary-communications.

Este Capítulo resulta de la confluencia entre protección de datos y el derecho fundamental a la tutela judicial efectiva, en la Administración de Justicia española, esto es, en el ámbito judicial; así como, además, de la confluencia con el derecho a la información veraz y la comunicación. Es decir, se pone en conexión su proyección en el área de convergencia con el derecho a la libertad de información mediante el análisis de las principales medidas y recomendaciones que establece en el Protocolo de Comunicación de la Justicia de 2018 elaborado por la Oficina de Comunicación del Consejo General del Poder Judicial (CGPJ, en adelante) para que la información judicial, especialmente del orden penal, llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados.

- El **Capítulo IV** incluye la tercera publicación: López Medina, C., "El derecho fundamental a la protección de datos personales en el ámbito penal", en Ruiz Rico-Ruiz, G; Pomares Cintas, E; Revenga Sánchez, M; Vergara Galaz, D. (coords.), *Derecho Penal y Garantías Constitucionales. Una perspectiva iberoamericana*, Tirant lo Blanch, Valencia, 2020, págs.113-133.

Este Capítulo se dedica a la confluencia entre protección de datos y derecho penal, orden de especial interés social y de mayor calado mediático, tal y como se ha indicado. Expone las principales cuestiones sobre este derecho fundamental en el ordenamiento jurídico español y sus particularidades en el ámbito penal en respuesta a sus interrogantes de cuál es el régimen jurídico de protección de datos en el proceso penal, cómo incide protección de datos en el proceso penal y en la actividad investigadora criminal; y si es posible ejercer el derecho a la libertad de información veraz con respeto al derecho de protección de datos, en especial al derecho a la información derivada de procesos penales.

- El **Capítulo V** contiene la última publicación: López Medina, C., "Protección de datos personales en el sector sanitario, en el contexto del derecho a la salud y de la digitalización impulsada por la pandemia Covid-19", en *La Protección de los derechos humanos por las defensorías del pueblo en situaciones de emergencia constitucional*, Tirant Lo Blanch, aceptada pendiente de publicación en el año 2024.

Esta publicación contiene la convergencia de protección de datos y derecho a la salud, refleja las principales particularidades de protección de datos en el ámbito sanitario y el marco normativo de protección de datos en sector salud, con especial atención en la digitalización y con especial referencia al impuso tras la pandemia Covid-19. Adicionalmente, hace alusión a la telemedicina o *ehealth*, su evolución, alcance, principales ventajas y barreras desde el punto de vista de protección de datos.

Por último, se incluyen los apartados de Resumen global y Discusión de resultados, junto a las principales Conclusiones y las Referencias bibliográficas.

III. Metodología

En lo que respecta a la metodología, se ha recurrido fundamentalmente a los métodos histórico, lógico-sistemático de análisis normativo y jurídico-comparado, con fuentes primarias y secundarias, entre las que se citan las Declaraciones de derechos, Pactos y Convenios internacionales, así como las Directrices sobre privacidad de la OCDE de 1980. Con especial foco en la normativa europea, el RGPD, y la nacional de España en materia de protección de datos, LOPDGDD 3/18. Junto a ello, han sido objeto de análisis las principales resoluciones emitidas por la autoridad de control en materia de protección de datos, en particular por la Agencia Española sobre Protección de Datos (AEPD, en adelante), especialmente sus Guías de interpretación, Informes, Dictámenes; la autoridad francesa "The Commission nationale de l'informatique et des libertés" (CNIL, en adelante) y Autoridad de Protección de Datos del Reino Unido (ICO, por sus siglas en inglés, en adelante). Adicionalmente, se han analizado las principales resoluciones o sentencias por los Tribunales españoles.

Con carácter general, la metodología ha consistido fundamentalmente en la recopilación y análisis de bibliografía, artículos y monografías doctrinales sobre los derechos humanos, los derechos fundamentales y en concreto, el derecho a la protección de datos personales. Igualmente, se han tomado como referencia las monografías doctrinales preexistentes sobre esta materia y las publicadas durante la investigación.

A modo complementario, se ha asistido a cursos, seminarios y jornadas presenciales y *online* "*Webminars"* de expertos y profesionales sobre el derecho a la protección de datos de carácter personal y su régimen normativo, así como relacionadas en el ámbito de la ciberseguridad y seguridad de la información. Entre otros, se señalan a modo ejemplificativo, el Seminario "*¿Qué tengo que hacer para cumplir la normativa de protección de datos?"*, celebrado el día 19 de septiembre de 2019 en la sede de la Confederación de Empresarios de Jaén (CEF) o el Congreso Internacional sobre *Cuestiones actuales en materia de protección de datos*, celebrado en la Universidad de Sevilla con fecha 17 de mayo 2019. También, al Seminario "*nuevos principios y garantías para responsables y encargados de tratamiento según el Reglamento General de Protección de Datos y el Proyecto de Ley Orgánica de Protección de*

datos", celebrado en mayo de 2018 en la sede de la Confederación de Empresarios de Jaén (CEF).

De otro lado, destaca la asistencia a la 10ª y 11 ª Sesión Anual Abierta sobre Protección de Datos, organizada en Madrid por la AEPD en junio de 2018 y en 2019; al seminario "La protección de datos personales en el marco de la epidemia COVID - 19", Universidad Internacional Menéndez Pelayo (UIMP) celebrado del 2 al 4 de septiembre de 2020 (20 horas). Adicionalmente, al XIV Foro de Privacidad organizado por el ISMS *Forum* y a la presentación del primer y segundo informe del Observatorio de Derecho Digital del Instituto de Empresa-ECIJA en 2023. Por último, resalta el "Curso técnico básico de Ciberseguridad" y "Protección de datos para autónomos y pymes", cursados durante el año 2023-2024 del Instituto Nacional de Ciberseguridad (INCIBE).

Otra fuente de búsqueda de información ha consistido en la revisión periódica de noticias nacionales e internacionales sobre protección de datos, alertas de *newsletter*, depositorios públicos de resoluciones sancionadores o de archivo y bibliografía sobre cuestiones relacionadas.

Finalmente, para una mayor especialización, se superó el Máster de especialización en Protección de Datos y Seguridad de la Información impartido como Título Propio en la Universidad Complutense de Madrid (UCM), 2021/2022, junto con la experiencia profesional especializada en la materia, trabajando dos años como Abogada de Protección de Datos y Privacidad, además de un año y medio de investigación durante una Beca de investigación europea en la Universidad de Jaén.

Respecto a las normas de estilo utilizadas en la citación y referencias bibliográficas, se ha optado por el criterio seguido por las Normas de Estilo en Ciencias Jurídicas 2.0., además de las normas de estilo requeridas por las revistas y editoriales en las que se han realizado las publicaciones que compendian la presente tesis.

Por todo ello, se puede concluir que el presente trabajo de investigación que se presenta es fruto de una evolución reflejada en los "Planes de Investigación" académicos que, en las primeras evaluaciones (años académicos 2018/2019 y 2010/2020) se centraban en la protección de datos en general y su implicación en el

ámbito de la Administración de Justicia Española. Lo anterior, fundamentalmente motivado por mi interés en este sector, en el que estuve anteriormente casi dos años opositando a Carrera Judicial y Fiscal (2014/2016) y otros dos años como pasante de abogada en un despacho del ámbito civil y mercantil (2016/2017).

No obstante, los "Planes de Investigación" académicos se fueron adaptando y modulando según las necesidades de la investigación y las nuevas áreas de interés de proyección identificadas durante su desarrollo. De tal forma que el trabajo de investigación se presenta años después (2018/2024) con un Capítulo más teórico de aproximación a la protección de datos, al que se une el compendio de cuatro publicaciones publicadas durante el periodo de Doctorando. Así, se observa que su contenido y título es más amplio al previsto inicialmente, pues contiene publicaciones sobre protección de datos no solo en el ámbito judicial, sino también, en el ámbito penal y en el sector sanitario.

El siguiente gráfico ilustrativo muestra la evolución de los Planes de Investigación académicos presentados:

En particular, el **Capítulo I** es resultado del periodo (año académico 2018/2019) como personal investigador en el Departamento de Derecho Constitucional, el seno de Beca de investigación europea, en la que tuve la oportunidad de recopilar y realizar un análisis preliminar del material doctrinario, legislativo, noticias y resoluciones existentes en la materia. También, en este periodo se crearon las publicaciones que constituyen el **Capítulo II**, publicada posteriormente en el año 2021, el **Capítulo III**, también publicada posteriormente en septiembre de 2019; y finalmente, el **Capítulo** que, actualizado posteriormente, constituye el **IV**.

En una segunda etapa de desarrollo del trabajo de investigación (años académicos 2019/2020 a la actualidad 2023/2024), se ha compaginado con mi etapa profesional como abogada (habiéndome especializado en protección de datos y seguridad de la información). En particular, durante este periodo se derivó la última publicación, que conforma el **Capítulo V** del Compendio de publicaciones (aceptada y pendiente de publicar en el año 2024).

En último lugar, durante la etapa final se ha terminado de perfilar el enfoque más amplio e innovador de la tesis, así como realizado las correcciones, actualizaciones y revisiones finales junto con mi tutor y director de tesis para depositarla para su lectura y defensa ente los miembros del Tribunal en el año 2024, optando al Título de Doctor en Derecho.

Se concluye que, como se ha evidenciado, la presente tesis es fruto de la evolución durante los años académicos de estudio (2018/2024), investigación y práctica profesional en el ámbito del derecho a la protección de datos; siendo ampliada (siempre desde la óptica de protección de datos y dentro del margen del “Plan de Investigación”) en sus áreas de convergencia y proyección en los diversos sectores, con un enfoque más global e innovador. Aunque existen y se han publicado múltiples estudios de protección de datos personales, ninguno lo ha hecho con la visión, metodología y orientación en que se realiza en el presente trabajo de investigación.

CAPÍTULO I.- APROXIMACIÓN AL DERECHO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: PRINCIPALES HITOS JURÍDICOS A NIVEL INTERNACIONAL, EUROPEO Y ESPAÑOL. CONCEPTO Y DELIMITACIÓN DEL DERECHO A LA INTIMIDAD; Y NOCIONES SOBRE EL JUICIO DE PONDERACIÓN

1. Introducción y nociones básicas sobre los derechos humanos y su proceso de reconocimiento, con especial referencia al derecho a la protección de datos.

A) Introducción

Este primer capítulo contiene una referencia a las particularidades del derecho a la protección de datos, los principales hitos jurídicos en esta materia en el marco normativo internacional (en el seno de la OCDE y del Consejo Europeo), europeo y del ordenamiento jurídico español, como se ha indicado en el apartado introductorio; así como también, la concreción del concepto "protección de datos" y su delimitación del derecho fundamental a la intimidad personal y familiar. Ello, junto a unas nociones básicas sobre el juicio de ponderación de derechos a realizar en caso de convergencia.

Aunque, con carácter previo y, dado que el presente proyecto investigador se presenta en el Departamento del Derecho Constitucional, se realiza una breve aproximación a la noción de "derechos humanos" y a su proceso de reconocimiento, como se muestra a continuación.

B) Nociones básicas sobre los derechos humanos y su proceso de reconocimiento, con especial referencia al derecho a la protección de datos.

Los derechos humanos pueden ser entendidos como las facultades para las que desde finales del siglo XVII se generalizó la denominación de "humanos" al pertenecer y obligar a todos por igual, le son inseparables y deben estar siempre garantizados. En cuanto a los procesos de reconocimiento de los derechos humanos, primero, por el proceso de positivización se pasó de la "filosofía de los derechos" al "Derecho positivo" con la incorporación de los derechos humanos en los textos de las Constituciones, pasando a tener otras denominaciones como derechos "fundamentales" (como se

denominan actualmente en España), derechos "constitucionales" o "garantías esenciales"[13].

Cabe precisar que las nociones "derechos humamos" y "derechos fundamentales" no son lo exactamente mismo, aunque en ocasiones se utilicen como sinónimos, pues todos los derechos fundamentales son humanos, pero no al contrario. Así, no todos los derechos humanos, son fundamentales y, por tanto, constitucionalizados. Aunque realmente la determinación puramente jurídico-positiva de los derechos fundamentales no permite olvidar su conexión con los humanos[14]. Independientemente de cómo se denominen, en el siglo XXI culminó un giro "individuo céntrico" en virtud del cual consideramos que hay un ámbito de autodeterminación intangible en cada persona y que corresponde a las normas reconocerlo, propiciarlo y tutelarlo[15].

En cuanto al proceso de reconocimiento de los derechos humanos, mediante el proceso de positivización, "las posibilidades de que se materialice cualquier aspiración que se considere justa y digna de defensa aumenta exponencialmente cuando aparece recogida en un *corpus* jurídico coherente y cerrado, capaz de reflejar cambios consensos y de abrir vías para realizaciones concretas"[16]. Así, ha ocurrido en el ordenamiento jurídico español desde que inicialmente apareció en la conciencia social la existencia de un ámbito privado libre de injerencias indebidas de terceros, hasta que

[13] Rubio Llorente, F. "Derechos fundamentales, derechos humanos y Estado de Derecho", en Punset Blanco, R. y Bastida Freijedo, F. y Varela Suanzes-Carpegna, J. (dirs.), *"Fundamentos. Cuadernos monográficos de Teoría del Estado"*, Derecho Público e Historia Constitucional, Junta General del Principado de Asturias. pág. 212. Siguiendo a Truyol y Serra, los derechos fundamentales son un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humana, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional, en Pérez Luño, A.E., "Derechos Humanos, Estado de Derecho y Constitución", Tecnos, Madrid 2010, pág. 50. De otro lado, para Fernández-Galiano y De Castro Cid, son aquellos de los que es titular el hombre no por concesión de normas positivas, sino con anterioridad e independientemente de ellas y por el mero hecho de ser hombre, de participar en la naturaleza humana. Tales derechos son poseídos por todo hombre, cualquiera que sea su edad, condición, raza, sexo o religión, estando, por tanto, más allá y por encima de todo tipo de circunstancia discriminatoria. Fernández-Galiano y De Castro Cid establecen en su obra esta definición para los derechos fundamentales, pero afirman que los términos "Derechos Humanos", "derechos del hombre" y todas las designaciones similares se pueden utilizar también. Por tanto, tendrían cabida dentro de la propia definición.

[14] Rubio Llorente, F., "Derechos fundamentales, …", (op. Cit. Nota 13), pág. 213.

[15] Revenga Sánchez, M., "Regeneración Democrática y Reforma constitucional", en Revenga Sánchez, M; Porras Nadales, A y Ruiz Rico-Ruiz, G. (coord.), Tirant Lo Blanch, Valencia, 2017, pág.13.

[16] *Ibidem*, pág.14.

más tarde se positivaron los derechos a la intimidad personal y familiar y el derecho a la protección de datos personales.

De otro lado, a través del proceso de generalización de los derechos humanos, se introdujeron en la fórmula de los derechos componentes igualitarios por la influencia del movimiento obrero y del socialismo democrático. Más adelante, por el proceso de internacionalización, a lo largo del siglo XX se produjo su evolución histórica, siendo tras la Segunda Guerra Mundial cuando se tomó conciencia general de que la promoción de los derechos humanos es un asunto internacional, que trasciende más allá de las fronteras y del ámbito nacional.

Por último, el proceso de especificación en el proceso de reconocimiento de los derechos humanos supuso la concreción de los titulares y del contenido de los derechos, pasando desde la reflexión abstracta de los derechos, a su determinación o concreción. En este punto, se traen a colación las dos posturas doctrinales, respecto a las que una postura minoritaria entendería que los derechos fundamentales configuran un listado cerrado; mientras que otro posicionamiento mayoritario consideraría que configuran un listado abierto, entendiendo que "el progreso moral y material de la humanidad se proyecta o debe proyectarse en una continua ampliación"[17].

Siguiendo esta última postura, junto a los derechos clásicos (como el derecho a la vida, a la propiedad privada o a la libertad personal) se han ido reconociendo progresivamente otros de creación más reciente, como el derecho a la intimidad personal y familiar, al honor, a la imagen o a la protección de datos.

También se considera ilustrativo hacer referencia a la concepción de PECES-BARBA en su obra *Derecho positivo de los Derechos Humamos*[18], en la que diferenciaba dos periodos en cuestión de derechos: la "prehistoria de los derechos" (que abarcaría el periodo en que rasgos, ideas y elementos de la sociedad fueron el germen de lo que pasó más tarde a considerarse derechos humanos) y la "historia de los derechos", momento a partir de su consagración en textos. Centrándonos en este último, como

[17] Rubio Llorente, F., en "Derechos fundamentales …", (op. Cit. Nota 13) pág. 206.
[18] Peces Barba, Martínez, G., "Derecho Positivo de los Derechos Humanos", Colección Universitaria, Editorial Debate, Madrid, 1987.

principales hitos jurídicos se consideran destacables la *Bill of Rights* de 1688, la Declaración de Derechos del pueblo de Virginia de 1776, la Declaración de Independencia de los Estados Unidos de 1776 y la Declaración francesa de los Derechos del Hombre y del Ciudadano de 26 de agosto de 1789[19].

Aunque realmente no fue hasta a partir del siglo XIX cuando los derechos humanos se constitucionalizaron, "en una evolución que ha ido abarcando otros, como los derechos sociales o colectivos, y que se ha ido preocupando de instaurar mecanismos de tutela que no se agotan en el ámbito interno, sino que, con el tiempo, se han internacionalizado"[20]. Entre estos derechos, se enmarca el reconocimiento y desarrollo del derecho fundamental a la protección de datos personales de la persona física.

Por tanto, la evolución del reconocimiento de los derechos humanos, y en particular del derecho a la protección de datos, ha derivado de un progresivo desarrollo, que se prevé seguirá en adelante en el transcurso de los próximos años siguiendo la tendencia actual, en la que el avance de la digitalización genera retos y desafíos constantes en la tutela de la privacidad y el derecho a la protección de datos. A los que se han unido la IA (la auténtica protagonista del año 2024), el Metaverso y la ciberdelincuencia.

En particular, el desarrollo y la evolución exponencial del derecho a la protección de datos, comenzaría a partir de la segunda mitad del siglo XX, a mediados de los años ochenta, cuando la aplicación de la informática permitió la aparición de "instrumentos de trabajo automatizados y el desarrollo de las telecomunicaciones (…), a través del sistema global de redes informáticas que encabeza internet"[21]. Dado que en dicho siglo XX se produjo "la consolidación de los derechos económicos, sociales y culturales que aparecieron en el siglo XIX[22]", fue durante dicho periodo cuando se empezó a apreciar en la sociedad la necesidad de tutelar y garantizar la privacidad, el honor, la intimidad y posteriormente, con la irrupción de las nuevas tecnologías en todos los ámbitos, de proteger y controlar la información personal.

[19] Esta última proclama derechos naturales e imprescriptibles, anteriores a los poderes establecidos, aplicables en cualquier lugar y cualquier época, como a la libertad y la igualdad en derechos, a la seguridad, a la propiedad o a la libertad de opinión y conciencia.
[20] Manual Derecho Constitucional para preparación oposición de acceso a la Carrera Judicial y Fiscal, Carperi S.L, tema 14, 2014,
[21] García Almeida, Á., y Medina Sánchez, N., Castillo Singh, C., "Situación de la brecha…(op. Cit. Nota 5), pág.3.
[22] De La Torre Reyes, T., "Evolución Histórica, concepto y fundamentación de los Derechos Humanos", Módulo I, Universidad de Colima, 2008, pág. 30.

Inicialmente, los datos personales fueron objeto de tutela junto con el derecho a la intimidad personal y familiar, pues era entendido como dimensión o manifestación del mismo[23]. No obstante, más adelante (a mediados de la segunda mitad del siglo XX, sobre la década de los ochenta) fue reconocida su independencia y autonomía del derecho a la intimidad, como se analizará de forma profunda más adelante.

En cuanto al reconocimiento del derecho a la intimidad, se remonta fundamentalmente a la Declaración Americana de los Derechos y Deberes del Hombre de 1948 (DADH, en adelante) o Carta de San José aprobada por la IX Conferencia Internacional Americana en Bogotá el 2 de mayo de 1948, que reconocía explícitamente el derecho de toda persona a la "protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar" (artículo 5 DADH).

Posteriormente, la Declaración Universal de los Derechos Humanos (DUDH, en adelante), proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948[24], expresó de forma literal que: "Nadie será objeto de

[23]Así, inicialmente, la intimidad se representaba en su vertiente negativa u obstativa a no hacer del dominio público informaciones privadas o reservadas; y otra positiva, como la facultad de control sobre datos concernientes a la propia persona. Aunque, protección de datos o también denominado "*habeas data"* se puede definir el derecho de la persona física de controlar el uso y el destino de la información personal de la que es titular, constituyendo en la actualidad un derecho distinto e independiente del derecho a la intimidad, aunque en ocasiones es frecuente que converjan y no sea fácil su delimitación. Posteriormente, las resoluciones del TC como máximo intérprete de la CE han precisado que los derechos a la intimidad y a la protección de datos personales son dos derechos autónomos e independientes. Destaca el FJ7 de la STC nº 292/2000, de 30 de noviembre, que expresa de forma literal: "El derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven para la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales (...). (STC 254/1993, FJ7). Estos poderes se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero".

[24]Aunque, como expone su Preámbulo, la DUDH aspiraba a ser el "ideal común por el que todos los pueblos y naciones deben esforzarse", existen diversas posturas doctrinales sobre su valor jurídico. Algunos niegan su carácter jurídico internacional, como H. kelsen, "Principios de Derecho Internacional Público", El Ateneo, Buenos Aires, 1965, (trad. de H. Caminos y E. C. 1952, Hermida del original *Principles of International Law*, Rinehart & Co., Nueva York,), págs. 124 y 125; *Idem*, The Law of the United Nations. A Critical Analysis of its Fundamental Problems, Praeger, Nueva York, 1950, págs. 39 y 40; o Rodríguez Zapata, J., "Teoría y práctica del Derecho Constitucional", Tecnos, Madrid, 1996, pág. 296.
Otros mantienen su autoridad jurídica directa, como González Campos; y para otra parte de la doctrina, como Bassin o Truyol y Serra, es un tratado con fuerza jurídica vinculante para todos los Estados Miembros. Fuente: Manual de Derecho Constitucional. Oposición Acceso Carrera judicial y Fiscal, Carperi S.L, 2014. En cualquier caso, siguiendo a Bobbio, la citada Declaración "representa la conciencia histórica que la humanidad tiene de sus propios valores

injerencias arbitrarias en su vida privada, su familia, su domicilio, su correspondencia, ni ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (artículo 12 DUDH). Dicho precepto fue reproducido literalmente en el artículo 8 del Convenio Europeo de los Derechos Humanos de 1950 (CEDH, en adelante) y en el Pacto Internacional de los Derechos Civiles y Políticos (PIDCP, en adelante), de diciembre de 1966, en su artículo 17.1.

Por su parte, la Convención Americana sobre los Derechos Humanos o Pacto de San José de Costa Rica (CADH, en adelante), adoptada el 22 de noviembre de 1969 y en vigor el 18 de julio de 1978 - que instituyó la Corte Interamericana de Derechos Humanos (CIDH, en adelante) [25]-, reconoció el derecho a la intimidad de forma literal en su artículo 11: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Por último, sobre el concepto de protección de datos y su delimitación del derecho a la intimidad personal y familiar nos referiremos en detalle en el último apartado de este Capítulo I, el apartado 5, refiriéndonos en los siguientes a los principales hitos jurídicos del derecho a la protección de datos personales desde una perspectiva de Derecho Internacional (en el marco de la OCDE y de El Consejo de Europa), europeo (con especial referencia al RGPD) y en el ordenamiento jurídico español (con especial referencia a la LOPDGDD 3/18).

fundamentales en la segunda mitad del siglo XX. Es una síntesis del pasado y una inspiración para el porvenir; pero sus tablas no han sido esculpidas una vez y para siempre" en Román Díaz, M., "La Declaración Universal de los derechos del hombre y sus conceptos de libertad e igualdad: una aproximación axiológica desde el prisma Bobbiano", en *Revista de Ciencias Económicas*, núm. 29, 2011, pág.14.

[25]Véase el art. 33 CADH. La CIDH es Tribunal supranacional, con competencia consultiva y contenciosa, compuesto por siete jueces nacionales de los Estados miembros que supervisa la afinidad de CADH y los actos hechos y las normas estatales. Su jurisprudencia es creadora del concepto de «control de convencionalidad", por todas, se cita la Sentencia CIDH 2006, que significa que el poder judicial debe realizar el control entre normas jurídicas internas que aplican en casos concretos y la CADH. En cuando a la relación que mantienen la CIDH y el Tribunal Europeo de Derechos Humanos, es de un dialogo indirecto entre Tribunales. Tienen en común que nacen de Declaraciones de Derechos Humanos y tienen el mismo objeto de protección, pero son independientes. Por último, hay que señalar que la CIDH emite resoluciones efecto directo con capacidad de anular directamente la norma nacional y es el órgano de tutela en los casos afectan a sociedad en su conjunto por vulneración de derechos fundamentales.

C) Resultados.

Expuestas las nociones básicas sobre los derechos humanos y su proceso de reconocimiento, se ha evidenciado en primer lugar, que los conceptos “derechos humanos” y “derechos fundamentales” no son exactamente mismo (aunque en ocasiones se utilicen como sinónimos). Al hilo de lo anterior, se ha evidenciado que todos los derechos fundamentales son humanos, pero no al contrario; siendo los derechos humanos las facultades para las que desde finales del siglo XVII se generalizó la denominación de “humanos” al pertenecer y obligar a todos por igual, le son inseparables y deben estar siempre garantizados.

En segundo lugar, se ha evidenciado que, tras los procesos de reconocimiento de los derechos humanos de positivación, generalización e internacionalización, a los que posteriormente se añadió el de especialización, se ha demostrado que la evolución del reconocimiento de los derechos humanos, y en particular del derecho a la protección de datos personales, ha derivado de un progresivo desarrollo. Desarrollo que se prevé seguirá en adelante siguiendo la tendencia actual, en la que el avance de la digitalización genera retos y desafíos constantes en la tutela de la privacidad y el derecho a la protección de datos.

Adicionalmente, se ha constatado que el reconocimiento de un ámbito privado de la persona física susceptible de ser legalmente protegido frente a toda injerencia arbitraria no es esencialmente novedoso, sino que encontraría su origen hace más de setenta años en el marco del Derecho Internacional. Aunque, no fue hasta mediados de la segunda mitad del siglo XX, sobre la década de los ochenta, cuando el derecho a la protección de datos pasó a ser considerado un derecho o una facultad con sustantividad propia, independiente y autónomo del derecho a la intimidad personal y familiar. Así es como se considera actualmente, como se analizará en profundidad a lo largo de los siguientes apartados.

2. Principales hitos jurídicos sobre la protección de datos a nivel internacional en el marco de la OCDE y de El Consejo de Europa.

A modo de introducción, partiendo de las consideraciones preliminares del apartado anterior, cabe indicar que nos referirnos a continuación a los principales hitos jurídicos del derecho a la protección de datos personales desde una perspectiva de Derecho Internacional, en el marco de la OCDE[26] y de El Consejo de Europa (fundado por el Tratado de Londres en 5 de mayo de 1949) por su fundamental papel en el reconocimiento y la protección de los derechos humanos y en particular, del derecho sobre el que versa la presente tesis.

A) Principales hitos jurídicos sobre la protección de datos a nivel internacional en el marco de la OCDE.

En el seno de la OCDE, los hitos jurídicos que se considerarían de mayor relevancia en torno al tema objeto de estudio en investigación son los siguientes:

1º En primer lugar, las Directrices sobre Privacidad y Protección de datos publicadas en 1980 (DPPD o las Directrices de 1980, en adelante) que, en un panorama de diversidad legislativa nacional sobre protección de datos y privacidad (en la que mientras unos revisaban sus normativas nacionales sobre la materia, otros comenzaban a elaborar proyectos de leyes o no disponían de ninguna referente a protección de datos y privacidad), contribuyeron a unificar la regulación en cuanto a la protección de datos y privacidad en sus Estados Parte. Así, para resolver dicha disparidad legislativa[27] las DPPD partían de la consideración de que el principal efecto de la digitalización y el desarrollo del tratamiento de datos es permitir los flujos

[26] Además, la OCDE fue la impulsora de la Red Global de Autoridades de Protección de Datos.
[27] Lo que ya se entendía como un obstáculo directo y grave el libre flujo transnacional de datos- se encargó el año 1976 su elaboración a un grupo de expertos. Recuperado de: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (fecha de consulta: 2019).

transfronterizos de datos que contribuirían al desarrollo socioeconómico, pudiendo ser obstaculizados por la legislación local sobre la materia[28].

Las Directrices de 1980 configuraron unas normas mínimas básicas para la protección de la privacidad y las libertades individuales aplicables a los datos personales del sector público o privado que, por la forma en que son tratados, su naturaleza o el contexto en que se utilizan, representen un peligro para la privacidad y las libertades individuales[29]. También, son relevantes debido a que introdujeron en el plano internacional las definiciones de "controlador o inspector de datos"[30] (que equivaldría a la figura del responsable de tratamiento en la actual normativa europea sobre protección de datos); de "flujos transfronterizos de datos" como los movimientos o desplazamientos de datos personales más allá de las fronteras nacionales (que serían las denominadas en la normativa actual europea transferencias internacionales de datos personales); y de "datos personales", entendidos como "toda información relativa a un individuo identificado o identificable de una persona interesada".

Además, ya reflejaban una serie de principios básicos de privacidad y protección de datos de aplicación nacional e internacional, como a los principios de limitación de la recogida de datos personales[31]; de calidad del dato[32], de especificación de los fines[33] y de limitación del uso de los datos personales[34]. Adicionalmente, se refería a los

[28] En este punto, refleja que los Países Miembros debían tomar medidas oportunas y razonables para garantizar que los flujos transfronterizos de datos sean ininterrumpidos y seguros, así como evitar restringirlos con otros Países Miembros salvo si no cumplían sustancialmente las Directrices o si la reexportación de los datos pudiera transgredir su Ley nacional sobre privacidad.

[29] Se excluyen de su ámbito de aplicación aquellos datos que no representen "riesgo para la privacidad y las libertades individuales" y la aplicación sólo al tratamiento automático de datos personales.

[30] Por "controlador de datos" se entiende aquel que, según la ley nacional, "es competente para decidir sobre el uso y contenidos de los datos personales", independientemente de si son o no "recogidos, guardados, tratados o difundidos por esa persona o por un representante en su nombre".

[31] Por el que su recogida está sujeta a límites y han de obtenerse por medios legales y justos, y en su caso, con el conocimiento o consentimiento de su titular.

[32] Los datos deberían corresponder a los fines para los que se recogen y, en la medida en que sean necesarios para dichos fines, deberían ser concretos, completos y estar actualizados.

[33] Implica que se debe especificar en el momento de la recogida de los datos los fines concretos para los que son recopilados. De tal forma, su uso posterior estaría limitado al cumplimiento de esos fines o de otros compatibles con estos y, además, tienen que especificarse los fines cada vez que haya un cambio de finalidad.

[34] Significa que no se debe divulgar, poner a disposición, ni usarlos para fines que no sean los especificados según el principio anterior, excepto con el consentimiento de su titular o por imperativo legal; de salvaguarda de seguridad, por el que los datos deberían estar protegidos por medidas razonables de seguridad contra riesgos, tales como su pérdida o acceso no

principios de participación individual, por el que la persona debería tener derecho acceso, rectificación o supresión de los datos[35] (que equivaldrían a los derechos actuales en materia de protección de datos) y el principio de "responsabilidad", por el que a todo inspector o controlador de datos se le deberían exigir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios anteriores.

Como se verá más adelante con motivo del análisis de la normativa europea de protección de datos, prácticamente la mayoría de los citados principios se recogen la normativa actual europea, que entró en vigor y aplicación más de treinta años después, el 25 de mayo de 2018.

Otro punto interesante es que las Directrices de 1980 establecían el deber de los Países Miembros implementar los principios, establecer procedimientos o instituciones legales, administrativos u otro tipo para la protección de la privacidad y las libertades individuales con respecto a los datos personales. Así mismo, preveían que se debería aprobar una legislación nacional adecuada, fomentar y apoyar la autorregulación; facilitar los medios razonables para que las personas físicas ejerzan sus derechos; procurar las sanciones y soluciones adecuadas en caso de incumplimiento; y asegurarse de garantizar la no discriminación desleal e injusta contra los sujetos de los datos[36].

Sin embargo, su principal problemática radicaba en que no eran legalmente vinculantes, si no que configuraban unas normas mínimas susceptibles de ser

autorizado, destrucción, uso, modificación o revelación; de transparencia, por el que debería existir una política general de transparencia sobre el tratamiento, uso y las políticas con respecto a los datos personales. Este implica que deberían ponerse los medios para establecer la existencia y naturaleza de datos personales, así como los fines principales para los que se van a usar y la identidad y domicilio habitual del denominado controlador o inspector de datos.

[35] Implica conseguir, a través de un controlador o inspector de datos o de otro modo, la confirmación de si tiene o no datos que le conciernan; de que se le comuniquen tales datos en un plazo razonable, con una tarifa no excesiva, en su caso; de manera razonable y en la forma que pueda entender fácilmente. También, implica el derecho a que se le den razones en caso de denegación de solicitud, hecha conforme con lo anteriormente indicado, y de recurrir ese rechazo. Igualmente, implica el derecho de recusar los datos, y si la recusación tiene éxito, de que se borren, rectifiquen, completen o modifiquen.

[36] Por último, preveía que los Países Miembros han de "establecer procedimientos para facilitar el intercambio de información relacionada con las Directrices", darse ayuda mutua en los asuntos de investigación y procedimiento en relación con la materia; y trabajar en la elaboración de principios, nacionales e internacionales, que regulen la ley aplicable en el caso de flujos transfronterizos de datos personales Recuperado de http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowofpersonaldata.htm (fecha de consulta: 2018).

complementadas con medidas adicionales por los Estados.

Por último, cabe señalar que, fueron actualizadas posteriormente a través de la *Privacy* Guidelines *de 2013,* con la inclusión de nuevos conceptos como el de *accountability* o principio de responsabilidad proactiva, vigente en la actualidad y que significa que los controladores de datos o responsables del tratamiento de datos o aquellos que los traten, adopten programas de cumplimiento efectivo de la normativa sobre protección de datos. Así mismo, se añadieron el deber de notificación de las brechas de seguridad y el principio de cumplimiento. A mayor abundamiento, fue la primera vez en la que se incluyó la referencia a las denominadas Autoridades de Protección de datos personales (*Privacy Enforcement Authorities*)[37].

2º En segundo lugar, otro jurídico destacable a nivel internacional en el marco de la OCDE fue la promulgación de la Declaración de la OCDE sobre Flujos de Datos Transfronterizos de 1985, el 11 de abril del año 1985, que abordó cuestiones políticas en torno a los flujos transfronterizos de datos sobre actividades comerciales, intra empresariales, servicios de información informatizada e intercambios científicos y tecnológicos. Mediante esta Declaración, los Países Miembros de la OCDE reafirmaron su compromiso por desarrollar enfoques comunes ante las cuestiones de flujos de datos y de desarrollar soluciones armonizadas.

3º En tercer lugar, destaca la Declaración Ministerial sobre la protección de la privacidad en las redes globales, derivada de la Conferencia Ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en octubre de 1998 en Ottawa. Mediante esta Declaración los ministros reafirmaron su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

Además, expusieron que trabajarían para vincular los diferentes enfoques por los Países Miembros para asegurar la protección de la privacidad en las redes globales basándose en las DPPD y reflejaron su compromiso de proteger la privacidad en el

[37] Aunque esta actualización supuso la adaptación a la evolución de la sociedad tecnológica y a las nuevas realidades después de un transcurso de años desde su publicación, a raíz de los últimos acontecimientos, avances y de la modernización de las legislaciones sobre protección de datos personales y flujos transfronterizos de tales datos, sería conveniente una nueva actualización.

ámbito global, cooperando activamente con la empresa de la industria, la sociedad, los países no pertenecientes a la OCDE y otras Organizaciones internacionales. Ello, para valorar las tendencias económicas y tecnológicas clave que pueda afectar a la privacidad, desarrollando políticas exhaustivas y coherentes[38].

B) Principales hitos jurídicos sobre la protección de datos a nivel internacional en el marco de El Consejo de Europa.

1º En primer lugar, entre los principales hitos jurídicos en relación con el derecho a la protección de datos de carácter personal de la persona física y el derecho a la intimidad en el seno de El Consejo de Europa[39], destaca el citado CEDH o Convenio de Roma de 1950[40] que en su artículo 8.1 reconoció el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia a toda persona que se encuentre bajo su jurisdicción. Además, en su apartado segundo del mismo artículo 8 expresó de forma literal que: *"*no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[38]Conexionando lo anterior con la Agenda 2030 que contiene los 17 Objetivos de Desarrollo Sostenible (adoptada en septiembre de 2015 por líderes mundiales de las Naciones Unidas, instan países a iniciar esfuerzos por en los próximos 15 años: transformar el mundo actuales) versión ampliada de los 8 Objetivos de Desarrollo del Milenio de 2015, entre los que se encontraban lograr la educación básica para todos, promover la igualdad entre los sexos y el empoderamiento de la mujer, y lograr una sociedad global para el desarrollo; se puede afirmar que, en relación con la superación de la brecha digital por edad y por género, se va en el buen camino en la consecución de los Objetivos de Desarrollo Sostenible relacionados con la igualdad y no discriminación y crecimiento económico sostenido. En concreto, el Objetivo 5 sobre igualdad de género; el 8 sobre promover el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo y el trabajo decente para todos; y el 10 sobre reducir la desigualdad en los países y entre ellos. Relacionados con la transparencia y el acceso a la información pública, se traen a colación el Objetivo 16 en lo relativo a "crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas" y "Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales".

[39] En cuanto a su área de aplicación, mientras el Convenio 108 se ocupa del proceso automático de datos personales, las DPPD se aplican a los datos personales que implican peligros para la privacidad y las libertades individuales, con independencia de los métodos y la maquinaria utilizada en su tratamiento. En este sentido, se ha de entender que se aplica a los datos tratados por procesos automatizados como no automatizados, al igual que ocurre en la normativa actual europea, el RGPD[39].

[40] Ratificado por España en el año 1979.

2º En segundo lugar, resalta la Resolución nº 428 (1970) de la Asamblea Parlamento del Consejo de Europeo porque definió el conjunto de manifestaciones de la intimidad o privacidad como "el derecho de vivir la vida de cada uno con un mínimo de interferencia. Comprende la vida privada familiar, la vida en el domicilio, la integridad física y oral, el honor, la reputación, el evitar ser colocado bajo una falsa luz, la no revelación de hechos irrelevantes o embarazosos, la publicación no autorizada de fotografías privadas, así como la protección de la divulgación dada y recibida por el individuo de manera confidencial".

3º En tercer lugar, destacan las Resoluciones de los años 1973 y 1974 por el Comité de Ministros del Consejo de Europa sobre a la protección de la privacidad de los particulares frente a los bancos de datos electrónicos en los sectores público y privado respectivamente, que recomendaron "que los gobiernos de los estados miembros del Consejo de Europa tomarán medidas para la aplicación de ciertos principios básicos de protección relativos a la obtención de datos, la calidad de los datos y los derechos de los particulares a ser informados sobre los datos y las actividades de proceso de los mismos"[41].

4º Otro hito jurídico fundamental en este ámbito fue la publicación del Convenio 108/81 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108, en adelante), ratificado en Estrasburgo con fecha 28 de enero de 1981, en vigor el 1 de octubre de 1985[42]. El Convenio 108 destaca por su pretensión de unir aún más a sus Países Miembros, basándose en el respeto de la preeminencia del derecho, los derechos humanos y las libertades fundamentales, con el objeto de garantizar en los Estados Parte y a cualquier persona física, independientemente de su nacionalidad o residencia, el respeto de estos y concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona[43].

[41] Recuperado de: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (fecha de consulta: 2019).
[42] España lo ratificó con fecha el 27 de enero de 1984, entrando en vigor el 1 de octubre de 1985 y publicado en el Boletín Oficial del Estado (BOE en adelante) de 15 de noviembre de 1985. Recio M., "Día de la Protección de Datos: El Convenio 108 y tus datos personales". Recuperado de: http://www.lawyerpress.com/blogs/LPe_Miguel_Recio_11.html (fecha de consulta: 2018).
Recuperado de: http://www.lawyerpress.com/blogs/LPe_Miguel_Recio_11.html (fecha de consulta: 2018).
[43] En su Preámbulo reconoce que la protección de tales derechos y las libertades merece ser ampliada, especialmente el derecho al respeto de la vida privada, "teniendo en cuenta

Respecto a su ámbito de aplicación, mientras que las mencionadas Directrices de 1980 se aplicaban a los datos personales que implicasen "peligros para la privacidad y las libertades individuales", con independencia de los métodos y la maquinaria utilizada en su tratamiento; el Convenio 108 resulta aplicable tanto a los datos tratados por procesos automatizados como a los no automatizados , en el mismo sentido que la normativa actual europea, el RGPD, que otorga lo que se denomina una protección "tecnológicamente neutra"[44].

De otro lado, al igual que ocurría con las Directrices de 1980, el Convenio 108 también contenía definiciones básicas, muchas de cuales mantienen su vigencia en la actualidad, como las de "dato de carácter personal"; fichero automatizado (entendido como cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado), "tratamiento automatizado" (entendido como las operaciones de registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión; ellas efectuadas total o parcialmente con ayuda de procedimientos automatizados) y "autoridad controladora[45]". Así mismo, el Convenio 108 también consagraba una serie de principios básicos para la protección

intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Reafirmando al mismo tiempo su compromiso a favor de la libertad de información sin tener en cuenta las fronteras; reconociendo le necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos". Recio M., "Día de la Protección de Datos: El Convenio 108 y tus datos personales". Recuperado de: http://www.lawyerpress.com/blogs/LPe_Miguel_Recio_11.html (fecha de consulta: 2018).

[44] A modo de comparativa entre las DPPD y el Convenio 108 sobre protección de datos del Consejo de Europa, aunque tienen en común que se refieren a la protección de datos personales, tanto los principios de protección como los detalles propuestos por ambos organismos no son idénticos. La terminología empleada difiere en algunos aspectos y el marco institucional para la cooperación continua se trata con más detalle en el Convenio del Consejo de Europa que en las DPPD. Recuperado de: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (fecha de consulta: 2018).

[45] Entendida como la "persona física o jurídica, autoridad, servicio y cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán".

de datos (como los de calidad del dato[46], de garantías apropiadas[47], de seguridad de los datos[48] y de garantías complementarias para la persona, configurando estos últimos los derechos actuales en materia de protección de datos[49]) similares a los vigentes en la actualidad, para cuya eficacia se preveía que las partes tomarían en su derecho interno las medidas necesarias.

Adicionalmente, el Convenio 108 reguló también los flujos transfronterizos de datos personales estableciendo disposiciones aplicables a las transmisiones a través de las fronteras nacionales por cualquier medio, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento. Otro punto relevante es que en materia de sanciones el Convenio 108 preveía que cada parte se comprometía a establecer las sanciones y los recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos de protección de datos. Finalmente, establecía una regla de colaboración entre las Partes, que se obligaron a concederse mutuamente asistencia para el cumplimiento del Convenio[50].

[46] Significa que los datos personales que sean objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con las mismas; serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; serán exactos y si fuera necesario actualizados; y se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

[47] Preveía mayores garantías para los datos de carácter especial que revelen origen racial, las opiniones políticas, las convicciones religiosas u otras, así como los datos de carácter personal relativos a la salud o a la vida sexual, a los que se incluía en caso de datos personales referentes a condenas penales. Se impedía su tratamiento salvo que el derecho interno prevea garantías apropiadas.

[48] Dispone que se tomarán medidas se seguridad apropiadas para la protección de datos personales registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

[49] Este último implica que por el que cualquier persona deberá poder a) conocer la existencia de un fichero automático de datos personales, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del mismo; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos personales que conciernan a dicha persona, así como la comunicación de dichos datos en forma intangible; c) obtener, llegado el caso, la rectificación o borrado de dichos datos cuando se hayan tratado con infracción de las disposiciones del Derecho interno que hagan efectivos los principios básicos del Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere e caso, de comunicación, ratificación o de borrado.

[50] A tal fin, preveía que cada parte designará a una o más autoridades cuya denominación y dirección comunicará al secretario general del Consejo de Europa. Cada parte que haya designado a varias autoridades indicará en la comunicación la competencia de cada una de dichas autoridades. Una autoridad designada por una parte, a petición de una autoridad

En último lugar, cabe señalar que, años después y ante el aumento de los intercambios de datos personales a través de las fronteras nacionales, el Convenio 108 fue actualizado mediante la publicación del Protocolo adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos, con objeto de garantizar la protección efectiva de los derechos humanos y las libertades fundamentales, y en particular el derecho a la intimidad en relación con dichos intercambios de datos personales. Dicho Protocolo Adicional estuvo abierto a la firma el 8 de noviembre de 2001 y obligaba a las Partes a crear Autoridades de Control que ejercieran sus funciones con total independencia, lo que constituía un elemento de protección efectiva de las personas en lo que respecta al tratamiento de datos personales[51].

C) Resultados.

Con la exposición de los principales hitos jurídicos en materia de derecho a la intimidad y protección de datos personales en el marco internacional, en el marco de la OCDE y de El Consejo de Europa, se ha evidenciado, en primer lugar, que en plano internacional existía ya, a finales del siglo XX, el reconocimiento expreso del derecho a la protección de datos personales de la persona física. Así como también, el reconocimiento de similares principios y definiciones básicas en materia de protección de datos, tal y como se entienden en la actualidad en la normativa europea de protección de datos, aunque de una forma más desarrollada.

En segundo lugar, se ha constatado la existencia de una preocupación a nivel internacional, no solo por la protección de la privacidad y de la información personal de los ciudadanos, sino también por la importancia de no limitar los flujos transfronterizos de datos, de la cooperación internacional, la colaboración en la

designada por otra parte: Facilitará informaciones acerca de su derecho y su práctica administrativa en materia de protección de datos; Tomará toda clase de medidas apropiadas, con arreglo a su derecho interno y solamente a los efectos de la protección de la vida privada, para facilitar informaciones fácticas relativas a un tratamiento automatizado determinado efectuado en su territorio con excepción, sin embargo, de los datos de carácter personal que sean objeto de dicho tratamiento (art. 13).

[51] Al igual que ocurrió con las DPPD, el Convenio fue actualizado en 2018, comúnmente conocido como Convenio 108+ “plus”, ha sido pieza clave para los desarrollos normativos a nivel internacional y europeo en esta materia. Recuperado de: https://rm.coe.int/la-convention-108-visual/1680981499 (fecha de consulta: 2019) y https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (fecha de consulta: 2019).

protección de la privacidad y en la elaboración de principios comunes (lo que va en consonancia con la voluntad armonizadora de las normas que se han publicado posteriormente). Por último, se ha constatado el papel fundamental de la OCDE y de El Consejo de Europa en el reconocimiento y la protección de los derechos humanos y en particular, del derecho sobre el que versa la presente tesis.

3. Principales hitos jurídicos sobre la protección de datos a nivel europeo, con especial referencia al RGPD.

A modo de introducción, se ha de partir de la premisa de que, como es sabido, en el marco normativo de la Unión Europea o UE coexisten el sistema de protección del Derecho Internacional y el sistema de protección supranacional del modelo europeo, donde a su vez coexisten la tutela por el Consejo de Europa y por la Unión Europea; y, además, existe la legislación nacional de cada uno de los Estados Miembros de la UE (España, Francia, Italia, Alemania, Portugal, etc.). Aunque a *prima facie* puedan parecer niveles de protección de derechos independientes, forman parte de un todo y la visión ha de ser panorámica e interrelacionada.

Así, en ámbito comunitario rigen los principios de primacía del Derecho Comunitario o europeo sobre el derecho interno y de armonización, según el cual los jueces van a aplicar la doctrina del Tribunal Europeo de los Derechos Humanos (TEDH, en adelante) sin necesidad de que sea recibida por los Tribunales Constitucionales, lográndose un entendimiento común de *ius commune* de los derechos humanos proclamados constitucionalmente en Europa.

No obstante, consecuencia de la globalización y la internacionalización, la sociedad actual no podría modelarse únicamente en el ámbito nacional, sino que responde a reglas que son globales y supraconstitucionales. De ahí, que puedan ser frecuentes las divergencias en aspectos como la aplicación o la interpretación de las mencionadas reglas supranacionales. A pesar de ello, la UE es considerada pionera en el reconocimiento de derechos, siendo incluso modelo de referencia o inspirador en otros sistemas de protección, como ocurre con la regulación europea en materia de protección de datos, en la que la normativa europea se considera actualmente la más restrictiva y garantista.

A) Principales hitos jurídicos en ámbito europeo en materia de protección de datos con carácter previo a referirnos al RGPD.

Con carácter previo a referirnos al RGPD, que constituye la actual normativa europea de protección de datos, interesa mencionar los principales hitos jurídicos en ámbito europeo en materia de protección de datos, derecho que ya era reconocido en otros textos de derechos anteriores, como se viene manteniendo a lo largo del presente Capítulo.

1º En primer lugar, el derecho a la protección de datos se reconocía en la Carta de Derechos Fundamentales de la Unión Europea de 2007 (Carta de Derechos Fundamentales de 2007, en adelante), proclamada en Niza en diciembre del año 2000, y posteriormente adjuntada al Tratado de Lisboa firmado en 2007, en vigor desde 2009, cuando reconocía de forma literal:

> "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente" (artículo 8).

2º En segundo lugar**,** el Tratado de Funcionamiento de la UE (TFUE, en adelante) también reconocía el derecho protección de datos al expresar, de forma literal:

> "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", precisando que "El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes" (artículo 16).

3º En tercer lugar, resaltan años después la publicación de la *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (Directiva 95/46/CE, en adelante), predecesora al RGPD y derogada por este por lo que nos centraremos a continuación en el análisis de la normativa vigente en la época actual.

De otro lado, y en conexión con la anterior, destaca el *Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos* (Reglamento nº 45/2001, en adelante).

4º En cuarto lugar, se considera necesario mencionar la *Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos* (Directiva 2016/680, en adelante).

Esta Directiva fue publicada a la vez que el RGPD, sin embargo, no se transpuso en España hasta varios años después de haber transcurrido el plazo establecido al efecto, lo que generó una sanción económica. En concreto, su transposición al ordenamiento jurídico español fue mediante la *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*[52] (Ley Orgánica 7/2021, en adelante).

[52] Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806 (fecha de consulta: 2023).

B) Especial referencia al RGPD, la normativa vigente sobre protección de datos.

Actualmente, el RGPD desde su entrada en vigor configura la normativa básica de aplicación directa en la UE, sobre la que en este apartado vamos a referirnos a sus puntos más relevantes, toda vez que su estudio y análisis puede por sí misma generar otra tesis independiente e incluso el estudio de cada uno de sus apartados pueden engendrar una investigación por separado.

Como se ha indicado anteriormente, el RGPD derogó la Directiva 95/46/CE que regulaba la protección de datos personales en el ámbito europeo (aunque requería transposición nacional para su aplicación)[53], entrando en vigor y aplicación desde el 25 de mayo de 2018, si bien ya era directamente aplicable y obligatorio en todos sus elementos desde su entrada en vigor desde el 25 de mayo de 2016.

Compuesto por una extensa Parte Preliminar, 173 Considerandos, 11 Capítulos, y un total de 99 artículos, el RGPD fue creado con objeto de regular las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento[54] de datos personales[55] y las normas relativas a la libre circulación de tales datos"[56]; eliminando obstáculos a la circulación de datos personales en la UE, facilitando la libre circulación dentro esta y la transferencia a terceros países y organizaciones internacionales. Lo anterior, garantizando al mismo tiempo un elevado nivel de protección de los datos mediante un marco más sólido y coherente para la protección de datos, respaldado

[53] Adsuara Varela, B., "El nuevo Reglamento General de Protección de Datos", Lid Learning: Nuevo RGPD. Recuperado de: https://www.youtube.com/watch?v=U2thY0yEsIE (fecha de consulta 2020).
[54] Es "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (Art. 4. 2 RGPD).
[55] Por dato personal se entiende "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (art. 4. 1 RGPD).
[56] Véanse los Considerandos nº 2 y nº 4 RGPD.

por una ejecución estricta[57]. No obstante, la realidad es que al prever en parte de su articulado la posibilidad de que los Estados mantengan o introduzcan disposiciones más específicas a fin de adaptar la aplicación de sus normas, se ha evidenciado que genera consecuentemente la no existencia de forma absoluta y plena de la homogeneidad y armonización por él mismo pretendida.

Dicho esto, junto con el RGPD, en el ordenamiento jurídico español, también conforma la normativa de protección de datos la LOPDGDD 3/2018 que vino a actualizar la anterior normativa a la luz del RGPD y que es objeto de análisis en el siguiente apartado. De otro lado, se considera de gran relevancia tener en cuenta además las resoluciones, informes, circulares, respuesta del Gabinete Jurídico a consultas entre otros recursos que tienen las Autoridades de Control europeo y el Comité Europeo de Protección de Datos (CEPD o EDPB por sus siglas en inglés) y el Supervisor Europeo de Protección de Datos, que vienen a aclarar, matizar o interpretar el articulado de la normativa.

Partiendo de lo anterior, a continuación, se destacan de forma resumida las principales particularidades del RGPD, pues la presente tesis no tiene por objeto reflejar un análisis pormenorizado de esta normativa, que ya ha sido objeto de numerosos estudios (aunque como se ha puesto de manifiesto cualquiera de los aspectos que regula el RGPD puede por si originar un investigación y tesis en sí mismo).

Es decir, se parte en la presente tesis del RGPD para investigar sobre la unidad temática, que recordamos versa sobre la proyección del derecho a la protección de datos en las áreas de convergencia con otros derechos fundamentales, lo que se considera de contenido más innovador y de mayor implicación práctica.

[57] En este sentido, establece que “la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales”. Además, es una exigencia del buen funcionamiento del mercado interior, tal y como expone el Considerando nº 13 RGPD, al que nos remitimos.

Pues bien, en virtud de lo anterior, las diez particularidades a las que nos referiremos sobre el **RGPD,** se mencionan y desarrollan brevemente a continuación:

1. **Aplicabilidad directa del RGPD**
2. **Ámbito de aplicación**
3. **Principios básicos de tratamiento de datos. Responsabilidad proactiva - accountability**
4. **Tutela especial sobre las categorías de datos especiales y tratamientos de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas**
5. **Derechos de los interesados.**
6. **Roles del tratamiento de datos y medidas técnicas y organizativas**
7. **Brechas de seguridad**
8. **La figura del Delegado de Protección de Datos (DPD o DPO)**
9. **Transferencias internacionales de datos**
10. **Cambio en el régimen sancionador**

1. **Aplicabilidad directa del RGPD:** una de las principales particularidades del RGPD es su **aplicabilidad directa**, lo que la diferencia de la anterior Directiva 95/46/CE que derogó, que sí requería de transposición estatal a los ordenamientos jurídicos nacionales produciendo una aplicación fragmentada en la UE, con diferentes niveles de protección de este derecho y, por ende, un elevado nivel de inseguridad jurídica. En el caso de España, su transposición se produjo mediante la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD 15/1999, en adelante), junto al *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. Actualmente, ambas normativos fueron derogados por la LOPDGDD 3/18, la vigente normativa de protección de datos en España que, como se verá en el siguiente apartado, fue modificada a mediados de 2023 en algunos preceptos.

2. **Ámbito de aplicación:** el RGPD resulta aplicable al tratamiento total o parcialmente automatizado de datos personales de las personas físicas, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero[58]. Es decir, el RGPD otorga una protección "tecnológicamente neutra", concediendo la tutela únicamente a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales"[59].

   Además, el RGPD prevé su aplicación al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la Unión Europea o no[60]. Así, se aplicaría al tratamiento de datos personales de interesados que residan en la UE (por ejemplo, España o Francia) por parte de un responsable o encargado no establecido en la Unión (por ejemplo, Brasil o México), cuando los tratamientos estén relacionados con:

   i) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
   ii) el control de su comportamiento, en la medida en que este tenga lugar en la UE[61].

[58] Define Fichero como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" (art. 4.6 RGPD). En cuanto al ámbito de aplicación, véase el artículo 2 RGPD.
[59] No se regula el tratamiento de datos relativos a personas jurídicas y, en particular, a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto. Tampoco, a la protección de datos personales de personas fallecidas, quedando su regulación competencia de los Estados miembros (Considerando nº 27 RGPD).
[60] Según el art. 4 RGPD, "responsable del tratamiento" es la "persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros. El encargado del tratamiento o encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Considerando nº 22 RGPD: "Todo tratamiento de datos en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto".
[61] Véanse los Considerandos nº 23 y nº 24 RGPD.

Como excepciones, el RGPD no resultaría de aplicación en algunos supuestos en él mismo previstos, como al tratamiento de datos en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la UE;[62] o en el ejercicio de actividades exclusivamente personales o domésticas[63] (como puede ser los tratamientos de datos personales en la organización de un evento privado o una boda). Tampoco se aplicaría por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[64], pues tiene su propia regulación, como se ha indicado anteriormente, (Directiva 2016/680 y la Ley Orgánica a la que ha sido transpuesta en cada Estado).

Aparte se ha de tener en cuenta que el citado Reglamento nº 45/2001 se aplicaría respecto al tratamiento de datos por parte de las instituciones, órganos y organismos de la Unión; que junto con actos jurídicos de la Unión se adaptarán a los principios y normas del RGPD[65].

3. **Principios relativos al tratamiento de datos. Responsabilidad proactiva - accountability:** el RGPD establece una serie de principios básicos de aplicación a toda información relativa a una persona física "identificada o identificable", teniendo en cuenta el concepto de dato personal. Con carácter general, los principios básicos se reconocen en su artículo 5 (como el de licitud, limitación del

[62] Como, por ejemplo, la seguridad nacional, según el Considerando nº 16 RGPD.
[63] Según el Considerando nº 18 RGPD, "entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas".
[64] En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, prevé que los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar su aplicación, que pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión.
[65] Véase el Considerando nº 17 RGPD. Además, el RGPD se entendería sin perjuicio de la aplicación de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de ocho de junio de 2000, relativa a determinados aspectos verídicos de los servicios de la sociedad de información, en particular, el comercio electrónico, en el mercado interior, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios derivadas del reconocimiento de derechos de interesados.

plazo de conservación o el de limitación de la finalidad), aunque existen otros reconocidos a lo largo de su articulado que es necesario garantizar y cumplir, como el de responsabilidad proactiva o *accountability* o el de protección de datos desde el diseño y por defecto. A continuación, se hace mención de forma resumida a los principios más relevantes:

3.1. Principio de licitud, lealtad y transparencia: supone que todo tratamiento de datos personales de la persona física ha de respetar los principios de licitud, lealtad, transparencia en relación con el interesado[66], considerando un tratamiento licito o legítimo aquel que cumple, al menos, una de las siguientes condiciones (las bases de legitimación del artículo 6.1 RGPD):

i) El interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos (ejemplo. Envío de comunicaciones comerciales), con las condiciones previstas en el artículo 4 RGPD[67], esto es, que sea una manifestación de voluntad libre, específica informada e inequívoca, lo que supuso la necesidad de la realización de una "reconversión" de todo consentimiento tácito a expreso.

Además, si el consentimiento expreso no se ha documentado por el responsable del tratamiento por cualquier medio que evidencie que el interesado lo ha prestado de forma válida, pasa a considerarse como si no se hubiese tenido lugar[68]. Por tanto, se exige que el responsable de tratamiento debe ser capaz de demostrar que el interesado consintió el tratamiento (artículo 7 RGPD).

[66] Véanse los Considerandos nº 39, 40, 41, 44 y 46 RGPD. Respecto a los principios de tratamiento leal y transparencia, y los Considerandos nº 58 y 60 RGPD.
[67] Es toda manifestación de voluntad libre, especifica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Hay que señalar que el responsable del tratamiento deber ser capaz de demostrar que ha dado su consentimiento (Considerando nº 42 RGPD).
[68] Adsuara Varela, B. "El nuevo Reglamento General … (op. Cit. Nota 53).

De otro lado, si el consentimiento se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se ha de presentar de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

Algo que es esencial y es que incluye el derecho del interesado a retirar su consentimiento en cualquier momento, del que debe ser informado antes de otorgarlo y que no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada, debiendo ser tan fácil darlo como retirarlo para el interesado[69].

En palabras de la AEPD[70]: "(…). El consentimiento se entiende como un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernan, prestada con garantías suficientes para acreditar que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. Y debe darse para todas las actividades de tratamiento realizadas con el mismo o mismos fines, de modo que, cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos de manera específica e inequívoca, sin que pueda supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de sus datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación negocial. A este respecto, la licitud del tratamiento exige que el interesado sea informado sobre los fines a que están destinados los datos (consentimiento informado).
El consentimiento ha de prestarse libremente. Se entiende que el consentimiento no es libre cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su

[69]Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. Véanse los Considerandos nº 32 y 33 RGPD sobre el consentimiento.
[70] Recuperado de: https://www.aepd.es/documento/ps-00078-2021.pdf (fecha de consulta 2024).

consentimiento sin sufrir perjuicio alguno; o cuando no se le permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato o prestación de servicio sea dependiente del consentimiento, aun cuando éste no sea necesario para dicho cumplimiento. Esto ocurre cuando el consentimiento se incluye como una parte no negociable de las condiciones generales o cuando se impone la obligación de estar de acuerdo con el uso de datos personales adicionales a los estrictamente necesarios.
Sin estas condiciones, la prestación del consentimiento no ofrecería al interesado un verdadero control sobre sus datos personales y el destino de los mismos, y ello haría ilegal la actividad del tratamiento (…)".

Respecto al consentimiento de los menores de edad, se prevé que, en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos de un niño se considerará licito cuando tenga como mínimo 16 años. Si es menor de 16 años, tal tratamiento únicamente lo será si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela, y solo en la medida en que se dio o autorizó.

No obstante, se posibilita a que los Estados miembros establezcan una edad inferior a tales fines, siempre que esta no sea inferior a 13 años[71], lo que configura uno de los asuntos en que se evidencia que, aunque nació con vocación armonizadora, permite particularidades mediante la determinación o

[71] Se trae a colación al respecto el Considerando nº 38 RGPD que considera que los niños merecen una protección especifica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección especifica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños. Desde la Declaración de los Derechos del Niño (20 de noviembre de 1959), reconoce, con el consenso internacional unánime por los 78 Estados miembros de la ONU, los principios fundamentales de los derechos del niño y sus derechos.

particularización a la legislación nacional. De hecho, en España, la edad se estableció en 14 años, pero en otros países se optó por otra edad dentro de la franja prevista por el RGPD, como ocurre en Francia que se estableció en 15 o en Portugal que se estableció en 13 años, el mínimo permitido.

En este punto, se pone en evidencia la necesidad de una especial protección homogénea en relación con los menores de edad en todos los ámbitos y en particular respecto a la edad de validez de su consentimiento. Ello, junto a una mayor atención y tutela por ser considerados menos conscientes de los riesgos a los que están expuestos, las consecuencias, así como de las garantías y derechos en materia de protección de datos, especialmente cuando vayan a ser tratados sus datos con finalidades relacionadas con la mercadotecnia[72].

ii) La segunda base de legitimación de un tratamiento es que el tratamiento sea necesario para la ejecución de un **contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales**;

[72] La Mercadotecnia es un proceso social y administrativo mediante el cual, grupos e individuos obtienen lo que necesitan y desean a través de generar, ofrecer e intercambiar productos de valor con sus semejantes. Se trata de entender todo lo que hay detrás de una venta, para motivarla e incentivarla. Recuperado de: https://www.rdstation.com/blog/es/mercadotecnia/#:~:text=La%20Mercadotecnia%20es%20un%20proceso,venta%2C%20para%20motivarla%20e%20incentivarla (fecha de consulta: 2022). Al hilo de lo anterior, resalta el Principio Segundo de la Declaración de los derechos del niño de 1959 reconoce el derecho del niño a una protección especial para el desarrollo físico, mental y social. Esta especial protección se traducirá en el establecimiento un régimen específico cuando los titulares de los datos personales son menores de edad, como ocurre la actual regulación sobre la protección de los datos personales. El Principio Tercero prevé el derecho a un nombre y a una nacionalidad desde su nacimiento, datos personales a los que en la regulación sobre datos personales se les dará una protección específica y extraordinaria. El Principio Séptimo regula el derecho a "recibir educación, que será gratuita y obligatoria por lo menos en las etapas elementales. Se le dará una educación que favorezca su cultura general y le permita, en condiciones de igualdad de oportunidades, desarrollar aptitudes y su juicio individual, su sentido de responsabilidad moral y social y llegar a ser un miembro útil de la sociedad".

iii) Otra base de legitimación es que el tratamiento sea necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento[73];

iv) Que el tratamiento sea necesario para proteger **intereses vitales del interesado o de otra persona física**;

v) Que el tratamiento sea necesario para el **cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento;

vi) Que el tratamiento sea necesario para la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Esto no será de aplicación al tratamiento realizado por las autoridades en el ejercicio de sus funciones"[74].

El cumplimiento del principio de licitud, es decir que el tratamiento se base en una o varias de las citadas bases de legitimación es esencial, toda vez que todo tratamiento de datos personales ha de ser legítimo y debería basarse, al menos, en uno de los supuestos anteriores, pudiendo concurrir en el mismo tratamiento más de una base de legitimación. De hecho, la identificación de la base de legitimación es uno de los puntos que deben de estar reflejados en el Registro de Actividades del Tratamiento o "RAT" o RPA por sus siglas en inglés, en relación con cada tratamiento que se incluye en el mismo de conformidad con el artículo 30 RGPD (junto como otras como las categorías de datos tratados, la finalidad o el responsable de tratamiento).

[73] Véase el Considerando nº 45 RGPD.

[74] Ahora bien, el RGPD prevé (art. 6.2) la posibilidad de que los Estados mantengan o introduzcan disposiciones más específicas a fin de adaptar la aplicación de sus normas o con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento licito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX." 6.3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por el Derecho de la Unión, o el Derecho de los Estados miembros que se aplique al responsable del tratamiento. Véanse los Considerandos nº 31, 40 y 41 RGPD.

También es clave el deber de información en relación con la base de legitimación, relacionado también con los principios de lealtad y de transparencia, que supone que se ha de dar la información al interesado de forma comprensible, clara y de forma transparente.

A modo ilustrativo de la importancia de detectar la base de legitimación de un tratamiento que se pretende realizar, se trae a colación un caso relativamente reciente en el que la AEPD impuso una sanción a un gimnasio por un importe de 27.000 euros por imponer como requisito a los usuarios el acceso a sus instalaciones mediante su huella dactilar. Aunque no entra a la valorar la necesidad, sí enmarca falta de consentimiento explícito, información suficiente en la política de privacidad, conservación del patrón de huella por tiempo excesivo, base de legitimación mal elegida, finalidad no concretada, ausencia de mención a decisiones automatizadas, falta de concordancia entre las finalidades declaradas en la política de privacidad, el contrato de socio del gimnasio, el RAT y la evaluación de impacto o EIPD, entre otras[75].

3.2. **Principio de limitación de la finalidad:** implica que los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. Aunque, el tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considera incompatible con los fines iniciales[76], por lo que estaría permitido. Por ejemplo, si se recoge un dato con la finalidad exclusiva de gestionar la relación laboral o un contrato de prestación de servicios, no se podría utilizar para una finalidad distinta, como el envío de publicidad propia o de terceros.

A modo ilustrativo, se hace referencia a una Resolución de la AEPD que impuso la sanción de 30.000 euros[77] y la adopción de las medidas

[75] Recuperado de: https://www.aepd.es/documento/ps-00413-2022.pdf (fecha de consulta:2024).
[76] Según el art. 4 RGPD: limitación del tratamiento es el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
[77] Recuperado de: https://www.aepd.es/documento/ps-00078-2021.pdf, (fecha de consulta: 2024).

necesarias para adecuar su actuación a la normativa de protección de datos personales a un establecimiento hotelero por una reclamación por escanear el pasaporte de un cliente (incluida la fotografía) y utilizarlo para evitar un uso fraudulento de la tarjeta de consumo interno del hotel, comprobando y verificando la identidad del cliente al realizar cargos en la cuenta de su habitación con el objetivo de no causar un perjuicio económico a los clientes.

En el caso en cuestión, la AEPD aclaró que, aunque los alojamientos turísticos deben registrar datos de los documentos de identificación de sus clientes para cumplir las normas españolas sobre registros de viajeros y comunicarlos a las Fuerzas y Cuerpos de Seguridad en cumplimiento de la normativa de seguridad ciudadana, la recogida y utilización de la fotografía supone un tratamiento de datos personales innecesario y desproporcionado para la finalidad establecida. Además, la AEPD interpretó que el establecimiento hotelero sancionado también recogía y utilizaba las fotografías de los clientes para el control de acceso y la facturación de sus consumos durante su estancia. No se incluía ningún detalle sobre la recogida y utilización de la fotografía, por lo que los clientes las desconocían. Tampoco se recogía este tratamiento en su Registro de Actividades de Tratamiento. Todo ello, llevó a la imposición de la sanción al establecimiento.

3.3. Principio de minimización de datos: la minimización implica que los datos personales a tratar serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, es decir, que los datos a tratar sean los estrictamente necesarios para la finalidad para la que se recaban. Por ejemplo, para realizar una compraventa física de un libro no se considera estrictamente necesario pedir datos personales o datos de carácter sensibles, como la dirección de correo, la matrícula de vehículo o el código postal.

A modo ilustrativo, se hace referencia a la Resolución de la AEPD en la que la que consideró que la petición de documentación completa relativa a la discapacidad y tarjeta acreditativa de persona con discapacidad” que la

reclamada formuló a la parte, "no puede considerarse adecuada, pertinente y limitada a lo necesario con relación a los fines para los cuales los datos contenidos en dicha documentación son "tratados. Primero, justificó que *"(…) no puede solicitarse a los participantes en los programas de empleabilidad de (…), datos personales que no son necesarios en el momento de su recogida, ni son pertinentes con el tratamiento cuestión, debiendo ser limitados a lo necesario para la formación y la posterior contratación. En consecuencia, no pueden recogerse datos personales sin que exista la causa que habilite al responsable del tratamiento en el momento en que éste se produzca".* Segundo, concluyó que la petición de *"documentación completa relativa a la discapacidad y tarjeta acreditativa de persona con discapacidad" que (…) formuló a la parte reclamante, no puede considerarse adecuada, pertinente y limitada a lo necesario con relación a los fines para los cuales los datos contenidos en dicha documentación son tratados"*[78].

3.4. Principio de exactitud: significa que los datos serán exactos y, si fuera necesario, actualizados (ejemplo, cambio de dirección de notificaciones o de contacto); siendo preciso adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos que sean inexactos con respecto a los fines para los que se tratan.

Al respecto de este principio, resulta ilustrativa la Resolución de la AEPD en la que desestima un recurso de reposición interpuesto por la reclamada pues consideraba que *"el reclamado ha vulnerado el artículo 5.1.d), principio de exactitud, en relación con el artículo 5 de la LOPGDD, Exactitud de los datos, al ser cedidos los datos de la reclamante a un tercero, adquiriente del crédito, quien a su vez los incluyo en el fichero ASNEF*[79]*, vinculados a una deuda sobre la que existía contienda judicial y cuyo Auto posterior declaró que contenía intereses abusivos, por lo que no existía certeza sobre la misma debiendo ser recalculada. En relación con el citado artículo y su actualización (que sería la manifestación del principio de exactitud que se entiende incumplido), exige que se adopten "las medidas*

[78] Recuperado de: https://www.aepd.es/documento/ps-00529-2023.pdf (fecha de consulta: 2024).
[79] Asociación Nacional de Establecimientos Financieros de Crédito.

razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan"[80].

3.5. Principio de limitación del plazo de conservación[81]**:** se trata de un principio especialmente relevante pues implica que los datos personales han de ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento. Aunque como no se establecen plazos concretos por parte del RGPD el responsable de tratamiento es quien debe determinar los plazos de conservación y los mecanismos adecuados de bloqueo y destrucción, o el empleo de técnicas para garantizar su protección.

No obstante, la realidad es que, actualmente, y derivado de la tradición anterior de guardar y conservar toda la documentación, se ha evidenciado que existe una tendencia a guardar toda la documentación y los datos sin plazo ni control, lo que no sería conforme con el RGPD. De hecho, el artículo 11 RGPD dispone que, si los fines para los que un responsable trata datos no requieren o ya no requieren la identificación de un interesado, el responsable no estaría obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el RGPD[82].

[80] Recuperado de: https://www.aepd.es/doc.nto/reposicion-ps-00053-2023.pdf (fecha de consulta: 2024).

[81] Al respecto, el Considerando nº 39 RGPD continua: Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

[82] Según el Considerando nº 57 RGPD, si los datos personales tratados por un responsable no le permiten identificar a una persona física el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo, mediante un mecanismo de autentificación como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

No obstante, es cierto que el RGPD permite que los datos puedan conservarse los datos durante periodos más largos en ciertos casos, como ocurre siempre que se traten exclusivamente con los citados fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Lo anterior, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades del interesado.

Este principio tiene una gran relevancia a la vez que puede presentar dificultades al llevarlo a la práctica de las organizaciones, generándose también disparidad de criterios según las legislaciones nacionales que se tengan en cuenta para el establecimiento de plazos. Por ejemplo, en la legislación nacional española se prevén unos determinados plazos de prescripción de acciones, de caducidad de acciones distintas en la legislación civil, mercantil, laboral, fiscal que habrán de ser tenidas en cuenta para establecer los plazos de conservación, bloqueo y destrucción. En cualquier caso, lo relevante y, ante la pregunta de cuánto conservar los datos, se ha de tener en cuenta el mínimo y estricto periodo que sea necesario para la finalidad para que fueron obtenidos. Finalizada esta desaparecería en principio la base de legitimación.

A modo ilustrativo, se trae a colación la sanción de la AEPD[83] de 50.000 euros por la conservación excesiva de los datos del reclamante sin ser cliente, en concreto denunciaba a la entidad bancaria por conservar sus datos pese a haber dejado de ser cliente hacía 16 años. En este caso, la sanción fue abonada en periodo de pago voluntario, por lo que supuso una reducción de un 20% del importe de la misma, de conformidad con el artículo 85.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP, en adelante).

[83] Recuperado de: https://www.aepd.es/documento/ps-00076-2020.pdf (fecha de consulta: 2024).

3.6. Principio de integridad y confidencialidad: implica que los datos personales han de ser tratados de tal manera que se garantice una seguridad adecuada de los datos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su perdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiada.

Cabe precisar que los citados principios (licitud, minimización, limitación del plazo de conservación, etc.) no se aplican a la información anónima[84] (aquella que no guarda relación con una persona física identificada o identificable, inclusive con fines estadísticos de investigación)[85]. En cambio, los datos personales seudonimizados (concepto distinto de anonimización, aunque a veces se confunden) que habría atribuir a una persona física mediante la utilización de información adicional, debe considerarse información sobre una persona física identificable[86]. Al respecto, para determinar si existe la probabilidad razonable de que se utilizan medios para identificar a una persona física, según el RGPD deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesario para identificación, teniendo en cuenta tanto la tecnología disponible en el momento de tratamiento como los avances tecnológicos.

A modo ilustrativo, en la Resolución de la AEPD se hace referencia a que la sanción e 15.000 euros a una empresa de seguridad por enviar correos electrónicos sin copia oculta. Supone una sanción puesto que se reveló la dirección de correo del reclamante y del resto de destinatarios sin su consentimiento. La empresa no contaba con legitimación para revelar la dirección del correo personal del reclamante. La AEPD consideró este hecho como una vulneración del principio de integridad y confidencialidad recogido en el art. 5.1 f del RGPD, por lo que se le sanciona con una multa de 15.000 €. Además, sancionó con 5.000 € por no aplicar las medidas de

[84] Recuperado de: https://www.aepd.es/documento/guia-basica-anonimizacion.pdf (fecha de consulta: 2024)
[85] Véase el Considerando nº 28 RGPD.
[86] Recuperado: https://www.aepd.es/prensa-y-comunicacion/blog/anonimizacion-y-seudonimizacion (fecha de consulta: 2024)

seguridad técnicas y organizativas para garantizar la confidencialidad de los datos[87].

3.7. Responsabilidad proactiva o *accountability*[88]: este principio implica que el responsable del tratamiento (esto es, aquel o aquellos que determina/determinan la finalidad o las finalidades y los medios del tratamiento) será responsable del cumplimiento en materia de protección de datos y capaz de demostrarlo.

Se trata de un principio que no se regula de forma específica en un precepto del RGPD, pero se hace referencia en todo el articulado, como en el citado artículo 5[89]. En palabras del autor PUYOL J.. "(..) la responsabilidad proactiva de los operadores jurídicos contemplados en la nueva normativa sobre privacidad, el *Compliance* y la ciberseguridad sobre los datos personales, crean un todo interconectado y complementario, máxime si se tiene en cuenta el aumento no solo de los riesgos sino del valor de los datos personales en sí abundan en la necesidad de reforzar el papel y la responsabilidad de los responsables del tratamiento de datos. Este nuevo marco normativo se orienta a esta nueva realidad, y debe incluir las herramientas necesarias para que los responsables del tratamiento establezcan y apliquen en la práctica aquellas medidas adecuadas y

[87] Recuperado de: https://www.aepd.es/documento/reposicion-ps-00452-2022.pdf (fecha de consulta: 2024).

[88] El empresario debe probar ante la AEPD y el resto autoridades de control que cumple estrictamente con la normativa y alienta a las organizaciones a poner en marcha y desarrollar buenas prácticas que garantice una gestión respetuosa con la protección de datos.

[89] Por ejemplo, en el Considerando nº 42 RGPD: Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

eficaces que cumplan los objetivos de los principios de protección de datos y del *Corporate Compliance*"[90].

En este punto, se pone en evidencia el cambio de mentalidad y de actuación a partir del RGPD. El cumplimiento de este principio se exige a todos los niveles y de forma continuada, debiendo, además, disponer de evidencias del cumplimiento. Sin embargo, se ha constatado a lo largo del periodo investigador que sigue siendo necesario fomentar este principio y su importancia por el aumento de las cifras de sanciones por incumplimiento de la normativa y la reiteración de los motivos de sanciones impuestas por las Autoridades de Control por la vulneración de la normativa.

En línea con lo anterior, se pone de manifiesto que aún no está completamente integrado en la mayoría de organizaciones y empresas, independiente de su tamaño, siendo necesario trabajar en la concienciación y formación en la materia de protección de datos y en la relevancia de la *accountability* para cumplir con el RGPD. Esto es, se exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que realicen.

3.8. Privacidad desde el diseño y por defecto: siguiendo la Guía de la AEPD de "Privacidad desde el Diseño"[91], este principio implica "utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida", entendido como todas las fases por las que atraviesa este desde su concepción hasta su retirada.

[90] Recuperado de: https://confilegal.com/20200227-compliance-y-proteccion-de-datos-dos-caras-de-la-misma-moneda/ (fecha de consulta: 2023).
[91] Recuperado de: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf (fecha de consulta: 2022).

Es preciso tener en cuenta, a su vez, los siguientes principios fundamentales de la privacidad desde el diseño:

1. Proactivo, no reactivo; preventivo, no correctivo.
2. La privacidad como configuración predeterminada.
3. Privacidad incorporada en la fase de diseño.
4. Funcionalidad total: pensamiento todos ganan.
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia.
7. Enfoque centrado en el sujeto de los datos.[92]

Respecto al principio privacidad por defecto, en virtud de la correspondiente definición de la Guía de la AEPD de "Privacidad por Defecto"[93], supone que se ha de respetar "bajo los criterios de adecuación, pertinencia y necesidad con relación a los fines en el diseño de las distintas fases del tratamiento", tal como establece el artículo 25.2. RGPD. Es decir, Significa que, por defecto, solo sean objeto de tratamiento los datos necesarios para cada uno de los fines específicos del tratamiento; debiendo el responsable de tratamiento aplicar las medidas apropiadas para ello. Además, significa que, por defecto los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas[94].

4. **Categorías especiales de datos y tratamientos de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas:** otro aspecto a destacar es que el RGPD prevé un especial tratamiento de los datos sensibles que denomina "categorías especiales de datos". Esta consideración tiene aquella información que revele el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos

[92] Véase la Guía de la AEPD de "Privacidad desde el Diseño".
[93] Recuperado de https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf (fecha de consulta: 2022).
[94] Véase el Considerando nº 78 del RGPD.

genéticos[95], datos biométricos dirigidos a identificar de manera univoca a una persona física, datos relativos a la salud[96] o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Como regla general, el RGPD prohíbe el tratamiento de los datos sensibles en el apartado primero de su artículo 9, aunque también prevé excepciones en el apartado 2, como cuando concurran una serie de circunstancias:

i) que el interesado diera su consentimiento explicito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado;
ii) que sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
iii) que el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.

A las que se añade la excepción relativa a que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud[97]. Dichas excepciones se verán con más detalle en la publicación del capítulo de libro

[95] Véase el Considerando nº 34 RGPD.
[96] Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera univoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro. (Considerando nº 35 RGPD).
[97] Véanse los Considerandos nº 51 a 54 RGPD.

que configura el Capítulo V del presente Compendio de Publicaciones, a la que nos remitimos.

En cuanto a los tratamientos de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, el RGPD prevé que solo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

5. **Derechos de los interesados**: el RGPD consagra una serie de derechos ejercitables por sus titulares, los interesados. Aunque la mayoría de ellos no eran novedosos, sí lo es el derecho a la portabilidad. Además, se pone de manifiesto que durante el periodo investigador se ha producido un gran desarrollo de los mismos, especialmente a través de los múltiples pronunciamientos de las autoridades de control en materia de protección de datos que han aclarado, precisado y matizado su contenido. A continuación, se realiza una breve referencia a los derechos reconocidos por la normativa sobre protección de datos.

   5.1. **Derecho a la transparencia, de información y acceso a los datos**: en primer lugar, el derecho de **acceso** a los datos personales supone el derecho del interesado a solicitar el acceso a los datos que disponen de su titularidad (si se tratan sus datos o no, para qué fines, cuál es la base de legitimación y si los han cedido a terceros, entre otros aspectos). Se prevé que es un derecho que podría ceder en serie de casos previstos en el RGPD (artículo 14.5. RGPD), como cuando:

   i) el interesado ya dispone de la información;
   ii) la comunicación resultase imposible o supusiese un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
   iii) cuando la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado;

iv) o cuando los datos deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria[98]. En todo caso, parte el RGPD que el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo publica la información.

A modo ilustrativo, se trae a colación que la AEPD ha sancionado a en numerosas ocasiones a empresas de telecomunicaciones por ejercicios de derecho de acceso por parte de los interesados que no recibieron contestación[99] o la recibieron incumpliendo la normativa. Al respecto de este derecho, se trae a colación que la AEPD está participando en una acción europea para analizar la aplicación del derecho de acceso, una iniciativa en el marco del CEPD o EDPB y pretende evaluar cómo están cumpliendo las organizaciones con este derecho[100].

En segundo lugar, en cuanto al derecho a la **información**, cuando los datos se obtuvieron del interesado, el responsable del tratamiento le debe facilitar en el momento de su obtención la siguiente información sobre el tratamiento:

[98] Recuperado de: https://www.elmundo.es/economia/empresas/2019/01/21/5c45e159fc6c8305148b4693.html (fecha de consulta: 2020). En este punto se trae a colación que, con fecha 21 de enero de 2019, la CNIL anunció la imposición de la a Google con 50 millones de euros por infringir la norma de protección de datos y falta de transparencia por haber usado datos personales de los usuarios sin haber informado claramente sobre el uso de estos. No negaban que *Google* informe a sus usuarios sobre el uso de sus datos personales, ha declarado a la AFP Mathias Moulin, director de la protección de los derechos y de las sanciones de la CNIL. "Pero la información no es fácilmente accesible y está diseminada en diferentes documentos", añadían. La CNIL tomó esta sanción tras recibir quejas colectivas de dos asociaciones en mayo del año pasado, poco después de la entrada en vigor de la directiva europea. Una fue presentada en nombre de unos 10.000 firmantes por la asociación *francesa Quadrature du Net*, mientras que la otra fue presentada por *None Of Your Business*, creada por el activista austriaco Max Schrems que había acusado a Google de obtener el "consentimiento forzado" mediante el uso de casillas emergentes en línea o en sus aplicaciones.

[99] Recuperado de: https://www.aepd.es/documento/pd-00211-2023.pdf (fecha de consulta: 2024).
Recuperado de: https://www.aepd.es/documento/pd-00189-2023.pdf (fecha de consulta: 2024).

[100] Recuperado de: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-participa-en-una-accion-europea-para-analizar-la (fecha de consulta: 2024).

i) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
ii) los datos de contacto del Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés, en adelante), en su caso;
iii) los fines del tratamiento y su base legitimadora;
iv) los destinatarios o las categorías de destinatarios de los datos;
v) en su caso, la intención de transferirlos a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado[101].
vi) el plazo de conservación o, los criterios utilizados para determinarlo;
vii) su derecho al ejercicio de los derechos en materia de protección de datos; en caso de que el consentimiento sea la base de legitimación, su derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; y su derecho a presentar una reclamación ante una autoridad de control;
viii) la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado, entre otros puntos[102].

En el caso de que la información no se haya obtenido del interesado, sino de otra fuente como puede ser un tercero, además de los aspectos anteriores, se le debe informar de la fuente de la que proceden los datos

[101] Es decir, cuando se produzcan transferencias internacionales de datos a países fuera del Espacio Económico Europeo el interesado tendrá derecho a ser informado de las garantías adecuadas. Respecto al modo de facilitar acceso al interesado, el responsable del tratamiento facilitaría una copia de los datos personales objeto de tratamiento y podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. Además, y este es otro punto relevante, se prevé que este derecho no afectará negativamente a los derechos y libertades de otros, terceros, por lo que habrá de revisar para que haya derechos de terceros que pudieran verse afectados.
[102] Según el Considerando nº 61 y 62 RGPD.

personales (por ejemplo, un familiar o una empresa) y, en su caso, si proceden de fuentes de acceso público.

Según el RGPD, dicha información se debe facilitar de forma transparente, clara y comprensible, además de gratuita como regla general, salvo en ciertos casos, y debe ser facilitada dentro de un **plazo razonable** y a más tardar dentro de **un mes** desde la solicitud o en casos complejos o por el número de solicitudes, puede ampliarse por **dos meses** informando y justificando el motivo con carácter previo. Al respecto, tal y como se ha evidenciado durante el periodo investigador, la AEPD es bastante estricta con el cumplimiento del plazo, habiendo sancionado en caso de que se haya resuelto el derecho ejercitado de forma extemporánea.

Respecto al momento en que se ha de facilitar información, el RGPD prevé que, si los datos personales han de utilizarse para comunicación con el interesado, se le informe en la primera comunicación con este (por ejemplo, la primera vez que le contactan por teléfono vía email), o si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que sean comunicados por primera vez.

Además, prevé que cuando el responsable proyecte el tratamiento ulterior para un fin distinto a la inicial (como, por ejemplo, se obtuvieron para la prestación de un servicio y posteriormente se desea utilizar con fines de marketing o publicidad), se debe proporcionar al interesado antes de dicho tratamiento ulterior información sobre ese otro fin.

5.2. Derecho a la rectificación, a la limitación del tratamiento y a la supresión: otros derechos reconocidos al interesado son el derecho de rectificación de los datos inexactos, para que sean rectificados sin dilación indebida por parte del responsable[103]; el derecho de limitación del tratamiento cuando el responsable ya no los necesite para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones[104].

[103] Véase el Considerando nº 65 RGPD.
[104] Véase el Considerando nº 67 RGPD.

De otro lado, el derecho de supresión supone que el interesado tendrá derecho a obtener, sin dilación indebida, la supresión de sus datos, cuando:

i) ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
ii) retire el consentimiento en que se basa el tratamiento y no se base en otra base de legitimación del artículo 6 RGPD;
iii) se oponga al tratamiento y no prevalezcan otros motivos legítimos;
iv) hayan sido tratados ilícitamente o deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5.3. Derecho de oposición al tratamiento: caso en el que siendo procedente el responsable del tratamiento dejará de tratar los datos, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. En concreto, se prevé que si el tratamiento de datos tiene por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de sus datos personales, incluida la elaboración de perfiles, entendida como toda forma de tratamiento automatizado de datos personales que consiste en usar información personal para evaluar determinados aspectos de una persona, en la medida en que esté relacionada con la citada mercadotecnia.

5.4. Portabilidad: un derecho que sí tuvo carácter novedoso respecto a la regulación anterior es el derecho a la portabilidad de los datos, que implica el derecho del interesado a recibir los datos de su titularidad que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.

Cuando el tratamiento esté basado en el consentimiento o en un contrato y el tratamiento se efectúe por medios automatizados, el interesado tendrá

derecho a que los datos se transmitan directamente de responsable a responsable cuando sea técnicamente posible, lo que puede hacer que en algunos casos este derecho pierda eficacia. Como ocurre en los derechos anteriores, el ejercicio de este derecho no deberá afectar negativamente a los derechos y libertades de otros interesados, punto relevante sobre el que se viene incidiendo por parte de las autoridades de control, en particular por la AEPD[105].

Como se indicaba anteriormente, el plazo para responder el ejercicio de derechos es de **un mes** desde la recepción de la solicitud. El responsable del tratamiento debe responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas, pudiendo prorrogarse por otros dos meses más informando del motivo debidamente, por ejemplo, cuando es complejo o atendiendo al número de solicitudes.

En cualquier caso, se recomienda acusar recibo de la recepción del ejercicio de derecho ejercitado, proceder a subsanar la información o identificación requerida en caso de que sea necesario, y responder en el plazo máximo del mes. En caso de que no sea posible, por la complejidad u otra cuestión justificable, se avisará de tal circunstancia al interesado y se responderá en el plazo de prórroga establecido en el RGPD. En caso de no hacerlo es denunciable ante la autoridad de control protección de datos, con el riesgo de sanción por la no atención o la atención extemporánea del derecho en cuestión.

6. **Roles en el tratamiento de datos y medidas técnicas y organizativas**: otra de las cuestiones esenciales es que el RGPD prevé los roles de tratamiento de datos de responsable de tratamiento, encargado de tratamiento, corresponsables de tratamiento y subencargados del tratamiento (artículos 24 y siguientes del RGPD), estableciendo el deber del responsable y el encargado del tratamiento de aplicar las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así

[105] Véanse los Considerandos nº 65 y 68 RGPD.

como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas (artículo 32 RGPD).

Así mismo, establece que cada responsable de tratamiento y, en su caso su representante, lleven a cabo un RAT de los tratamientos efectuados bajo su responsabilidad con la información mínima del art. 30 RGPD (el nombre y los datos de contacto del responsable y en su caso el corresponsable, representante del responsable y el DPO; los fines del tratamiento, las categorías del interesados y de datos personales, los destinatarios, en su caso, las transferencias internacionales de datos, los plazos de conservación o los criterios para determinarlo y cuando sea posible las medidas técnicas y organizativas de seguridad del tratamiento a las que se ha hecho referencia). Es esencial que el RAT se encuentre permanentemente actualizado y documentado a disposición de un posible requerimiento por autoridad de control, auditorías de cumplimiento o incluso de los proveedores que requieran prueba de cumplimiento del RGPD.

7. **Brechas de seguridad:** se regula en el RGPD la gestión y notificación de las brechas de seguridad, que pueden ser de confidencialidad, integridad o de disponibilidad o de varios tipos de forma conjunta. Independientemente del tipo de brecha, los efectos de sufrir una brecha de seguridad pueden ser irreparables (como pueden ser reputacionales o, aunque se abone la sanción por incumplimiento y recupere la actividad económica, los datos podrían estar a disposición de terceros que puede utilizarlos de forma ilícita).

   Según el RGPD, en caso de violación de la seguridad de los datos personales (artículo 33 RGPD) el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar **72 horas** después de que haya tenido constancia de ella, a menos que sea improbable que constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. Además, cuando sea probable que entrañe un alto riesgo para los derechos y libertades de las personas, el responsable del tratamiento la comunicará al interesado sin dilación indebida, salvo que:

i) haya adoptado medidas de protección técnicas y organizativas apropiadas y se han aplicado a los datos afectados por la violación de la seguridad de los datos, en particular, aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

ii) haya tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado; o

iii) suponga un esfuerzo desproporcionado, caso en el que se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados[106].

En caso de que se imponga una sanción económica tras una brecha de seguridad, por mínima que sea y aunque se abone con la rebaja del veinte por ciento por pago voluntario (derivada el artículo 85 de la LPACAP)[107] una fuga de datos resulta evidente que conlleva un perjuicio en su reputación y su imagen, tanto frente a sus clientes actuales, potenciales, y también frente a sus trabajadores, lo que puede suponer pérdidas más difíciles de recuperar que las económico.

8. **Figura del Delegado de Protección de Datos o DPO:** otra de las novedades más destacadas es la figura del **DPD** (artículos. 37 y siguientes del RGPD), respecto al que no existe referencia en la regulación anterior y nada tiene que ver con el responsable de tratamiento, el encargado de tratamiento, ni con la autoridad de control. En general, el DPO es la persona que ha de informar sobre las obligaciones de la empresa en materia de privacidad y protección de datos personales, se

[106] Al respecto, véanse los Considerandos nº 85, 86 y 87 RGPD.

[107] Expresa bajo la rúbrica "Terminación en los procedimientos sancionadores": "1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda. 2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción. 3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción. El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

encarga de ser el contacto ante las Autoridades nacionales de protección de datos, entre otras muchas funciones esenciales.

El RGPD y la legislación nacional, en el caso de España la LOPDGDD 3/18, expresa cuándo las organizaciones están obligados a su nombramiento (como colegios profesionales, centros sanitarios, empresas de seguridad privada, empresas de banca y cajas de ahorros o centros docentes), así como los requisitos que ha de cumplir y sus funciones, que ha de ejercer con total independencia, siendo el supervisor y responsable de velar por el cumplimiento del RGPD. En dicha función, además debe tener en cuenta las interpretaciones y recomendaciones de las Autoridades de Control y en particular, CEPD[108] (regulado en los artículos 68 y siguientes del RGPD, que sustituyó al anterior Grupo de Trabajo del artículo 29 o GT-29) [109] y la AEPD[110]; así como las normativas nacionales de aplicación según la especialidad, en su caso, de la organización de que se trate, como ocurre por ejemplo en el sector financiero, telecomunicaciones o de sanidad.

9. **Transferencia Internacional de Datos:** el RGPD parte del reconocimiento de la necesidad para la expansión del comercio y la cooperación internacionales de las transferencias internacionales de datos. Aunque prevé si hay transferencia de datos no se debe menoscabar el nivel de protección de las personas garantizado en la UE por el RGPD. Así, el principio general es que se puede realizar cuando la Comisión haya decidido que el país, territorio o uno o varios sectores específicos de ese tercer país u organización internacional de que se trate garantizan un nivel de protección adecuado. Esta transferencia no requiere ninguna autorización

[108] Se cita también la existencia del CEPD o Comité Europeo de protección de datos que emite orientaciones generales para explicar conceptos clave del RGPD o directrices de interpretación del RGPD o resuelve litigios entre los estados miembros, como de independencia, cooperación
[109] Recuperado de: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en (fecha de consulta: 2020). A modo de ejemplo, interesa mencionar las guías del EDPB sobre datos sensibles, de tratamientos que impliquen perfilado, sobre tratamientos de datos relativos a personas vulnerables. También, hay guías sectoriales, como las de protección de daos y prevención de delitos, de centros educativos o en los despachos de abogados. Ente las Directrices, recomendaciones y mejores prácticas más recientes se citan las relativas a los derechos de los interesados, derecho de acceso; sobre la identificación de la principal autoridad de control de un responsable o encargado de tratamiento o sobre el uso de la tecnología de reconocimiento facial en ámbito policial
[110] A modo de ejemplo, en el siguiente enlace se pueden encontrar las Guías con las interpretaciones de la AEPD. Recuperado de: https://www.aepd.es/guias-y-herramientas/guias (fecha de consulta: 2023), entre las que recientemente se han aprobado La Guía sobre tratamientos de control de presencia mediante sistemas biométricos y la Nota técnica de las pruebas de concepto sobre sistemas de verificación de edad.

específica. A falta de decisión de adecuación, se permite la transferencia con garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Las garantías adecuadas, que podrán ser aportadas a través de:

i) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
ii) Normas corporativas vinculantes.
iii) Cláusulas tipo de protección de datos adoptadas por la Comisión: con fecha 4 de junio de 2021, la Comisión Europea publicó el nuevo conjunto de cláusulas contractuales tipo que, además de sustituir a sus predecesoras, pretenden poder abarcar las transferencias entre responsables, entre responsable y encargado, entre encargados y entre encargado y responsable.
iv) Las cláusulas contractuales de las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE quedan derogadas a partir del 27 de septiembre de 2021. No obstante, los contratos celebrados antes de dicha fecha con arreglo a las anteriores Decisiones serán válidos hasta el 27 de diciembre de 2022, siempre que las operaciones de tratamiento permanezcan inalteradas y las cláusulas contractuales garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas.
v) Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
vi) Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión.
vii) Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.
viii) Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.

10. **Régimen sancionador:** finalmente, resalta el cambio en el régimen sancionador (artículos 77 y siguientes del RGPD) con el RGPD, previéndose solo dos categorías de multas administrativas[111] y ofreciendo distintas herramientas a las Autoridades de Protección de datos en caso de incumplimiento de las normas de protección de datos, como puede ser advertencias ante una posible infracción o frente a una infracción; apercibimientos, prohibiciones temporales o definitiva del tratamiento y la imposición de multas de hasta 20 millones de euros o un 4 % del volumen de negocio total anual.

El RGPD establece que las Autoridades de Control garantizará que la imposición de las multas administrativas según el RGPD en cada caso sean efectivas, proporcionadas y disuasorias, estableciéndose según las circunstancias de cada caso individual pudiendo llegar a 10.000 euros como máximo o tratándose de una empresa, de cuantía equivalente al 2 % como máximo del volumen de negocio total anual del ejercicio financiero anterior, optándose por la de mayor cuantía o de 20.000 euros como máximo o el 4 % como máximo de volumen de negocio total anual del ejercicio financiero anterior, optándose por la de mayor cuantía.

En caso de una infracción, se puede imponer una pena pecuniaria en lugar o además del apercibimiento o prohibición del tratamiento y que además, debe garantizar que las multas impuestas en cada caso particular sean efectivas, proporcionadas y disuasorias, y tendrá en cuenta varios factores, como la naturaleza, la gravedad y la duración de la infracción, su intencionalidad o negligencia, cualquier medida tomada para paliar los daños sufridos por las personas, el nivel de cooperación de la organización, etc.[112]

[111] En el anterior régimen se preveía una multa con un máximo de 600.000 euros: las infracciones leves serán castigadas con multas de 900 a 40.000 euros; las graves con multas de 40.001 a 300.000 euros; y las muy graves de 300.001 a 600.000 euros; a multas de 20 millones de euros o un 4% de la facturación anual.

[112] Recuperado de: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_es#:~:text=infracci%C3%B3n%3A%20las%20posibilidades%20incluyen%20un,de%20negocio%20total%20anual%20mundial (fecha de consulta: 2023).

C) Resultados.

En primer lugar, se ha evidenciado que la entrada en vigor y aplicación del RGPD supuso un hito jurídico en materia de protección de datos, introduciendo grandes novedades respecto a la normativa anterior que derogó, como su ámbito de aplicación, la figura del DPO, el cambio del régimen sancionador o la introducción del derecho a la portabilidad de los datos. Adicionalmente, el RGPD, supuso también un cambio de mentalidad y de actuación, debiendo ser continuado y a todos los niveles el cumplimiento de sus principios, desde el principio de licitud, toda vez que todo tratamiento de datos personales ha de ser legítimo, es decir, debería basarse, al menos, en uno de los supuestos que prevé (consentimiento del interesado, interés público, obligación legal, etc.); hasta el principio de responsabilidad proactiva.

En segundo lugar, se ha evidenciado que el RGPD logró en parte con su objetivo de homogeneización, aunque al dejar un cierto margen en algunas cuestiones a la legislación nacional (como la determinación de la edad del menor para prestar su consentimiento al tratamiento de datos), conlleva que no logre de forma absoluta con su pretensión de armonización. Además, se ha constatado la necesidad de una especial protección homogénea de los menores de edad en todos los ámbitos, junto a una mayor atención y tutela por ser considerados menos conscientes de los riesgos, las consecuencias, y las garantías y derechos en materia de protección de datos, especialmente cuando vayan a ser tratados sus datos con finalidades relacionadas con la mercadotecnia.

En conexión con lo anterior, se evidencia una especial tutela de los menores de edad en el entorno digital, trayéndose a colación de manera ilustrativa la Resolución de la AEPD de agosto de 2023[113], en la que sancionó a una inmobiliaria con 6.000 euros por publicar fotos de un inmueble con imágenes de menores. Dos fotografías de la cocina del inmueble permitían ver cuatro fotos de menores; otra, de un dormitorio, retratos de estas.

En tercer lugar, se ha evidenciado que el RGPD es la normativa más garantista y restrictiva en materia de protección de datos y ha tenido una gran influencia en otros

[113] Recuperado de: https://www.aepd.es/es/documento/ps-00526-2022.pdf (fecha de consulta 2023)

continentes y países en el marco de protección de datos, como ocurre en los países en América Latina, donde la protección de datos personales es tan diversa como los países que la forman, con realidades sociales, económicas, políticas y culturales muy diferentes.

En cuarto lugar, se ha constatado a lo largo del periodo investigador que, aunque se han producido grandes avances en la tutela de este derecho, especialmente en el ámbito europeo, casi seis años después de la entrada en vigor y aplicación del RGPD la realidad demuestra que siguen existiendo organizaciones y empresas que no se han adaptado. Otras se han adaptado al cumplimiento de la normativa de protección de datos sin profundizar o en un plano meramente "formal", probablemente para exonerarse de posibles sanciones o cumplir de cara a la cara visible y a favor de su reputación, lo que no es conforme el espíritu del RGPD y de la cultura de cumplimiento en privacidad de protección de datos y la responsabilidad proactiva.

De otro lado, se ha evidenciado que las cifras de sanciones por incumplimiento en materia de protección de datos no dejan de aumentar, llegándose a reiterar los motivos de sanciones impuestas por las Autoridades de Control por la vulneración de la normativa de protección de datos y en aspectos esenciales de cumplimiento, tal y como ponen de manifiesto las sanciones de Autoridades de Control de protección de datos impuestas durante el periodo investigador desde el año 2018 (en que entró en vigor y aplicación el RGPD y se inició la presente investigación) a la actualidad.

A continuación, se trasladan en las siguientes tablas las sanciones más relevantes, ordenadas por orden cronológico que han sido objeto de análisis a lo largo del periodo investigador, con especial foco en las sanciones más recientes durante los años 2023 y lo que llevamos del año 2024 hasta el depósito de la tesis:

Años 2018 y 2019

- En el año 2018, considerada la sanción de mayor calado social, destaca la sanción derivada de la cesión ilícita de datos personales por parte de la red social *Facebook* a la empresa *Cambridge Analytica* para fines ilícitos, que fue noticia a principios del año 2018 y en marzo del mismo año, la AEPD impuso una multa de 300.000 euros a la empresa de mensajería instantánea *WhatsApp* y a la red social *Facebook* por el tratamiento indebido de la información de los usuarios cuando dicha red social compró la aplicación de mensajería. Entre otras sanciones impuestas durante el año 2018, fue noticia la sanción de 5.000 euros por la AEPD a un médico tras perder las imágenes de una paciente en una operación[114].

- Durante el año 2019 destacan las sanciones impuestas i) por la Autoridad de Protección de Datos francesa o CNIL a *Google* con 50 millones de euros por infringir la normativa y por falta de transparencia al utilizar datos de usuarios sin haberles informado de forma clara sobre su uso o finalidades[115]; ii) a *Facebook* por infringir de nuevo la normativa dejando expuestos datos de cientos de sus usuarios[116]; y iii) a la aplicación *La Liga Nacional de Futbol Profesional* con una multa de 250.000 euros. Esta última, junto a la obligación de adecuación al principio de transparencia en relación con el uso de la aplicación en los términos individuales por mecanismos que refuercen el conocimiento por los usuarios de la activación de la funcionalidad del micrófono de los dispositivos que instalen la aplicación en el momento en que esta se produzca[117].

[114] Recuperado de: https://www.europapress.es/madrid/noticia-agencia-proteccion-datos-sanciona-5000-medico-perder-imagenes-paciente-operacion-20181113113507.html (fecha de consulta: 2023).

[115] Recuperado de: https://www.elmundo.es/economia/empresas/2019/01/21/5c45e159fc6c8305148b4693.html (fecha de consulta: 2023).

[116] "Facebook eleva a 87 millones los usuarios afectados por el escándalo de Cambridge Analytica". Recuperado de http://www.europapress.es/internacional/noticia-facebook-eleva-87-millones-usuarios-afectados-escandalo-cambridge-analytica-20180404212958.html (fecha de consulta: 2023); "Encuentran datos de millones de usuarios expuestos en la red". Recuperado de: https://www.efe.com/efe/america/tecnologia/encuentran-datos-de-millones-usuarios-facebook-expuestos-en-la-red/20000036-3943507(fecha de consulta: 2023).

[117] Recuperado de: https://www.eldiario.es/tecnologia/Agencia-Proteccion-Datos-Liga-microfono_0_908859408.html. Procedimiento Sancionador Nº: PS/00326/2018 (fecha de consulta: 2023).

Años 2018 y 2019

También, destaca en este año 2019 la sanción impuesta por la Autoridad de Protección de Datos británica, la Oficina del Comisionado de Información de Reino Unido a una compañía aérea con 205 millones de euros por el robo de datos de los clientes con potencialmente 500.000 afectados, tras un ataque informático producido en la filial en verano de 2018[118] desde la web de la aerolínea e incluyendo información financiera de la tarjeta de crédito.

[118] Resolución del Procedimiento Procedimiento Nº: PS/00051/2020. Recuperado de: https://elpais.com/economia/2019/07/08/actualidad/1562569904_267036.html (fecha de consulta: 2023).

Año 2020

Durante el año 2020 destacan las sanciones impuestas a i) una conocida tienda de ropa con una multa récord de 35,3 millones de euros por espiar a sus empleados en Alemania[119]; así como a ii) un partido político por una brecha de seguridad sufrida que vulneró los principios de integridad y de confidencialidad al no contar con las medidas adecuadas de seguridad y hacerse público un fichero de afiliados[120]. Se trae igualmente a colación la multa por la AEPD a iii) otro partido político con 1.500 euros por remitir un correo electrónico sin autorización ni consentimiento del receptor, al haber este solicitado su baja con carácter previo y haber sido confirmada por el denunciado mediante correo electrónico remitido al interesado[121].

Otra de las sanciones destacables durante el citado año, es la impuesta por la AEPD frente a iv) una compañía tecnológica de entrega a domicilio con 25.000 euros por no tener designado DPO, configurando esta la primera multa a una empresa por este motivo en España y que, a pesar de que, en enero de 2020, nombró a un responsable de protección de datos, no logró evitar la sanción[122].

[119] Recuperado de: https://www.elmundo.es/economia/ahorro-y-consumo/2020/10/01/5f75c05c21efa06d7f8b457b.html (fecha de consulta: 2023).
[120] Recuperado de: https://www.aepd.es/es/documento/ps-00051-2020.pdf (fecha de consulta: 2023).
[121] Recuperado de: https://www.aepd.es/es/documento/ps-00051-2020.pdf (fecha de consulta: 2023).
[122] Recuperado de: "25.000 euros de multa a Glovo por no contar con un delegado de protección de datos". Recuperado de: https://www.expansion.com/juridico/actualidad-tendencias/2020/06/10/5ee0bc66468aeb756a8b45f2.html (fecha de consulta: 2024). Al respecto, interesa puntualizar que la figura del DPO configuraba una de las novedades del RGPD, como figura esencial encargada, principalmente y entre muchas otras funciones que varían dependiendo de la organización en que se trate y su estructura, de supervisar el cumplimiento de la normativa sobre protección de datos y el respeto de sus principios en la compañía, analizar los tratamientos de datos y los riesgos para los derechos y libertades de las personas, velar por los derechos de los interesados en materia de protección de datos, revisar los proyectos desde la compañía, controlar a los proveedores y los contratos en los que esté implicada la protección de datos o ser la persona de contacto entre la organización y la autoridad de control de que se trate.

Año 2021

A lo largo del año 2021 resaltan las sanciones impuestas por la AEPD a una entidad bancaria por tratamiento el ilícito de datos de sus clientes y a una compañía de telefonía por un doble motivo. Por un lado, por no frenar las comunicaciones comerciales cuando se le pedía, por la falta de control real, continuo, permanente y auditado de los tratamientos realizados por los encargados de tratamiento; por realizar transferencias internacionales de datos; por el envío de comunicaciones comerciales sin consentimiento y por no haber atendido el ejercicio de derechos o realizado una atención suficiente o temporánea con un total de 8.150.000 euros. Por otro lado, dicha compañía de telefonía fue sancionada por la realización de llamadas comerciales insistentes y continuadas con un importe de 50.000 euros.

Adicionalmente, destacan en este año las sanciones impuestas por la AEPD a un conocido supermercado, dando por finalizada una prueba piloto de reconocimiento facial, abonando 2,5 millones por su sistema de reconocimiento facial que fue testado durante varios meses en 48 de las 1.640 tiendas en España; a una entidad financiera al pago de una multa de 200.000 euros por no garantizar la seguridad en el tratamiento de datos al facilitar a través del sistema de atención telefónica automatizado información asociada a un documento nacional de identidad con tan solo facilitar su número.

También, se considera reseñable la sanción impuesta a un club deportivo con 4.000 euros por incluir en un grupo de WhatsApp a un antiguo usuario de su entidad, sin su previo o autorización y no existiendo relación entre las partes desde hace más de diez años. Por último, cabe resaltar que WhatsApp recibió una multa récord por el mencionado ICO de 225 millones de euros por no decir cómo compartía datos con *Facebook* y por infringir las leyes europeas de protección de datos.

Año 2022

A principios del año 2022, destacan las sanciones i) de la AEPD por un importe de 12.000 euros por vulneración del principio de licitud de tratamiento y ausencia de justificación e información[123] de la negativa a la celebración de contrato por su inclusión en un fichero de morosidad; y la sanción ii) por solicitar a los candidatos el certificado de antecedentes penales en un proceso de contratación con 2.000.000 euros y ordenando dejara de pedir dicho documento[124].

Junto a ellas, resalta iii) la sanción a una entidad financiera de 2.100.000 euros por la infracción de la normativa por parte de otra entidad financiera con la que se fusionó, por no cumplir el consentimiento con los requisitos RGPD con la solicitud al interesado de un consentimiento ilícito pre marcado y/o condicionado para el tratamiento de datos no necesarios supeditado a la prestación del servicio[125].

[123] Más información en el siguiente enlace. Recuperado de: https://www.dataguidance.com/news/spain-aepd-fines-servicios-financieros-carrefour-20000 (fecha de consulta: 2023). Resolución en el siguiente enlace: https://www.aepd.es/es/documento/ps-00478-2021.pdf (fecha de consulta: 2023).

[124] Considera en que la recogida y utilización de dicho certificado constituye un tratamiento de datos excesivo al existir formas menos intrusivas para proteger la confianza de los clientes. Recuperado de: https://www.businessinsider.es/crece-ritmo-sancionador-aepd-multa-amazon-2-millones-1011967 (fecha de consulta: 2023).

[125] Recuperado de: https://www.europapress.es/economia/finanzas-00340/noticia-aepd-multa-caixabank-millones-ligar-exencion-comisiones-cesion-datos-personales-20220304135750.html.

Años 2023 y 2024 (hasta la fecha de depósito de la tesis)

Durante el año 2023 y lo que llevamos del año 2024, se evidencia que no solo siguen incrementando el número de sanciones, sino que se sigue sancionando por las Autoridades de Control a grandes empresas por motivos básicos y aspectos elementales de la normativa de protección de datos. A modo de ejemplo, se citan las sanciones recientes por no disponer de DPO estando obligadas a ello según el RGPD, por falta de información y transparencia en la Política de Privacidad[126], por la no tención de derechos en materia de protección de datos o su atención extemporánea o incompleta[127]; o incluso tras detectar irregularidades por parte de un usuario de una web en la Política de Cookies de un comercio de ropa[128].

- Así, se observa que las empresas de telecomunicaciones siguen siendo sancionadas por mala praxis al realizar duplicados de tarjeta SIM o eSIM (tarjeta virtual), a través de suplantación de identidad o casos de *sim swapping o* estafas de duplicación fraudulenta de tarjeta SIM de una persona[129]. También, el aumento de las denuncias por llamadas comerciales a individuos que se ha opuesto y/o están registrados en la lista de exclusión publicitaria o Lista Robinson[130;] así como por no contar con medidas suficientes se seguridad para evitar una suplantación de identidad y realizar portabilidad sin verificar el consentimiento[131]; así como por tratar ilícitamente de datos al renovar una promoción sin el consentimiento del cliente y contra su decisión[132].

- En el sector bancario se evidencia que se sigue sancionando por reclamar mediante entidades de recobro, deudas a entidades bancarias que quedaron anuladas por sentencia judicial[133] o por utilizar datos de terceras personas sin permiso para crear cuentas bancarias a menores e ingresar el dinero de una

[126] Recuperado de: https://confilegal.com/20230425-kfc-pagara-25-000-euros-por-no-tener-delegado-de-proteccion-de-datos-y-por-irregularidades-en-la-politica-de-privacidad/ (fecha de consulta: 2023).
[127] Más información en Resolución AEPD PS-00448-2022.
[128] Recuperado de: https://confilegal.com/20230829-la-aepd-multa-con-5-000-euros-a-massimo-dutti-por-irregularidades-en-las-cookies-de-su-web/ (fecha de consulta: 2023).
[129] Más información en Resolución AEPD PS-006655-2022.
[130] Más información en Resolución AEPD PS-00553-2022.
[131] Más información en Resolución AEPD PS-000453-2022.
[132] Más información en Resolución AEPD PS-00553-2022.
[133] Más información en: Resolución AEPD PS-00482-2022.

Años 2023 y 2024 (hasta la fecha de depósito de la tesis)

herencia. Merece, en este sentido, especial atención la reciente sanción impuesta en verano de 2023 a una entidad bancaria online de 2,5 millones de euros por no facilitar medios seguros para el envío de información sobre Prevención de Blanqueo de Capitales[134].

En el sector bancario también destaca la sanción impuesta por la AEPD por falta de medidas de seguridad por una brecha que permitió que sus clientes pudieran ver datos sobre transferencias por otros con los que no tenían ninguna relación. Se trata de una de las sanciones más cuantiosas impuestas, tras un proceso de tres años y con una resolución oficial anonimizada al extremo, lo que impide extraer más detalles sobre la brecha o las medidas tomadas. La AEPD valoró la potencial afectación a un gran volumen de interesados y que durante la instrucción se detectaron graves deficiencias estructurales en cuanto a medidas de seguridad y diseño que podrían ser sancionadas en sí[135].

- Adicionalmente, se trae a colación la sanción impuesta por la AEPD a una empresa con 550.000 euros, por incumplimiento del RGPD y una vigilancia excesiva a los repartidores y permitir que cualquier empleado pudiera acceder al sistema de reparto y consultar datos. La AEPD consideró en este caso que la empresa tenía que haber aplicado las medidas que garantizasen que los datos tratados eran estrictamente necesarios para la finalidad explícita por la que fueron recogidos La sancionada ha interpuesto recurso de reposición que ha sido desestimado[136].

- Por último, se traen a colación las siguientes recientes sanciones:

  i) Sanción de la AEPD a un establecimiento por infracción del artículo 5.1. a), 13, 14 y 6 RGPD porque su software funcionaba como una extensión

[134] Recuperado de: https://www.economistjurist.es/actualidad-juridica/open-bank-sancionado-con-25-millones-de-euros-por-su-gestion-de-los-datos-personales/ (fecha de consulta: 2023).
[135] Recuperado de: https://www.aepd.es/documento/ps-00020-2023.pdf (fecha de consulta: 2024).
[136] Recuperado de: https://www.aepd.es/documento/reposicion-ps-00209-2022.pdf (fecha de consulta: 2024).

Años 2023 y 2024 (hasta la fecha de depósito de la tesis)	
	de *Chrome* permitiendo rastrear la apertura de los correos electrónicos a través de píxeles[137];
ii)	Sanción AEPD a un gimnasio de 27.000 euros por imponer como requisito a los usuarios o el acceso a sus instalaciones mediante huella dactilar. Aunque no entra a valorar la necesidad, sí enmarca: falta de consentimiento explícito, información insuficiente en política de privacidad, conservación del patrón de huella por periodo excesivo, base de legitimación mal elegida, finalidad no concretada, ausencia de mención a decisiones automatizadas, falta de concordancia entre las finalidades declaradas en la política de privacidad, el contrato de socio del gimnasio, el RAT y la evaluación de impacto, entre otras[138].
iii)	Sanción AEPD a una empresa con 6.000 euros por instalar por instalar una cámara de videovigilancia en el hall de un domicilio sin que el inquilino tuviese constancia. La empresa alegó que el Decreto Ley 50/2020 de 9 de diciembre de medidas urgentes para estimular la promoción de viviendas de protección oficial y de las nuevas modalidades de alojamiento en régimen de alquiler define el coliving como "alojamientos compartidos o con espacios comunes". La AEPD considera que la presencia de las cámaras supone "un tratamiento de datos desproporcionado a la finalidad del sistema". No se consideró ajustada a la normativa vigente en al ser un método de control excesivo "existiendo medidas menos lesivas"[139].
iv)	Sentencia de la Audiencia Provincial de las Islas Baleares de 8.000 euros a un cirujano por vulneración al derecho a la intimidad y la propia imagen de un paciente por publicar fotografías de su mamoplastia en una red social sin su consentimiento. Se considera que las imágenes publicadas no ilustran una noticia o información relacionada con la medicina o la

[137] Recuperado de: https://www.aepd.es/documento/reposicion-ps-00328-2022.pdf (fecha de consulta: 2024).
[138] Recuperado de: https://www.aepd.es/documento/ps-00413-2022.pdf (fecha de consulta: 2024).
[139] Recuperado de: https://www.aepd.es/documento/reposicion-ps-00496-2022.pdf (fecha de consulta: 2024).

Años 2023 y 2024 (hasta la fecha de depósito de la tesis)
ciencia, sino corresponden a una finalidad publicitaria y comercial. Se considera que las imágenes publicadas no ilustran una noticia o información relacionada con la medicina o la ciencia, sino corresponden a una finalidad publicitaria y comercial. Por tanto, estimó el recurso de la afectada y condena a la cirujana plástica al pago de una indemnización[140].
➢ Desde el punto de vista comparado, se constata que también se imponen cuantiosas sanciones, entre las que destacan las siguientes:
v) Sanción CNIL con 75.000 euros por recoger datos de prospectos sin un consentimiento válido, debido a la apariencia engañosa de sus formularios de concurso[141].
vi) Sanción de la autoridad holandesa The Dutch data protection authority con colaboración de la CNIL a Uber B.V. y Uber Technologies Inc. de 10 .000.000 de euros por varias omisiones a la hora de informar a los conductores[142.].

[140] Recuperado de: https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbH1CjUwMLA0NDYzN7JUK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMByEyHQUUAAAA=WKE (fecha de consulta: 2024).

[141] Recuperado de: https://www.cnil.fr/en/data-brokers-tagadamedia-fined-eu75000 (fecha de consulta: 2024).

[142] Recuperado de: https://www.cnil.fr/en/uber-dutch-data-protection-authority-imposes-eu10-million-fine (fecha de consulta: 2024).

Por tanto, como se indicaba, queda evidenciado que los incumplimientos de la normativa sobre protección de datos se producen en todos los sectores y por diversos motivos, habiendo alcanzado incluso al ámbito judicial, entre las que resaltan la sanción impuesta por la Audiencia Provincial de Barcelona a *Google* por no borrar el rastro digital en los buscadores a un indultado, como indemnización a su derecho al honor[143]; por la filtración derivada de la caída del sistema *online* de comunicación judicial *LexNET* o por la filtración de datos de sentencias del orden jurisdiccional penal o la recogida de documentos judiciales con datos personales en contenedores de ciertos Juzgados[144].

[143] Otras noticias destacadas, por orden cronológico, serían las siguientes: "Google acuerda pagar 22,5 millones de dólares por jugar sucio con Safari. La compañía ha violado una orden que le obligaba a respetar la privacidad de los usuarios del navegador Safari". Recuperado de: http://www.abc.es/20120810/medios-redes/abci-multa-google-safari-201208092154.html (fecha de consulta:2018); "Bruselas impone una multa millonaria a Facebook por mentir en la compra de WhatsApp". Recuperado de: https://www.efe.com/efe/espana/economia/bruselas-impone-una-multa-millonaria-a-facebook-por-mentir-en-la-compra-de-whatsapp/10003-3269695 (fecha de consulta: 2018); "Protección de datos multa a Google por captar con sus coches datos de WiFi privadas entre 2008 y 2010". Recuperado de: https://elpais.com/economia/2017/11/07/actualidad/1510047554_209959.html (fecha de consulta:2018); "Protección de Datos resuelve que es ilegal incluir a personas en grupos de WhatsApp sin su consentimiento". Recuperado de: https://elpais.com/tecnologia/2017/12/20/actualidad/1513786075_415535.html?rel=mas (fecha de consulta: 2017); "Se filtran los resultados del MIR 2018 y del EIR antes de que los publique el Ministerio de Sanidad". Recuperado de: http://www.elmundo.es/espana/2018/03/05/5a9d92d9e2704e157d8b45d4.html (fecha de consulta: 2018). "La AEPD sanciona a Facebook con 1,2 millones por vulnerar la normativa de protección de datos". Recuperado de: http://www.publico.es/economia/aepd-sanciona-facebook-1-200-000-euros-vulnerar-proteccion-datos-usuarios.html (fecha de consulta: 2019); "La Agencia de Protección de Datos sanciona a WhatsApp y Facebook en España: Les impone sendas multas de 300.000 euros por el tratamiento de la información de sus usuarios cuando se realizó la compra de la aplicación de mensajería", Resolución AEPD (R/00259/2018 de 15 de marzo de 2018); "La Agencia de Protección de datos multa a WhatsApp por insegura, pero la utiliza con menores de edad". Recuperado de: http://vozpopuli.com/economia-y-finanzas/empresas/Agencia-Protección-Datos-WhatsApp-insegura-proteccion-menores-multa-0-1121588904.html (fecha de consulta: 2019); "Miles de aplicaciones para Android podrían violar la ley al recopilar datos privados de los niños", en Reyes, I. (Corresponding Author); "Won't Somebody Think of the Children?", Examining COPPA Compliance at Scale", Magazine Proceedings on Privacy Enhancing Technologies, 2018, págs. 63-83; 10ª "La Agencia de Protección de Datos sanciona con 5.000 € a un médico tras perder imágenes de una paciente en una operación". Recuperado de https://www.lavanguardia.com/local/madrid/20181113/452903454744/la-agencia-de-proteccion-de-datos-sanciona-con-5000-a-un-medico-tras-perder-imagenes-de-una-paciente-en-una-operacion.html (fecha de consulta: 2022).

[144]Recuperado de: "El caso LexNET dejó al descubierto los problemas de empresas y Administración para cumplir la legislación de protección de datos". Recuperado de Paniagua, E. https://retina.elpais.com/retina/2017/08/11/tendencias/1502446063_042539.html (fecha de consulta: 2019); y "Justicia recoge de un contenedor de los juzgados de Valencia documentos judiciales con datos personales". Recuperado de http://www.elmundo.es/comunidad-valenciana/2018/04/26/5ae1a3c7ca4741995d8b4678.html (fecha de consulta:2018).

En quinto lugar, se evidencia que el riesgo de sanción de las empresas de todos los ámbitos y tamaños podría ser el mismo que antes de la regulación del RGPD, la diferencia es que ahora las sanciones son más en número, siendo la tendencia al alza, como se refleja, por ejemplo, en las Memorias que con carácter anual publica la AEPD. Así, la tendencia es que la cuantía de las sanciones en materia de protección de datos sea mayor, recayendo la carga de la prueba de demostrar el cumplimiento en el responsable del tratamiento, de ahí, la importancia de no solo cumplir sino guardar una trazabilidad y documentarlo, generando las oportunas evidencias del cumplimiento.

En definitiva, se ha constatado durante el periodo investigador que, aunque se va en la dirección correcta, queda trabajo por hacer para conseguir una cultura y normativa de protección de datos a nivel global y en todos los niveles. Como ejemplos de instrumentos para demostrar cumplimiento con la normativa de protección de datos pueden ser la llevanza como responsable y como encargados del tratamiento de un RAT con el contenido mínimo previsto en el artículo 30 del RGPD (nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del DPO; fines del tratamiento, categorías de interesados y de datos personales; categorías de destinatarios, los plazos de conservación; en su caso las transferencias internaciones y las medidas técnicas y organizativas de seguridad del artículo 32 RGPD) o de una forma más completa.

También, la formación y concienciación periódica, así como disponer e implantar (y mantenerlos actualizados) textos legales adaptados a la empresa u organización que se trate, como políticas de protección de datos y políticas de Cookies, guías o manuales de protección de datos, procedimientos (como de gestión y notificación de brechas de seguridad, videovigilancia, de gestión del ejercicio de derechos); así como Códigos de buenas prácticas en protección de datos. Otros mecanismos serían los procedimientos de gestión del riesgo y de evaluación de impacto en tratamientos de datos personales y del nivel de riesgo de vulneración a la protección de datos[145].

[145] Recuperado de: https://www.aepd.es/es/guias-y-herramientas/guias (fecha de consulta: 2022).

4. Principales hitos jurídicos sobre la protección de datos en el ordenamiento jurídico español, con especial referencia a la LOPDGDD 3/18.

A modo introductorio, en el ordenamiento jurídico español la protección de datos configura un derecho fundamental consagrado en el texto constitucional en el artículo 18.4 CE - que dispone: "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"[146].

Así, la protección de datos configura un derecho autónomo e independiente, tal y como ha reiterado el Tribunal Constitucional. Por todas, se citan la Sentencias TC de noviembre de 2000, nº 290/2000 y nº 292/2000, en su Fundamento Jurídico 7, refiriéndose de forma expresa a esta última, el Preámbulo de la legislación específica española vigente sobre protección de datos, la LOPDGDD 3/18; junto a la Sentencia del TC nº 94/1998, de 4 de mayo, que ya aclaraba que la protección de datos constituye un derecho fundamental.

En cuanto al régimen jurídico, además de la aplicación directa de la normativa europea, el RGPD, y, por ende, sus principios, limitaciones, garantías y derechos reconocidos a los interesados; resulta de aplicación la legislación específica, la LOPDGDD 3/18, en vigor desde el 6 de diciembre de 2018. Como se ha indicado anteriormente, la LOPDGDD 3/18 derogó la anterior regulación LOPD 15/1999, desarrollada por el Real Decreto 1720/2007 para adecuarla a las líneas y principios del RGPD. Esta, a su vez, sustituyó a la anterior Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD, en adelante).

[146] Basta reseñar que ya desde el año 1978, con la CE, el legislador y la sociedad eran conscientes de los riesgos que el uso de la informática generaba sobre los derechos a la intimidad y familiar de los ciudadanos y el pleno ejercicio de los derechos. Lo que se materializó en la inclusión del transpuesto apartado 4 del art. 18 CE.

A) Especial referencia a la LOPDGDD 3/18.

Partiendo del régimen jurídico en el marco europeo, de igual forma ocurre que cada una de las cuestiones que regula la LOPDGDD 3/18 es susceptible de ser objeto de una investigación y tesis individual, siendo el objeto de la presente tesis la realización de las proyecciones de este derecho fundamental en áreas de convergencia con otros derechos fundamentales. Dicho esto, la LOPDGDD 3/18 constituyó un hito jurídico básico en el ordenamiento jurídico español, que vino a "adaptar" la normativa europea, aunque ya era directamente aplicable al ser un Reglamento; desarrollar las materias previstas sobre las que este permite adaptación en la legislación nacional, como la determinación de la edad para que el menor de un consentimiento válido; pero también, vino a reforzar los derechos, clarificar conceptos, y, en definitiva, tratar de dar seguridad jurídica a los operadores jurídicos.

En virtud de lo anterior, las principales particularidades básicas a las que nos referiremos sobre el LOPDGDD 3/18 son las siguientes:

1. **Principios de protección de datos y derechos ejercitables**
2. **Disposiciones aplicables a tratamientos concretos**
3. **AEPD y régimen sancionador**
4. **Garantías de los derechos digitales – Título X**

1. **Principios de protección de datos y derechos ejercitables:** en línea con el RGPD, la LOPDGDD 3/18 regula principios de protección de datos y derechos en materia de protección de datos de forma similar a los previstos en la normativa europea, como los principios de exactitud o el deber de confidencialidad de los responsables y encargados del tratamiento y de las personas que intervengan en cualquier fase del tratamiento, complementario del deber de secreto profesional.

   Respecto a los derechos en materia de protección de datos, reconoce también los derechos a la transparencia e información, además de los derechos de acceso, rectificación, supresión, limitación del tratamiento, derecho a la portabilidad y oposición.

En cuanto al tratamiento basado en consentimiento, prevé igualmente que ha de cumplir los requisitos del artículo 4 RGPD y que cuando un tratamiento se pretenda basar en esta base para una pluralidad de finalidades será preciso que conste para todas ellas. Así mismo, introduce la especialidad respecto al consentimiento de menores de edad, estableciendo que únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años, lo que supone una matización nacional del periodo previsto en el RGPD.

2. **Disposiciones aplicables a tratamientos concretos**: la LOPDGDD 3/18 regula una serie de disposiciones aplicables a tratamientos concretos, como los sistemas de información crediticia[147], tratamientos con fines de videovigilancia[148], los sistemas de exclusión publicitaria[149] o los sistemas de información de denuncias internas, modificado por la disposición final 7 de *Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*[150].

   i) Al respecto de los sistemas de exclusión publicitaria, según la LOPDGDD 3/18 (artículo 23), será lícito el tratamiento que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. A tal efecto, prevé que podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados.

   Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a

[147] Véase el art. 20 LOPDGDD 3/18.
[148] Véase el art. 22 LOPDGDD 3/18.
[149] Véase el art. 23 LOPDGDD 3/18. Recuperado de: https://www.aepd.es/areas-de-actuacion/publicidad-no-deseada (fecha de consulta: 2023).
[150] Se modifica por la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513#df-7 (fecha de consulta: 2022). El artículo 24 de LOPDGDD 3/2018, de 5 de diciembre, que queda redactado como sigue: "Artículo 24. Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.
Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.
Dichos tratamientos se regirán por lo dispuesto en el RGPD, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción."

las procedentes de determinadas empresas. Además, prevé que cuando un afectado manifieste su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, el responsable de tratamiento deberá informarle de los sistemas de exclusión publicitaria existentes (como el *Servicio de Lista Robinson*), pudiendo remitirse a la información publicada por la autoridad de control competente.

De igual manera, se establece que quienes pretendan realizar comunicaciones de mercadotecnia directa (forma de comunicación de marketing que utiliza uno o más medios para comunicarse directamente con un público objetivo y obtener de él una respuesta medible)[151], deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo.

ii) En lo referido a los sistemas de información de denuncias internas, los denominados "canales de denuncias", cabe resaltar que son regulados de forma específica por la citada *Ley 2/2023, con la que se incorporaba al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019*. Esta reconocía en su Preámbulo que ya la LOPDGDD 3/18 contemplaba la creación y mantenimiento de sistemas de información mediante los que pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión (en el seno de la misma o en la actuación de terceros que contratasen con ella) de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

En particular, la citada Ley 2/2023 busca proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados. Fundamentalmente establece el régimen jurídico del Sistema interno de información, que abarca tanto el canal de denuncias (entendido como buzón o cauce para recepción de la información), como el

[151] Recuperado de: https://es.wikipedia.org/wiki/Mercadotecnia_directa (fecha de consulta: 2023).

Responsable del Sistema interno de información y el procedimiento de gestión de informaciones. Imponía que la configuración del Sistema debe reunir determinados requisitos, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante. Asimismo, resulta indispensable para la eficacia del Sistema interno de información la designación del responsable de su correcto funcionamiento.

Por último, destacar de la citada Ley 2/2023 los siguientes puntos que se mencionan que no se explican en profundidad por centrarnos en el objeto del presente trabajo investigador, pero se considera de interés hacer referencia a los mismos:

a) permite la comunicación anónima al considerar que los canales de denuncias anónimas "han colaborado a instituir un instrumento esencial para el cumplimiento de una empresa y ha sido fundamental para poder recibir denuncias graves que de otra manera las personas trabajadoras y los colaboradores no se atreverían a señalar por temor a represalias en caso de ser identificados";

b) regula el régimen del tratamiento de datos personales que deriven de la aplicación de esta ley, expresando que se regirán por el RGPD, la LOPDGDD 3/18 y la Ley Orgánica 7/2021; y

c) obliga a disponer de un sistema interno de información a las personas físicas o jurídicas del sector privado que tengan contratados a 50 o más trabajadores, las personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la UE en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente y también, los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

3. **AEPD y régimen sancionador:** la LOPDGDD 3/18 dedica un apartado a regular la AEPD (estableciendo una colaboración con el CGPJ en aras del adecuado ejercicio de las respectivas competencias que a este atribuye la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial o LOPJ), el procedimiento en caso de posible vulneración de la normativa de protección de datos y el régimen sancionador.

   Distingue entre infracciones consideradas "muy graves" (como el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 RGPD, sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 RGPD o la utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello); "graves" (la falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados; No disponer del registro de actividades de tratamiento establecido en el artículo 30 RGPD o el incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento).

   Por último, como infracciones "leves", como el incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 RGPD; el incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento; o el incumplimiento de la obligación de documentar cualquier violación de seguridad.

   Más adelante, se analizará en el apartado C) el creciente ritmo sancionador de la AEPD y la tendencia de las sanciones, a la vista de las últimas Memorias Anuales publicadas por la AEPD.

4. **Garantías de los derechos digitales- Título X:** otra de las particularidades de la LOPDGDD 3/18 es que parte del principio de plena aplicabilidad de internet a los derechos y libertades reconocidos, como a la vida, la seguridad o a la libertad religiosa y los prestadores de servicios contribuirán a garantizar su aplicación y además, incluía la novedad de un Título específico dedicado a las "Garantías de los derechos digitales", cuya consagración legal configuró un hito jurídico y cuyo análisis es el objeto de la publicación que conforma el Capítulo II de la presente investigación, a la que nos remitimos.

   La LOPDGDD 3/18 se refiere también a las facultades de acceso universal, asequible y de calidad a internet independientemente de toda condición personal, social o económica; de neutralidad de internet (que implica que los proveedores de internet oferten sus servicios de forma transparente sin discriminación a usuarios por motivos económicos o técnicos y seguridad digital; las comunicaciones se transmitan y reciban de forma segura; y los usuarios sean informados de sus derechos). También, se refiere al testamento digital, al derecho de desconexión digital del trabajador y a la educación digital por su implicación en la sociedad, pues la formación en todos los niveles en el correcto, legal, ético y apropiado uso de los medios digitales, así como de los riesgos y consecuencias derivados de su uso, contribuirá a un mayor respeto de los derechos fundamentales y libertades públicas en el entorno digital, y en particular, a fomentar la cultura de la protección de datos.

   Especialmente novedosa fue la regulación del testamento digital, en relación con el que establece que las personas "vinculadas" al fallecido por razones familiares o, de hecho, así como sus "herederos" están legitimados al acceso a los contenidos gestionados por el prestador de servicios de la sociedad de información y de decidir sobre su uso, destino o supresión. Ello, salvo que el fallecido lo hubiera prohibido expresamente o así se establezca legalmente. Cabe señalar como otros legitimados el albacea o el Ministerio Fiscal. De ahí, que se evidencia el riesgo de que resulten afectados derechos de terceros, como puede ocurrir al acceder a conversaciones, mensajes o fotografías.

   Finalmente, en cuanto a la significación jurídica del reconocimiento, se ha evidenciado que más que una nueva generación de derechos, las garantías digitales configuraron facultades ligadas a los derechos fundamentales a la

protección de datos y a la intimidad personal y familiar. Al mismo tiempo, se ha constatado que su efectividad puede presentar limitaciones en la práctica, porque su reconocimiento ha de completarse con medidas de apoyo y financieras efectivas, así como con garantías de control por parte de las autoridades competentes. También, debido a la falta de trayectoria doctrinal y jurisprudencial consolidada, precisando ser interpretados y concretado su contenido por parte de los órganos judiciales y autoridades competentes; y trasladados a medidas y protocolos de cumplimiento concretos a concretar por parte de las empresas e instituciones.

B) Modificación de la LOPDGDD 3/18 por la Ley 11/2023.

A modo de actualización, en el año 2023 se publicó la *Ley 11/2023, en transposición de varias Directivas de la UE, el 8 de mayo de 2023*, que introdujo varias modificaciones de gran relevancia en la LOPDGDD3/18 y en la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSICE, en adelante).

Centrándonos en las modificaciones que afectan a la LOPDGDD 3/18, las principales novedades estarían relacionadas con el cambio de configuración del apercibimiento, que, si tenía la consideración de una sanción, pasa ser una medida de naturaleza no sancionadora, dentro de las competencias correctoras de la AEPD. De otro lado, se modifica el procedimiento sancionador ampliando sus plazos y la duración de las medidas previas de investigación por la complejidad de los asuntos. Así, se incluye un nuevo apartado que regula las actuaciones de investigación a través de sistemas digitales, a discreción de la AEPD y previa conformidad del inspeccionado en relación con su uso y funcionamiento. Sistemas que se podrán usar para el intercambio de documentos e información para regular la opción de realizar investigaciones o remotas.

Además, se amplió la duración máxima de las actuaciones previas de investigación de 12 a 18 meses y del procedimiento sancionador de 9 a 12 meses y se añade un nuevo apartado que prevé la posibilidad de que, a condición de que se demuestre haber adoptado medidas para cumplir con la norma aplicable, la AEPD archive la reclamación y adopte soluciones correctivas, alternativas o más moderadas, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos previstos.

Adicionalmente, con la modificación, se elimina la posibilidad de sanción con apercibimiento y se crea un procedimiento de apercibimiento como específico, más flexible y rápido, con una duración máxima de 6 meses, que, según manifiesta la AEPD, permitirá agilizar la respuesta a reclamaciones presentadas por ciudadanos.

También, se introdujo la Disposición Adicional vigésima tercera que prevé la posibilidad de que la AEPD establezca modelos de presentación de reclamaciones en los ámbitos de su competencia, de uso obligatorio para los interesados, ya estén (o no) obligados a relacionarse electrónicamente con las Administraciones Públicas. Estos modelos serán publicados en el Boletín Oficial del Estado (BOE) y en la Sede Electrónica de la AEPD y, según interpreta la AEPD, serían de obligado cumplimiento al mes de su publicación y facilitarán y simplificarán la presentación de reclamaciones[152].

Por tanto, las modificaciones introducidas son relevantes y tendrán que ser tenidas en cuenta, así como las directrices, instrucciones y orientaciones que da la AEPD, así como el CEPD[153].

C) Análisis de las últimas Memorias publicadas de la AEPD de 2021 y 2022

Expuesto lo anterior, del análisis de las Memorias que con carácter anual publica la AEPD se refuerza la evidencia del incremento de sanciones por vulneración de la normativa de protección de datos a nivel internacional, europeo y español, siendo además la tendencia al alza. Así, en línea con el segundo objeto de la tesis (que se recuerda es evidenciar que, aunque han sido grandes los avances en la tutela de este derecho, aún queda trabajo por hacer para conseguir una conciencia en todos los niveles y una cultura global sobre protección de datos, armonizada y con homogeneidad regulatoria), se evidencian los resultados de las últimas Memorias anuales de la AEPD que se trasladan de forma comparativa:

[152] Acceso a los modelos publicados en el Boletín Oficial del Estado en el siguiente enlace: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-16062. Resolución de 29 de junio de 2023, de la Dirección de la Agencia Española de Protección de Datos, por la que se aprueban los modelos de presentación de reclamaciones.
[153] Recuperado de: https://edpb.europa.eu/edpb_en (fecha de consulta: 2023).

Notificaciones de brechas de seguridad:

- En la Memoria de 2021, se refleja que las brechas de seguridad causadas por ciber incidentes de origen externo malintencionado seguían teniendo el mayor protagonismo, siendo 1647 notificaciones de brechas gestionadas entre el 1 de enero de 2021 y el 31 de diciembre de 2021; considerando que los responsables y encargados del tratamiento deben ser particularmente diligentes para aplicar medidas técnicas y organizativas[154] adecuadas para poder afrontar las brechas de seguridad.

- En la Memoria de 2022 se informaba que se había gestionado un mayor número de notificaciones de brechas de seguridad, un total de 1751 notificaciones y, además, se han generado 31 requerimientos a los responsables; lo que se preveía seguirá al alza y así se reflejará en la Memoria anual de 2023.

Hitos relevantes:

- La Memoria de 2021 señalaba como hito relevante de 2021 el relativo al desarrollo y cumplimiento del "Plan de Responsabilidad Social de la AEPD". Otro aspecto clave es que se hace referencia al desarrollo de una nueva iniciativa a promover un gran acuerdo por la convivencia ciudadana en el ámbito digital compatibilizando la protección de datos con la innovación, la ética y la competitividad empresarial: El Pacto Digital para la Protección de las Personas, finalizando el año con 349 entidades adheridas.

- La Memoria de 2022 señala como una de las principales preocupaciones del entorno digital relacionado con el acceso por menores a dispositivos móviles, al periodo que los utilizan y los servicios de internet que acceden[155]. Además, se

[154] En cuanto a las medidas de seguridad, a modo de ejemplo entre las técnicas se encuentran el cifrado o la pseudonimización, y como organizativas la implementación de códigos de conductas, mecanismos de certificación, políticas internas de protección de datos; además se precisa la necesidad de realizar auditorías o medidas de evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas.

[155] En esta línea se ha publicado el 14 de diciembre de 2023 un Decálogo de Principios. Verificación de edad y sistemas de protección de personas menores de edad ante contenidos inadecuados disponible en el siguiente enlace. Recuperado de: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf (fecha de consulta: 2023).

centra en que los desafíos para la privacidad son el uso de la IA por los poderes públicos y empresas privadas, el tratamiento de datos a una escala desconocida hasta ahora, planteando el uso de "espacios de datos" como un modelo de tratamiento de gran complejidad organizativa y tecnológica, así como el escalado en la diversidad de categorías de datos procesadas, número de sujetos afectados, ámbitos involucrados, intervinientes y otros.

En tal sentido, expresa que cuando en él se realicen tratamientos, el cumplimiento del principio de responsabilidad proactiva exige la aplicación de medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento cumple con la normativa, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento. Así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.

Cifras de multas y reclamaciones:

- Refleja la Memoria de 2021 el incremento en las cifras de multas impuestas guarda relación con el mayor número de procedimientos sancionadores resueltos y también, denota un incremento en la envergadura y complejidad de los casos derivado a su vez de las magnitudes de los tratamientos de datos investigados. Señala como muestra de ello la imposición de varias multas por un importe superior al millón de euros, de las cuales cinco son ya ejecutivas, y que el importe medio de las multas se haya triplicado con respecto al año anterior[156].

  En conexión con lo anterior, se refleja un significativo incremento, de más del 90% con respecto al año 2020, de las reclamaciones relacionadas con la promoción publicitaria, que supusieron casi un 15% del total de reclamaciones registradas. Precisa que el 70% de las reclamaciones vinculadas con la promoción publicitaria se referían específicamente a la recepción de llamadas telefónicas no deseadas. También, considera que fueron numerosas las reclamaciones por suplantación de la identidad de la persona reclamante, de hecho, en la Memoria de 2022 pasa a formar parte de las áreas más sancionadas.

[156] Como multas superiores al millón de euros destacan sanción a Caixabank, Amazon Road, Transport Spain SL y Google LLC. Recuperado de: https://www.aepd.es/es/documento/memoria-aepd-2022.pdf (fecha de consulta: 2023).

- La Memoria anual de 2022 refleja un incremento del número de reclamaciones en el ámbito online, más de un 40% con respecto a 2020, hasta situarse en casi un 20% del total de reclamaciones registradas[157]. Además, según la Memoria de 2021 las reclamaciones recibidas en la AEPD han alcanzado una cifra sin precedentes, con un total de 13.324, superando las 10.324 reclamaciones presentadas en el año 2020.

  El número de reclamaciones resueltas ha sido también extraordinario, y un 35% superior al año anterior. En la Memoria de 2022 se informa que la tasa de reclamaciones resueltas frente a reclamaciones recibidas se ha mantenido en el entorno del 100 %. Se especifica un total de 14.3937 reclamaciones resueltas. Adicionalmente, considera que se observa un aumento del número de multas impuestas por la AEPD, si bien el importe total se reduce debido a una disminución en el número de grandes procedimientos resueltos durante este último año frente a lo sucedido el año pasado.

Top áreas de actividad con mayor número de reclamaciones:

- El último aspecto para destacar de las últimas Memorias anuales de la AEPD es que las top áreas de actividad con mayor número de reclamaciones recibidas serían: Servicios de internet, video vigilancia, publicidad (excepto o correo no deseado), ficheros de morosidad, reclamación de deudas, Administración Pública, Sanidad, Comercios, transporte y hostelería, Entidades financieras/acreedoras y publicidad a través de email o móvil.

  Por último, resulta relevante que en la Memoria de 2022 se mantienen las áreas en el mismo orden, salvo Comercios, transporte y hostelería que adelanta a la Administración Pública, y entran contratación fraudulenta y sanidad. Destaca así mismo, que los seis temas con mayor importe total en 2022 de multas son servicios de internet, publicidad (excepto *spam*), asuntos laborales, brechas de datos, contratación fraudulenta y telecomunicaciones.

[157] En particular, los hechos se refieren, en una proporción importante, a la difusión no consentida de datos personales en sitios web, particularmente en redes sociales y servicios equivalentes de la sociedad de la información, y a la desatención de las solicitudes de supresión dirigidas a los prestadores de servicios, que en no pocas ocasiones presentan deficiencias informativas en sus políticas de privacidad.

D) Resultados.

En primer lugar, se ha evidenciado que la LOPDGDD 3/18 constituyó un hito jurídico básico en el ordenamiento jurídico español, que vino a “adaptar” la normativa europea, aunque ya era directamente aplicable; desarrollar las materias previstas sobre las que este permite adaptación en la legislación nacional, como la determinación de la edad para que el menor de un consentimiento válido; pero también, vino a reforzar los derechos, clarificar conceptos, y, en definitiva, tratar de dar seguridad jurídica a los operadores.

En segundo lugar, en cuanto a los derechos y garantías digitales reconocidos en el Título X de la LOPDGDD 3/18, se ha evidenciado a lo largo del periodo investigador que más que una nueva generación de derechos configuró facultades ligadas a los derechos fundamentales a la protección de datos y a la intimidad personal y familiar. Al mismo tiempo, se ha evidenciado que su efectividad puede presentar limitaciones en la práctica, porque su reconocimiento ha de completarse con medidas de apoyo y financieras efectivas, así como con garantías de control por parte de las autoridades competentes. También, debido a la falta de trayectoria doctrinal y jurisprudencial consolidada, precisando ser interpretados y concretado su contenido por parte de los órganos judiciales y autoridades competentes; y trasladados a medidas y protocolos de cumplimiento concretos a concretar por parte de las empresas e instituciones.

En tercer lugar, se ha hecho referencia a que en el año 2023 se publicó la Ley 11/2023, en transposición de varias Directivas de la UE, el 8 de mayo de 2023, que introdujo varias modificaciones de gran relevancia en la LOPDGDD3/18, como la ampliación de la duración máxima de las actuaciones previas de investigación de 12 a 18 meses y del procedimiento sancionador de 9 a 12 meses y se añade un nuevo apartado que prevé la posibilidad de que, a condición de que se demuestre haber adoptado medidas para cumplir con la norma aplicable, la AEPD archive la reclamación y adopte soluciones correctivas, alternativas o más moderadas, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos previstos.

En cuarto lugar, y teniendo en cuenta las sanciones en las tablas por orden cronológico, en las que se reflejan numerosas sanciones de la AEPD, se ha constatado que casi seis años tras la entrada en vigor y aplicación, del RGPD y de la LOPDGDD

3/18 se sigue sancionando a empresas por infracciones reiteradas o incluso por obligaciones básicas, por lo que se estima que el riesgo de sanción podría ser el mismo que antes. La diferencia puede ser que ahora las sanciones son más, en particular la autoridad de control española evidencia en sus Memorias Anuales el ritmo sancionador y el incremento de sus sanciones por vulneración de la normativa de protección de datos, siendo además la tendencia al alza (al mismo tiempo que aumentan las cifras de cibercriminalidad), como se prevé se reflejará en la Memoria del año 2023 que se publicará próximamente.

Por último, se ha constatado que el uso generalizado de las TIC, las redes sociales, la red de internet, la IA y el resto de las herramientas digitales, generan escenarios en los que se generan retos y desafíos para la protección de datos personales, a la vez que sigue aumenta la preocupación social por la importancia de respetar y hacer respetar este derecho fundamental y cumplir la normativa reguladora.

En cumplimiento del segundo objetivo de la tesis, se ha confirmado que la tutela de los datos personales y de los derechos digitales sigue configurando uno de los retos actuales en todos los ámbitos y en particular, del Derecho Constitucional, debiendo ser el objetivo común compartido seguir promocionando la cultura de la protección de datos, la responsabilidad proactiva de cumplimiento y la concienciación en el respeto de los derechos digitales con la finalidad de que sean respetados y percibidos por la sociedad como una necesidad inherente a la dignidad humana. Tal y como se viene afirmando a lo largo de la presente tesis.

5. Concepto de protección de datos personales y su delimitación del derecho a la intimidad personal y familiar. Nociones sobre el juicio de ponderación de derechos.

A) Concepto de protección de datos personales.

Teniendo en cuenta lo expuesto en los anteriores apartados, se cierra el primer Capítulo concretando y completando la definición de "protección de datos", a la que nos hemos referido e incluso adelantado en su significado anteriormente y a la que nos referiremos en las Publicaciones de los Capítulos siguientes; así como también, refiriéndonos más adelante a su delimitación del derecho a la intimidad personal y familia, junto con unas nociones básicas sobre el juicio de ponderación de derechos.

Protección de datos personales:

Pues bien, aunque existen múltiples y diversas definiciones sobre qué se entiende por protección de datos, y su concepto actual ha sido fruto de un importante desarrollo como se ha expuesto, el derecho a la protección de datos personales (también denominado derecho de libertad informática, de *habeas data* o de autodeterminación informativa[158]) se refiere a la facultad de la persona física de controlar el uso y destino de su información personal por terceros distintos del interesado titular, ya sean particulares, agentes, organizaciones o empresas, públicas o privadas.

Por ende, la protección de datos implica la facultad de toda persona física de decidir qué datos personales facilitar, a quién, para qué y comprende otros, como el derecho a solicitar el acceso, la rectificación o cancelación de los datos, oponerse a su tratamiento o limitar su tratamiento. Control que se realiza, principalmente, para

[158] El Tribunal Constitucional de la República Federal de Alemania, en sentencia de 15 de diciembre de 1983, elaboró el concepto de autodeterminación informativa. Fuente: Cuervo Álvarez, J, "Autodeterminación informativa", 2014. Recuperado de: http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/#1.1.%20ASPECTOS%20GENERALES (fecha de consulta: 2023). De ahí, que el derecho a la protección de datos también se denomine *habeas data* o derecho de autodeterminación informativa.

proteger, respetar e impedir su tráfico o tratamiento ilícito o lesivo para la dignidad y los derechos de su titular[159].

Desde el punto de vista jurisprudencial de construcción, se trae a colación que fue esencial la del Tribunal Constitucional Federal de Alemania, citándose por todas la Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, que declaró inconstitucional algunos artículos de la Ley del Censo en 1983 estableciendo los elementos esenciales de del derecho de protección de datos o como lo denominada, de autodeterminación informática; y otra de 2008, Sentencia del Tribunal Constitucional Alemán, de 27 de febrero de 2008, por la que se declara inconstitucional la norma que posibilita los registros *on line* de sistemas informáticos, en la que precio el alcance del derecho en relación con la integridad y confidencialidad de las TIC.

Dicho esto y al hilo de lo anterior, se evidencia que en su concepción actual "protección de datos" no es un concepto idéntico a la "privacidad", concepto anglosajón más amplio, que, aunque varía dependiendo del sistema jurídico de cada país (*Common Law* o Derecho Romano Germánico), con carácter general englobaría tres derechos fundamentales: el derecho fundamental a disfrutar de una vida sin intromisiones indeseadas, el derecho a libertad de comunicación sin el temor a ser vigilado y el derecho al control de acceso a la información personal. En cambio, protección de datos es un concepto específico de tutela de la información personal, la información concreta en el que el titular de los datos es el propio individuo, es decir, busca tutelar el derecho a la protección de dichos datos de las personas.

En cuanto a qué se entiende por "dato personal" en amplio sentido, comprendería toda la información que identifica o hace identificable a una persona física[160], por ejemplo,

[159] Guía Rápida Protección de Datos. Aplicación del RGPD, Francis Lefevre, ISBN: 978-84-17317-41-6, 2019, págs. 9 y ss.

[160] A efectos de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980, los datos personales son "cualquier información relacionada con un individuo identificado o identificable" (sujeto de los datos). En *Resumen, Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, pág. 4. A efectos del vigente RGPD, dato personal es "toda información sobre una persona identificada o identificable "el interesado") art. 3 RGPD. Siguiendo la regulación europea, "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (art. 4. 1. RGPD).

su nombre y apellidos, su correo electrónico, una dirección IP o un DNI. Nos referimos tanto a los datos normales, ordinarios o *regular data* (nombre, teléfono, dirección de correo electrónico, imagen, currículum vitae), como a las categorías especiales de datos (datos biométricos, relacionados con la religión, las opiniones políticas, la afiliación a un sindicato, la salud o la sexualidad).

Al respecto del DNI, se trae a colación la resolución en la que la AEPD confirmaba que "El identificador numérico del DNI junto con el carácter de verificación correspondiente al número de identificación fiscal identifica a una persona física de modo indubitado. Esta cualidad lo convierte en un dato particularmente sensible pues, en la medida en que su tratamiento no vaya acompañado de las medidas técnicas y organizativas necesarias para garantizar que quien se identifica con él es realmente su titular, un tercero puede suplantar la identidad de una persona física con total facilidad, o, con otras palabras, puede provocar un fraude de identidad, con los riesgos que ello comporta para la privacidad, el honor y el patrimonio del suplantado"[161].

A sensu contrario, el resto de los datos que no se comprenden en la anterior definición de "dato personal", esto es, aquellos que no identifican o hacen identificable a una persona física son considerados como datos no personales. En concreto, y siguiendo la normativa europea de protección de datos, cuando se trata de datos de carácter personales será de aplicación el RGPD, y cuando no tengan tal consideración, lo será el *Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea*. Este último se limita a definir en su art. 3.1) los datos como aquellos que no sean datos personales tal y como se definen en el artículo 4, punto 1 del RGPD.

Con independencia de que un dato de carácter especial o no, es necesario proteger la totalidad de los datos personales de las personas físicas, pues una persona puede considerar que su salario o su dirección de residencia o de trabajo como un dato íntimo o sensible, y podría vulnerarse este derecho si esa información en concreto se difunde o un tercero no autorizado accede a ellos.

[161] Recuperado de: https://www.aepd.es/es/documento/ps-00012-2022.pdf (fecha de consulta:2024).

En consecuencia, toda persona que realice operaciones de tratamiento de datos personales, entendido como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (artículo 4 RGPD)", habrá que determinar (previamente y siguiendo los principios de protección de datos y la normativa) el carácter de los datos que van a ser objeto de tratamiento. Esto es, si son personales o no, sensibles o no, cuál es la base de legitimación para su tratamiento, realizar un análisis de riesgos, entre otras operaciones para garantizar el uso legítimo de los datos y conforme a los principios básicos de tratamiento.

Características esenciales de la protección de datos:

De otro lado, entre las características esenciales del derecho a la protección de datos, además de las ya expuestas con anterioridad, destacan que se configura como un auténtico derecho fundamental de cuarta generación, esto es, propio de las sociedades tecnológicas o avanzadas; cuya evolución y desarrollo ha sido progresiva en el tiempo, siendo en las últimas décadas y especialmente, años en las que se ha evidenciado una mayor evolución en su tutela y garantía, además de su internacionalización, especialmente en el ámbito europeo.

Así mismo, es un derecho transversal, pues tiene influencia e implicación en todos los ámbitos, siendo abordado en este estudio desde la perspectiva del Derecho Constitucional.

Desde la perspectiva del ordenamiento jurídico español, es, además, un derecho fundamental constitucional, sobre el que se ha pronunciado nuestro TC como máximo intérprete de la CE, que a través de sus resoluciones se ha precisado que es un derecho que deriva del artículo 18.4 CE. De dicho carácter de fundamental en el ordenamiento jurídico español derivan los efectos de garantía previstos en el art. 53 CE, en sus apartados primero y segundo.

Respecto a artículo, que se sitúa en el Capítulo Segundo del Título I CE, sobre los derechos y libertades comprendidos en los artículos 14 a 38 CE, “vincula a todos los poderes públicos” y “sólo por ley, que en todo caso deberá de respetar su contenido esencial, podrá regularse su ejercicio, que se tutelará conforme el art. 161.1 a)”. Este último precepto se refiere al recurso de inconstitucionalidad, competencia del TC (artículo 53.1 CE), regulado en la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional o LOTC en sus artículos 31 y siguientes.

Así, el derecho a la protección de datos no solo vincula a los poderes públicos, sino también a la generalidad de personas, físicas o jurídicas, que en el ejercicio de su actividades o funciones han de respetar los derechos fundamentales, en particular el derecho a la protección de datos.

En esta línea, el RGPD partía de que la protección de datos es un derecho con carácter fundamental, como expresa su Considerando nº 1; y aunque no es un derecho absoluto, como expresa su Considerando nº 4, “debe estar concebido para servir a la humanidad” y “considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad”.

De ahí, que protección de datos es, en su concepción actual, un derecho limitado y no absoluto, como los derechos fundamentales, siendo susceptible de ceder ante un interés o derecho constitucional, como puede ocurrir con el derecho a la libertad de expresión o de información veraz (artículo 20 CE). Es por ello por lo que otras de sus principales cualidades es que se encuentra estrechamente relacionado con otros derechos y libertades fundamentales (intimidad, honor, tutela judicial efectiva).

El presente trabajo investigador se centra en la “Protección de datos personales y su proyección en áreas de conflicto o convergencia con otros derechos fundamentales”, como puede ocurrir con el derecho a la intimidad personal y familiar consagrado en el artículo 18.1 CE, en el que incluso se consideraba incluido inicialmente aunque como más adelante precisó el TC español pasó a considerarse un derecho autónomo e independiente, que sirve a la función de garantizar a la persona un poder de control

del uso y destino sobre sus datos personales (la citada STC nº 292/2000, de 30 de enero, Fundamento Jurídico 6) [162].

A mayor abundamiento, la referida sentencia STC nº 292/2000 afirmó que el derecho a la protección de datos incorpora un instituto de garantía frente a "(…) "una forma de amenaza concreta a la dignidad y a los derechos de la persona", y que es "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática", lo que se ha dado en llamar "libertad informática"[163] (STC 254/1993, de 20 de julio, Fundamento Jurídico 6, reiterado luego en las SSTC 143/94, Fundamento Jurídico 7, 11/1998, Fundamento Jurídico 4, 94/1998, Fundamento Jurídico 6 202/1999)".

B) Delimitación del derecho a la intimidad personal y familiar.

En cuanto a la delimitación del derecho de protección de datos y el derecho a la intimidad personal y familiar, como se ha indicado, aunque inicialmente se entendía integrado en este, con el tiempo se delimitaron como derechos interrelacionados, pero independientes y autónomos, no siendo fácil de delimitar en ciertos casos.

Su principal diferencia radica en que, mientras el derecho a protección de datos se refiere a la facultad de toda persona de controlar el uso y destino de la información personal por parte de terceros distintos de su titular, tal y como se ha evidenciado anteriormente; el derecho a la intimidad implica el ámbito de la persona libre de injerencias ajenas, de terceros.

[162] La resolución citada resuelve un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra incisos de los arts. 21.1 "comunicación de datos entre AAPP" y 24.1 y 2 "otras excepciones a los derechos de los afectados "LOPD 15/99 por vulneración de los arts. 18.1 y 4 y 53.1 CE. Consideraba que en interpretación conjunta de ambos hace posibles cesiones entre datos Administraciones Públicas para fines distintos a los que motivaron su recogida y que el titular no sea informado al recabarlos de esa posibilidad, así como que la cesión se efectúa sin consentimiento del afectado y que la autorización para efectuar esas cesiones puede contenerse en una norma de rango inferior a la ley.

[163] Pérez Luño define la libertad informática como el derecho fundamental a la información, control sobre los datos y el establecimiento de los recursos necesarios para garantizar la protección de los individuos; en Colmenero Guerra, "el derecho a la autodeterminación informativa" II Jornadas de estudio sobre" protección de datos y derechos fundamentales", Instituto Vasco de Administración Pública (IVAP),1991, págs. 304 y ss.

En este mismo sentido, expresa nuestro TC español que ambos "comparten el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar" (STC nº 292/2000, de 30 de noviembre, Fundamento Jurídico 5 *in fine*). Sin embargo, en su Fundamento Jurídico 6 de la citada Sentencia expresaba que difieren en su función, su objeto y su contenido[164], tal y como se expone a continuación:

1º Primero, tendrían una distinta función, mientras el derecho a la protección de datos personales garantiza "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 protege "frente a cualquier invasión que pueda realizarse en el 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 (por todas, se cita la STC nº 155/99, de 22 de julio, Fundamento Jurídico 8)".

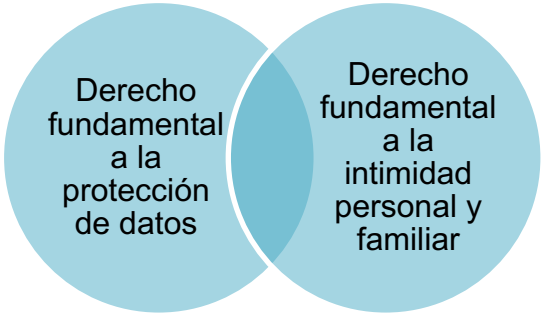
2º Segundo, tendrían un distinto objeto, toda vez que el derecho a la protección de datos tiene un objeto más amplio que el del derecho de intimidad pues extiende su garantía, no sólo a la intimidad en su dimensión protegida por el art. 18.1 CE, sino a lo que en ocasiones el TC ha definido en términos más amplios como "la esfera de los bienes de la personalidad que pertenecen al ámbito la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC nº 170/1987, de 30 de octubre, Fundamento Jurídico 4), como el derecho al honor (…), e igualmente, en expresión bien amplia del propio artículo 18.4 CE, al pleno ejercicio de los derechos de la persona (…)". De ahí que, la protección de datos personales ampararía todos los datos personales, sean o no íntimos, cuyo conocimiento o empleo ajeno pueda afectar a sus derechos; así como también, a los datos públicos sobre los que el titular sigue teniendo poder de disposición.

3º Tercero, respecto a su diferente contenido, mientras el derecho a la intimidad otorga a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de los

[164] Megías Quirós, J.J, insiste en que hay diferenciar entre la facultad de excluir del conocimiento de los datos personales (derecho a la intimidad) y la facultad de controlarlos (derecho a la protección de datos personales, privacidad en Internet: intimidad comunicaciones y datos personales". Recuperado de: http://revistas.ucm.es/index.php/ANDH/article(viewFile/ANDH0202110515A/20978 (fecha de consulta: 2020).

desconocidos; el derecho a la protección de datos personales atribuye al titular un "haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos", como se indicaba anteriormente al respecto de la STC nº 292/2000, de 30 de noviembre.

A mayor abundamiento, el derecho a la intimidad sería una facultad introspectiva, en cuanto a que se refiere a un ámbito privado personal libre de injerencias externas y al que únicamente pueden acceder las personas autorizadas o consentidas por su titular. Así, de forma ilustrativa, dicho derecho operaría, en términos coloquiales, "de puertas hacia adentro". Mientras que la protección de datos opera "de puertas hacia fuera", respecto a la información de personas identificadas o identificables[165].



Por tanto, se ha evidenciado que ambos derechos fueron positivados en el ordenamiento jurídico español en la segunda mitad del siglo XX, pero tras una evolución jurisprudencial se fueron configurando como dos derechos fundamentales independientes y autónomos, así como derechos no absolutos, que comparten su carácter de derecho fundamental y el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar. No obstante, es de reconocer que están estrechamente interrelacionados, por lo que en determinados supuestos pueden generarse dificultades o convergencias sobre si el derecho en cuestión es uno u otro[166].

[165] Fernández Acevedo, J. Conferencia Centro de Empresarios de Jaén, 2018.
[166] Igual ocurre con los términos protección de datos y privacidad, pues a veces se habla de privacidad de forma más genérica, pero a nivel jurídico esta se podría situar entre la intimidad y la protección de datos que, insistimos no es lo mismo. La privacidad es subjetiva, para una persona puede ser dato íntimo como su fe, su número de cuenta bancaria o su correo electrónico; pero para otras no y lo exponen públicamente.

C) Nociones básicas sobre el método y ponderación de derechos

Tal y como se ha expuesto anteriormente, es frecuente que en la práctica se produzcan convergencias de más de un derecho fundamental, como puede ser protección de datos y libertad de información veraz. En este punto, interesa evidenciar que el Tribunal Supremo español (TS, en adelante) se ha pronunciado sobre el método y ponderación en los supuestos de colisión o covergencia de derechos; destacando, por todas, su Sentencia nº 593/2022, de 28 de julio, dictada a propósito del caso enjuiciado en el que se producía una convergencia entre el derecho a la libertad de información[167] y el derecho a la propia imagen (artículo 18.1 CE)[168].

En el supuesto de hecho, se solicitaba la declaración de la existencia de una intromisión ilegítima en el derecho a la propia imagen y, por ende, la condena a la mercantil demandada al pago de una indemnización de 220.000 euros, a la retirada de todas las imágenes relativas a su persona en los reportajes emitidos, así como de todas las plataformas (YouTube, en concreto) en las que podían encontrarse[169].

[167] La libertad de información contiene una dimensión activa, constituida por el derecho a informar libremente, y una dimensión pasiva o derecho a ser informado. Recae sobre la comunicación de hechos susceptibles de contraste con datos objetivos, tiene como titulares a los miembros de la colectividad y a los profesionales del periodismo, y consiste en comunicar o recibir información veraz por cualquier medio de difusión (sentencias del Tribunal Constitucional 104/1986, de 17 de julio; 139/2007, de 4 de junio; 29/2009, de 26 de enero y sentencias de esta Sala 370/2019, de 27 de junio; 491/2019, de 24 de septiembre; 172/2020, de 19 de noviembre; 26/2021, de 25 de enero; 852/2021, de 9 de diciembre y 48/2022, de 31 de enero, entre otras muchas). La importancia que ostenta la libertad de información requiere que goce de un espacio blindado para que pueda cumplir su fundamental función de transmitir e investigar hechos de interés general, que son fundamentales en un Estado de Derecho para formar una opinión pública plural, para la consecución de la transparencia en la actuación de los poderes públicos, y posibilitar, de esta forma, el ejercicio de los derechos políticos por parte de los ciudadanos con conocimiento de causa, los cuales gozan, a su vez, del derecho, también constitucional, de recibir una información veraz (SSTS 852/2021, de 9 de diciembre; 887/2021, de 21 de diciembre).
Esta función fundamental que desempeña la libertad de información comprende también la información gráfica relacionada con los hechos sobre los que versa (STS 697/2019, de 19 de diciembre, entre otras muchas).

[168] Sentencia nº 593/2022, Tribunal Supremo, Sala de lo Civil, Recurso 67/2021 de 28 de Julio de 2022. Recuperado de: https://vlex.es/vid/908473403 (fecha de consulta: 2023).

[169] Al respecto, expresa la citada STS que "Las imágenes del actor, objeto de este proceso, figuran en YouTube, en donde fueron anexadas por el hijo del demandante, sin cuestionar el actor, en momento alguno, tal circunstancia, lo que implica un consentimiento a la incorporación de su imagen a dicha plataforma de acceso general. YouTube es un sitio web, que permite a sus usuarios subir vídeos para que otros puedan visionarlos en cualquier momento y de manera online. No obstante, permite configurar la privacidad de los vídeos incorporados para controlar quién puede acceder a su contenido y dónde aparecerá, bajo tres niveles u opciones: público, oculto o privado. En la primera de ellas, cualquier usuario de YouTube puede ver los vídeos de tal forma anexados. Además, se pueden compartir con cualquier persona que use la plataforma.

En lo que concierne al juicio de ponderación en estos casos de colisión de derechos fundamentales, destaca lo expresado en el Fundamento Jurídico 3 de la citada STS nº 593/2022:

> "*3.1* (…) *Como hemos señalado, reiteradamente, la decisión del recurso de casación exige, en casos como el presente, determinar el acierto del juicio de ponderación entre los derechos fundamentales en conflicto, llevado a efecto por la audiencia provincial, que consideró, en atención a las particularidades concurrentes, prevalente el derecho a la propia imagen del actor* [170] *sobre el también derecho de rango constitucional de la demandada a transmitir información veraz.*

Ahora bien, la circunstancia de que los vídeos se hubieran subido a la plataforma You tube, no permite deducir que quepa hacer un uso indiscriminado de los mismos, de manera que la imagen del actor quede a disposición de cualquier sujeto de derecho para utilizarla sin su consentimiento, en el ámbito y de las formas que considere oportunas, como si el titular del derecho a la propia imagen se hubiera desprendido libremente del mismo y quedara a la indiscriminada disposición de cualquier miembro de la comunidad de usuarios, máxime cuando los derechos fundamentales, por ministerio de la ley y su propia esencia, son irrenunciables, inalienables e imprescriptibles, como señala el art. 1.3 de la LO 1/1982, que añade que la renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de dicha ley.
En definitiva, no se pierde el control sobre el vídeo incorporado, con base en una supuesta presunción de autorización de uso indiscriminado, que derivase del simple y único dato de la incorporación del vídeo a esta plataforma. No obstante, ello no significa que tal circunstancia no deba ser valorada desde la perspectiva de los usos sociales y en el contexto que supone el acceso público a los contenidos voluntariamente incorporados a You tube. Esta Sala ha proclamado en sentencias 1.225/2003, de 24 de diciembre; 1.024/2004, de 18 de octubre; 1.184/2008, de 3 de diciembre; 311/2010, de 2 de junio, y posteriormente en sentencias de pleno 91/2017, de 15 de febrero y 220/2021, de 21 de abril, que el consentimiento dado para publicar una imagen con una finalidad determinada no legitima su publicación con otra finalidad distinta".

[170] Al respecto de la propia imagen, aclara que, refiriéndose la sentencia a otra de la Sala 887/2021, de 21 de diciembre, en los términos siguientes: "(v) El derecho a la propia imagen consiste en el "(..)derecho a determinar la información gráfica generada por los rasgos físicos personales de su titular que puede tener difusión pública" y, por lo tanto, abarca "(..) la defensa frente a los usos no consentidos de la representación pública de la persona que no encuentren amparo en ningún otro derecho fundamental" (por todas, SSTC 23/2010, de 27 de abril, FJ 4; 12/2012, FJ 5, 19/2014, de 10 de febrero, FFJJ 4 y 5 y 25/2019, de 25 de febrero, FJ 4, así como SSTS 476/2018, de 20 de julio; 491/2019, de 24 de septiembre; 697/2019, de 19 de diciembre y 209/2020, de 29 de mayo).
"Se trata de un derecho autónomo respecto de los otros derechos fundamentales al honor y a la intimidad personal y familiar, lo que constituye una peculiaridad de nuestro ordenamiento jurídico, en comparación con otros de nuestro entorno y con el Convenio de Roma de 4 de noviembre de 1950 para la Protección de los Derechos Humanos y de las Libertades Fundamentales (SSTS de 22 de febrero de 2006, rec. n.º 2926/01, y 9 de junio de 2009, rec. n.º 2292/05). (…)

> *En las sentencias 48/2022, de 31 de enero y 318/2022, de 20 de abril, nos referíamos a este* ***juicio de ponderación*** *como: "[...] la operación racional y motivada de examinar el grado de intensidad y trascendencia con el que cada uno de los derechos fundamentales en colisión resulta afectado, con la finalidad de elaborar una regla resolutiva que permita solventar el conflicto objeto del proceso, y, de esta manera, determinar cuál ha de prevalecer, en tanto en cuanto no existen derechos absolutos, que deban gozar de una incondicionada prioridad en cualquier contexto de enfrentamiento entre sus respectivos núcleos de protección jurídica". En dicho juicio de ponderación, debemos determinar cuál de los derechos en conflicto tiene mayor peso para reputarlo prevalente, en tanto en cuanto no puedan convivir, de forma armónica, en la balanza del derecho. (…)"* (Subrayado añadido).

Aplicando lo anterior al caso en concreto en cuestión, consideró el Alto Tribunal de forma literal que:

> " (…) si bien es cierto, …desde un punto de vista axiológico abstracto, la libertad de información ha de gozar de una protección reforzada, dada la función constitucional que le corresponde para formar opinión pública en un estado democrático, tal circunstancia tampoco implica que nos hallemos ante un derecho absoluto de protección ilimitada, ya que todas las libertades reconocidas en el art. 20 CE tienen sus límites, como señala dicho precepto, "en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia", que cumplen lo que la sentencia del Tribunal Constitucional 23/2010, de 27 de abril, FJ 3, ha denominado "función limitadora" en relación con dichas libertades. En este sentido, las SSTC 12/2012, de 30 de enero, FJ 6; 6/2020, de 27 de febrero, FJ 3; 93/2021, de 10 de mayo, FJ 4; así como las sentencias de esta Sala 139/2021, de 11 de marzo; 852/2021, de 9 de diciembre; 48/2022, de 31 de enero y 318/2022, de 20 de abril, entre las más recientes.

> En definitiva, tal y como destaca la jurisprudencia constitucional, de la que son expresión las SSTC 58/2018, FJ 7 y 25/2019, de 25 de febrero, FJ 7: "[...] la libertad de información puede llegar a ser considerada prevalente sobre los derechos de la personalidad garantizados por el artículo 18.1 CE, no con carácter absoluto sino caso por caso, en tanto la información se estime veraz y relevante para la formación de la opinión pública, sobre asuntos de interés general, y mientras su contenido se desenvuelva en el marco del interés general del asunto al que se refiere" (…).

Pues bien, se evidencia que esto mismo podría predicarse respecto al derecho a la protección de datos, considerando que podría perfectamente prevalecer sobre él otro derecho fundamental, como puede ser el de libertad de información, pero no con carácter absoluto, si no en el análisis de su aplicación al caso en concreto, a las circunstancias particulares del caso en concreto.

En este sentido, continuaba exponiendo el TS en la referida Sentencia, en el apartado 3.6 sobre "Ponderación de las circunstancias concurrentes, prevalencia del derecho fundamental a difundir información veraz, estimación del recurso", de forma literal que:

> "(…) resulta que la libertad de información puede llegar a ser considerada prevalente sobre los derechos de la personalidad garantizados por el artículo 18.1 CE, no con carácter absoluto sino caso por caso, conforme a estas tres pautas valorativas: A) que la información comunicada venga referida a un asunto de interés general o relevancia pública, sea por la materia, por razón de las personas o por las dos cosas; B) proporcionalidad; es decir, que no se usen expresiones inequívocamente injuriosas o vejatorias; y C), por último, aunque no por ello menos importante, el de la veracidad, que es un requisito legitimador de la libertad de información (sentencias 252/2019, de 7 de mayo; 26/2021, de 25 de enero; 852/2021, de 9 de diciembre y 48/2022, de 31 de enero, entre otras).
>
> En este sentido, proclama la STC n.º 27/2020, de 24 de febrero, que: "[...] la protección del derecho a la imagen cede en aquellos casos en los que la publicación de la imagen, por sí misma o en relación con la información escrita a la que acompaña, posea interés público, es decir, contribuya a la

> formación de la opinión pública. El derecho a la imagen deberá sacrificarse en aquellos casos en los que, aun sin su consentimiento, se capta, reproduce o publica un documento gráfico en el que la persona aparezca -de manera no accesoria- en relación con un acontecimiento público que posea el rasgo de noticiable, especialmente si es en el ámbito por el que es conocida la persona (…)".

Por ello, en la citada Sentencia, el TS falló en atención a las concretas circunstancias analizadas en el caso en concreto, en el juicio de ponderación de los derechos fundamentales en conflicto, considerando que ha de "prevalecer el derecho a la información de la entidad demandada sobre el derecho a la propia imagen del actor, lo que conduce a la asunción de la instancia, estimación del recurso de apelación interpuesto por la entidad demandada, y correlativa desestimación de la acción deducida por el demandante, con su repercusión en costas"[171]. Es un proceso similar al juicio de ponderación del interés legítimo del responsable del tratamiento cuando esta es la que se pretende sea la base jurídica del tratamiento[172].

D) Resultados.

En primer lugar, se ha evidenciado que el derecho fundamental a la protección de datos es, en su concepción actual, un derecho limitado y no absoluto, siendo susceptible de ceder ante un interés o derecho constitucional, como puede ocurrir con el derecho a la libertad de expresión o de información veraz (artículo 20 CE). Además, se ha constatado que se encuentra estrechamente relacionado con otros derechos y libertades fundamentales. De hecho, podría prevalecer sobre él otro derecho fundamental, como el de libertad de información, pero no con carácter absoluto, si no en el análisis de su aplicación al caso en concreto.

[171] Respecto al segundo motivo de casación, expresa: "Construido sobre la base de la vulneración del art. 9, apartados 2.º y 3.º, de la LO 1/1982, carece de sentido su examen, pues al declararse inexistente la intromisión ilegítima en el derecho fundamental a la propia imagen del actor, carece de sentido entrar a determinar la proporcionalidad de la indemnización fijada, en tanto en cuanto se encuentra condicionada a la previa declaración de la vulneración del derecho fundamental, que opera como indeclinable presupuesto, el cual, en este caso, no concurre, y, por consiguiente, ninguna indemnización cabe".

[172] Acceso a la Guía sobre interés legítimo del ISMS Forum. Recuperado de: https://www.ismsforum.es/ficheros/descargas/guiaintereslegitimo1637794373.pdf (fecha de consulta: marzo de 2024).

En segundo lugar, se ha reforzado la evidencia de que los derechos a la protección de datos y a la intimidad fueron positivados en el ordenamiento jurídico en la segunda mitad del siglo XX español, pero tras una evolución jurisprudencial se fueron configurando como dos derechos fundamentales independientes y autónomos, así como no absolutos, que comparten su carácter de derecho fundamental y el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar.

No obstante, están estrechamente interrelacionados por lo que en determinados supuestos pueden generarse dificultades o convergencias sobre si el derecho en cuestión es uno u otro[173].

En tercer lugar, se ha constatado que la digitalización genera nuevos escenarios en los que entran en conflicto los derechos fundamentales, y en los que los usuarios, inicialmente simples receptores o consumidores de contenidos, se han convertido en sujetos que incorporan y comparten a las redes sociales y los medios digitales información propia, con mayores o menores limitaciones.

En cuarto lugar, en cuanto a la noción de ponderación de derechos, se ha evidenciado que el derecho a la protección de datos podría prevalecer sobre él otro derecho fundamental, como el de libertad de información, pero no con carácter absoluto, si no en el análisis de su aplicación al caso en concreto. Se ha evidenciado en este sentido que el derecho a la protección de datos converge o confluye en la práctica con otros derechos fundamentales, como el citado de libertad de información veraz, pero la convergencia puede darse respecto a cualquier otro derecho fundamental. En estos casos, se concluye que se debe hacer una ponderación o análisis de prevalencia para ver, atendiendo a las circunstancias particulares del supuesto de hecho, cuál merece una prevalencia.

Para finalizar este Capítulo que cierra este primer Capítulo, se traen a colación las palabras de Mar España (directora de la AEPD desde julio de 2015) que afirmaba que

[173] Igual ocurre con los términos protección de datos y privacidad, pues a veces se habla de privacidad de forma más genérica, pero a nivel jurídico esta se podría situar entre la intimidad y la protección de datos que, insistimos no es lo mismo. La privacidad es subjetiva, para una persona puede ser dato íntimo como su fe, su número de cuenta bancaria o su correo electrónico; pero para otras no y lo exponen públicamente.

"la privacidad es como la salud, que no la valoramos hasta que la perdemos"[174]. Adicionalmente, se ha constatado que protección de datos y ciberseguridad configuran los principales retos a los que se enfrentan las empresas, los profesionales y la sociedad en general.

Ello pone en evidencia que la protección de la privacidad y de la información personal debería ser un asunto primordial y global, toda vez que - debido a la globalización y la digitalización- es un derecho cuya protección ha de ir más allá de las fronteras nacionales, siendo necesario y recomendable lograr un nivel similar de protección de datos personales en todos los países para que el nivel de protección sea completo y adecuado, en pro de la libre circulación de datos y de la economía.

En los siguientes Capítulos, se reflejan los Capítulos II a V, de carácter más innovador, conteniendo las publicaciones que conforman el Compendio del presente trabajo investigador, con el que se opta al Título de Doctorado en Derecho.

[174] Recuperado de: https://www.uimp.es/actualidad-uimp/la-agencia-espanola-de-proteccion-de-datos-cree-que-la-privacidad-es-como-la-salud-no-se-valora-hasta-que-se-pierde.html (fecha de consulta: 2024).

PUBLICACIONES

CAPÍTULO II.- “APROXIMACIÓN A LOS NUEVOS DERECHOS Y GARANTÍAS DIGITALES RECONOCIDOS EN LA LOPDGDD 3/2018”

1. **Referencia (autores, título):** Aproximación a los nuevos derechos y garantías digitales reconocidos en la LOPDGDD 3/2018. *Revista Asuntos Constitucionales,* primer número (0, enero-junio 2021).
2. **Breve resumen:** En esta publicación, de carácter innovador y la primera que conforma el Compendio de la tesis, se reflejó el régimen jurídico en el sistema español en materia de protección de datos en relación con el reconocimiento de un elenco de derechos y garantías digitales consagrados en el Título X de la LOPDGDD 3/18, cuyo reconocimiento explícito supuso un hito jurIdico.
   Los diecisiete derechos y garantías digitales reconocidos fueron agrupados en tres sectores. Primero, los reconocidos en el entorno digital; segundo, los que se refieren a una especial protección al menor de edad, en su consideración de colectivo vulnerable y de mayor riesgo; y tercero, los derechos reconocidos en el ámbito laboral.
   Se ha evidenciado que, aunque es de reconocer la significación jurídica de reconocimiento de estos derechos y garantías digitales, sobre los que se deja vía abierta para la ampliación en el entorno laboral mediante negociación colectica, han constituido un hito jurídico; pero más que un nuevo catálogo de facultades constituiría un elenco de facultades esenciales titularidad de la persona física, ligadas a los derechos fundamentales a la protección de datos y a la intimidad.
   Además, se pone en evidencia que su implementación puede presentar problemas, principalmente, al no gozar de la trayectoria doctrinal y jurisprudencial en comparación con la de otros derechos, requiriendo un grado de determinación y concreción de su contenido por las autoridades competentes; así como que su reconocimiento positivo deviene insuficiente si no se acompaña de medidas de garantía, apoyo y financiación por las autoridades competentes para hacerlos efectivos.
   A mayor abundamiento, al no establecerse medidas y protocolos para hacerlos eficaces, correspondería a cada ente establecer las que considere razonables, pudiendo dar lugar a divergencias interpretativas que supongan distintos niveles de protección de los derechos y garantías digitales. Además, se ha evidenciado la necesidad precisan ser ampliados y actualizados para proteger los derechos fundamentales de los ciudadanos conforme se vayan generando necesidades de tutela antes las innovaciones y la evolución tecnológicas.
3. **Fecha de publicación:** 2021.
4. **Estado:** Publicado.
5. **Tipo de publicación:** Artículo.
6. **Categoría:** Ordinaria.
7. **Ubicación:** Disponible en el siguiente enlace: https://www.asuntosconstitucionales.com/pdf/0-CLopez.pdf.
8. **Otros datos de interés**: N/A.

CAPÍTULO III.- "PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN DE JUSTICIA ESPAÑOLA. PROTOCOLO DE COMUNICACIÓN DE LA JUSTICIA 2018"

1. **Referencia (autores, título):** Protección de datos personales en la Administración de Justicia española. Protocolo de Comunicación de la Justicia 2018, en la *Revista Derecom de la Universidad Complutense de Madrid*, nº 26, pp. 115-130, (2019).
2. **Breve resumen:** En esta publicación, de carácter innovador y la segunda que conforma el Compendio de la tesis, se ha evidenciado que en el ámbito judicial también son objeto de tratamiento datos personales de los intervinientes en los procedimientos judiciales, así como que la protección de datos tiene un régimen jurídico particular.

   Además, se ha puesto en conexión dicho derecho con el derecho a la libertad de información mediante el análisis de las principales medidas y recomendaciones que el Protocolo de Comunicación de la Justicia de 2018, elaborado por la Oficina de Comunicación del CGPJ, que evidencia que la actividad de los órganos judiciales genera información judicial de gran interés social y periodístico, especialmente en el ámbito penal; que los ciudadanos son titulares del derecho a la protección de sus datos pero también del derecho a la libertad de información veraz por cualquier medio de comunicación, en relación con el principio constitucional de publicidad de actuaciones por lo que en el ejercicio de este último cumplen un papel esencial los medios de comunicación. Se han indicado sus principales medidas y recomendaciones para garantizar el derecho a la información derivada de los tribunales de forma eficaz, clara veraz, objetiva y responsable, con respeto a los derechos de los implicados en los procesos judiciales, especialmente en el orden penal, tanto en fase de instrucción como en fase de juicio oral y en la fase de publicación de las resoluciones judiciales.

   Para finalizar, se ha evidenciado que la protección de datos es un objetivo común compartido, siendo conveniente (consecuencia de las reformas legales y de las tendencias europeas) elaborar una regulación sistemática completa, desarrollada de protección de datos en el ámbito jurisdiccional, pues el actual régimen formado por varios artículos con remisión a otras normas deviene insuficiente. Además, lo casos de filtraciones de datos en el ámbito judicial tienen el efecto de incidir directamente en la percepción de la ciudadanía de la justicia como mejorable y cuestionan el tratamiento de los datos en la Administración de Justicia.
3. **Fecha de publicación:** 2019.
4. **Estado:** Publicado.
5. **Tipo de publicación:** Artículo.
6. **Categoría:** Ordinario.
7. **Ubicación:** Disponible en el siguiente enlace: http://www.derecom.com/secciones/articulos-de-fondo/item/374-personal-data-protection-in-the-spanish-judiciary-the-2018-protocol-on-the-judiciary-communications.
8. **Otros datos de interés:** En el apartado sobre Resumen global y discusión de resultados de la tesis se ha incluido una referencia a la actualización de su contenido, puesto que posteriormente a la publicación del artículo, se publicaron la Ley Orgánica 7/2021 (de trasposición de la Directiva 2016/690) y un Protocolo de Comunicación posterior (de 2020), que incorporó un Capítulo dedicado a la publicidad de las actuaciones judiciales en el marco de las medidas de prevención de contagio por la pandemia COVID-19 adoptadas en las sedes judiciales para garantizar que la información siga llegando al ciudadano de

forma eficaz, clara, veraz, objetiva y responsable, con absoluto respeto a los derechos y observancia de los deberes de todos los implicados en procedimientos judiciales.

CAPÍTULO IV.- "EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PENAL"

1. **Referencia (autores, título):** El derecho fundamental a la protección de datos personales en el ámbito penal. RUIZ-RICO RUIZ, G; POMARES CINTAS, E; REVENGA SÁNCHEZ, M; VERGARA GALAZ, D. (Coords.), *Derecho Penal y Garantías Constitucionales. Una perspectiva iberoamericana*. Tirant lo Blanch. Valencia, (2020).
2. **Breve resumen:** En esta publicación, de carácter innovador y la tercera que conforma el Compendio de la tesis, se han reflejado las principales particularidades de protección de datos en el proceso penal, evidenciándose que en estos también existen una gran cantidad de datos relativos a los sujetos intervinientes que han de ser necesariamente objeto de tratamiento por las autoridades competentes.

   Se ha reforzado la evidencia de que el orden penal el de mayor interés social y mediático, evidenciándose que la particularidad del régimen jurídico de protección de datos en el proceso penal consiste en que no se aplica directamente el marco normativo general sino que se aplica de forma supletoria. Respecto al tratamiento de datos de condenas e infracciones penales o medidas de seguridad por Administración de Justicia, abogados o procuradores, se evidencia que solo puede llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la UE o de los Estados miembros que establezca las garantías adecuadas para los derechos y libertades de los interesados. También, que, de conformidad con el CP, el condenado que haya extinguido su responsabilidad penal tiene derecho a obtener del Ministerio de Justicia la cancelación de sus antecedentes penales, que dejen de constar en el Registro Central de Penados y Rebeldes cuando hayan transcurridos los plazos establecidos (art. 136 CP).

   Del análisis de la protección de datos como garantía en el proceso penal y en la actuación investigadora criminal, se evidencia que protección de datos y Derecho penal están sujetos a límites, en su sentido subjetivo al ius puniendi del Estado, estando restringido por las garantías de respeto a los derechos de la dignidad humana, los principios de legalidad, culpabilidad, intervención mínima o el de non bis in ídem. Se ha demostrado que protección de datos opera como una garantía en el proceso penal y de la prueba.

   Del análisis de los delitos de descubrimiento y revelación de secretos y sus tipos agravados, se ha evidenciado que el bien jurídico tutelado es la intimidad en su sentido más amplio como facultad de autodeterminación informativa, lo que puede llevar a confusión con el derecho a la protección de datos, aunque se trata de dos derechos distintos y autónomos.

   Finalmente, se evidencia que es necesario tomar medidas para evitar cometer y ser víctimas de estos delitos, especialmente en el caso de los menores de edad al considerar que tienen un mayor riesgo, tal y como especificaba la Guía de la AEPD sobre protección de datos y prevención de delitos de la que se han traslado las medidas principales, como apostar por la educación digital y frente a ciberdelitos o no hacer una sobreexposición de la información como medida de tutela.
3. **Fecha de publicación:** 2020.
4. **Estado:** Publicado.
5. **Tipo de publicación**: Capítulo de libro de reconocido prestigio en el ámbito jurídico.
6. **Categoría:** Ordinario.
7. Ubicación: Derecho Penal y Garantías Constitucionales. Una perspectiva iberoamericana. Tirant lo Blanch. Valencia, (2020).

8. **Otros datos de interés:** N/A.

CAPÍTULO V. - “PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR SANITARIO, EN EL CONTEXTO DEL DERECHO A LA SALUD Y DE LA DIGITALIZACIÓN IMPULSADA POR LA PANDEMIA COVID-19”

1. **Referencia (autores, título):** Protección de datos personales en el sector sanitario, en el contexto del derecho a la salud y de la digitalización impulsada por la pandemia Covid-19. RUIZ-RICO RUIZ, G. *La Protección de los derechos humanos por las defensorías del pueblo en situaciones de emergencia constitucional*. Tirant Lo Blanc, (2024).
2. **Breve resumen:** En esta publicación, de carácter innovador y la última que conforma el Compendio de la tesis, se han comprobado que la protección de datos tiene particularidades también en el ámbito sanitario, en el que los datos de salud se consideran de carácter sensible y, por ende, susceptibles de una tutela adicional.

   Se han diferenciado conceptos esenciales como los de datos genéticos y biométricos y se ha manifestado que en el ámbito de la salud también el uso de medios digitales avanza a un ritmo sin precedentes, digitalización impulsada por la pandemia COVID-19.

   De otro lado, se ha evidenciado que se aplican en este sector los mismos principios en materia de protección de datos, con las particularidades propias (como las relativas al derecho de información, de limitación del plazo de conservación o al de limitación de la finalidad). También, se prohíben con regla general el tratamiento de datos de salud como datos sensibles, salvo cuando concurran las circunstancias previstas, entre la que se citan que sea necesario para proteger intereses vitales del interesado u otra persona física, en el supuesto de que o esté capacitado para consentir o se refiera a datos manifiestamente públicos por el interesado. Igualmente, aplica la excepción del apartado 4 del artículo 9 RGPD de que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, respecto al tratamiento de datos genéticos, biométrico o sobre salud; evidenciándose que no se logra de forma completa el objeto el RGPD de armonización en la materia.

   Así mismo, se ha comprobado que la aplicación de medios digitales a la HC se valora positivamente por los usuarios de sanidad e incluso un arma fundamental para identificar todos los tratamientos y patologías del usuario, para la medicina preventiva, desarrollar líneas epidemológicas o generar estadísticas de riesgos; así como evidenciado la evolución de la telemedicina en los últimos años en los que la digitalización ha transformado el sector de la salud, y a su impulso derivado de la pandemia COVID-19, que generó la publicación de normativa durante la pandemia y la toma de medidas. En definitiva, se evidenciaba que ha generado la revalorización de este derecho a la salud junto a otros derechos a raíz de la pandemia que se ha reflejado en jurisprudencia convencional y constitucional, que contienen pronunciamientos integrándolo en el derecho fundamental a la vida.

   Finalmente, que existen otros temas relevantes con impacto en protección de datos, como el IOT o las implicaciones de la IA y que generan continuos retos, que pueden suponer riesgos para la seguridad de la información y su uso indebido por parte de terceros, así como el riesgo de los datos, muchos sensibles, siendo necesario el establecimiento de un sistema de garantías adicionales.
3. **Fecha de publicación**:
4. **Estado**: Aceptada y pendiente de publicación (2024).
5. **Tipo de publicación:** Capítulo de libro de reconocido prestigio en el ámbito jurídico.
6. **Categoría:** Ordinario.

7. **Ubicación:** La Protección de los derechos humanos por las defensorías del pueblo en situaciones de emergencia constitucional. Tirant Lo Blanc, (2024).
8. **Otros datos de interés:** N/A.

D. Salvador Vives López, con DNI Nº25380614E, en calidad de Director de la Editorial Tirant Lo Blanch,

CERTIFICA

Que CAROLINA LÓPEZ MEDINA con DNI 77366430L, es autora dentro de la obra titulada:

LA PROTECCIÓN DE LOS DERECHOS HUMANOS POR LAS DEFENSORÍAS DEL PUEBLO EN SITUACIONES DE EMERGENCIA CONSTITUCIONAL

Ha participado en el siguiente capítulo titulado "***PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR SANITARIO, EN EL CONTEXTO DEL DERECHO A LA SALUD Y DE LA DIGITALIZACIÓN IMPULSADA POR LA PANDEMIA COVID-19***"

Con ISBN 9788411979122, ha sido aceptada para su publicación

Y para que así conste a los efectos oportunos a petición del interesado, firmo el presente certificado en Valencia, a 31 de octubre de 2023.

Fdo: Salvador Vives López.

EDITORIAL TIRANT LO BLANCH, S.L.
C.I.F. B - 46 091179
Artes Gráficas, 14
46010 VALENCIA

Resumen global y discusión de resultados

Resumen global y discusión de resultados

En esta sección se exponen y discuten de forma ordenada por Capítulos los resultados obtenidos durante la investigación en el periodo investigador (años académicos 2018/2019 a 2023/2024) en torno a la "Protección de datos personales y su proyección en áreas de convergencia con otros derechos fundamentales", en relación con los objetivos principales expuestos al inicio.

Resumen global y discusión del Capítulo I: "Aproximación al derecho de protección de datos de carácter personal: principales hitos jurídicos a nivel internacional, europeo y español. Concepto y delimitación del derecho a la intimidad; y nociones sobre ponderación de derechos".

I.- En los cinco apartados que constituyen este primer Capítulo se han reflejado, en un primer bloque (Apartados 2, 3 y 4), las principales **particularidades del derecho a la protección de datos que lo configuran un derecho único y los principales hitos jurídicos en esta materia en el marco normativo internacional, europeo y del ordenamiento jurídico español.**

- En resumen, mediante la referencia (en el Apartado 2) a los principales hitos jurídicos sobre protección de datos a nivel internacional en el marco de la OCDE y del Consejo de Europa (entre los que se han resaltado las Directrices de la OCDE sobre Privacidad y Protección de datos publicadas en 1980, el Convenio Europeo de los Derechos Humanos de 1950, el Convenio 108/81), se ha evidenciado que **en plano internacional ya se reconocía, a finales del siglo XX, el derecho a la protección de datos; así como similares principios y definiciones básicas** en la materia, tal y como se entienden en la actualidad en la normativa europea de protección de datos, como en concepto de protección de datos o de flujo transfronterizo de datos.

  También, se ha constatado la existencia de una **preocupación a nivel internacional, no solo por la protección de la privacidad y de la información personal de los ciudadanos, sino también por la importancia**

de no limitar los flujos transfronterizos de datos, la cooperación internacional, la colaboración en la protección de la privacidad y en la elaboración de principios comunes. Esta preocupación se ha mantenido y sigue existiendo en la actualidad, tal y como se ha reflejado a nivel normativo y en las tendencias de la sociedad actual expuestas en la presente tesis.

- Con la referencia (en el Apartado 3) a los principales hitos jurídicos sobre protección de datos a nivel europeo (como la Carta de Derechos Fundamentales de la UE de 2007, el TFUE, la Directiva 95/46/CE y el Reglamento nº 45/2001) **se ha reforzado la evidencia de que ha sido en las últimas décadas, y especialmente a partir de la entrada en vigor y aplicación del citado RGPD, cuando se ha producido la evolución exponencial de este derecho**. Así mismo, se ha evidenciado la previsión de continuará siendo desarrollado en los próximos años, en los que los incesantes avances de la digitalización y de la globalización seguirán generando retos y desafíos para la privacidad, la protección de datos y la seguridad de la información.

  Adicionalmente, se ha reforzado la evidencia de que **el RGPD supuso un hito jurídico en materia de protección de datos, introduciendo grandes novedades** respecto a la normativa anterior que derogó; otorgando una protección tecnológicamente neutra y siendo aplicable al tratamiento de datos personales de personas físicas en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no.

  Entre las grandes novedades que introdujo se han destacado su aplicabilidad directa, el establecimiento de principios de tratamiento de datos personales básicos en materia (licitud, lealtad, transparencia, necesidad, limitación del plazo de conservación, limitación de la finalidad, responsabilidad proactiva y privacidad desde el diseño y por defecto), de un régimen de protección adicional para las categorías especiales de datos y para la protección de las personas físicas en lo que respecta al tratamiento de datos por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Igualmente, se ha destacado como cuestión relevante las transferencias internacionales de datos y los mecanismos de garantía previstos para regularizarlas entre un país externo el Espacio Económico Europeo y otro que forma parte del mismo; junto al reconocimiento de derechos de los interesados, algunos de los cuales ya se habían recogido en otros textos anteriores a nivel internacional y europeo (acceso, rectificación, limitación, supresión, oposición), aunque otros sí fueron de carácter novedoso, como el derecho a la portabilidad de los datos.

A mayor abundamiento, entre otros puntos destacables del RGPD se han reseñado la delimitación de los roles en el tratamiento de datos, estableciendo la obligación de establecer medidas técnicas y organizativas apropiadas de cumplimiento (como a de llevanza y actualización de un RAT o la realización de análisis de riesgos y otras medidas de seguridad). Así mismo, la regulación de la gestión y notificación de las brechas de seguridad, estableciendo el plazo de 72 horas para la primera comunicación de la misma a la AEPD, aunque se permite hacer una segunda comunicación más completa más adelante; y la figura del DPO como el supervisor y responsable de velar por el cumplimiento del RGPD, entre otras relevantes funciones como la de informar sobre las obligaciones de la empresa y hacer de persona de contacto ante las autoridades nacionales de protección de datos, ente otras funciones esenciales.

De otro lado, se ha resaltado el cambio de su régimen sancionador a uno más gravoso, estableciendo que las autoridades de control garantizarán que la imposición de las multas administrativas según el RGPD en cada caso sean efectivas, proporcionadas y disuasorias, según las circunstancias del caso individual, pudiendo llegar a 10.000 euros como máximo o tratándose de una empresa, de cuantía equivalente al 2 % como máximo del volumen de negocio total anual del ejercicio financiero anterior; o de 20.000 euros como máximo o el 4 % como máximo de volumen de negocio total anual del ejercicio financiero anterior, optándose en ambos casos por la de mayor cuantía.

Así mismo, se ha evidenciado que **el RGPD logró en parte con su objetivo de homogeneización al dejar un cierto margen en algunos puntos a la**

legislación nacional (como la determinación de la edad del menor para prestar su consentimiento al tratamiento de datos). En conexión con ello, se ha constatado la necesidad de una especial protección homogénea de los menores de edad en todos los ámbitos, junto a una mayor atención y tutela por ser considerados menos conscientes de los riesgos, las consecuencias, y las garantías y derechos en materia de protección de datos, especialmente cuando vayan a ser tratados sus datos con finalidades relacionadas con la mercadotecnia.

- Por otro lado, se ha reforzado la evidencia de la **influencia del RGPD en otros continentes y países, destacando haber sido y ser referente en el marco de protección de datos en América Latina**, donde la protección de datos personales es tan diversa como los países que la forman, con realidades sociales, económicas, políticas y culturales muy diferentes.

  Al respecto de la protección de datos en América Latina, a modo de discusión, aunque no existe una regulación común sobre similar a la europea, la mayoría de los países coinciden en considerarlo un derecho fundamental, existiendo similitudes de la legislación latinoamericana sobre protección de datos y privacidad, en término general, con la europea[175], al ser considerada la más

[175] A ello, se añade lo reconocido y estipulado por los Países Latinoamericanos en los Encuentros anuales sobre protección de datos, entre los que destaca el I Encuentro Iberoamericano sobre Protección de Datos, que se celebró en San Lorenzo del Escorial (Madrid) en el año 2002 en el que se reconoció que el respeto a la intimidad y a la privacidad, y en particular, a la libre disposición de sus datos personales, es un derecho fundamental y la confianza ciudadana en un tratamiento leal y respetuoso de sus datos es un factor clave para la expansión del comercio electrónico entre otros recursos proporcionados por las tecnologías digitales. https://www.redipd.org/es/actividades/encuentro/i-encuentro-iberoamericano-el-escorial-2002. Además, expresaron su intención de promover un intercambio continuo y fluido de información respecto de la evolución de la situación en materia de protección de datos en sus países; informar a las autoridades públicas competentes y al sector privado de sus países de las conclusiones alcanzadas en el Encuentro; Promover la adopción de medidas que pudieran favorecer un nivel adecuado de protección de datos personales; establecer un Foro permanente que coordine estas actuaciones en http://www.redipd.es/actividades/encuentros/I/index-ides-idphp.php. Al año siguiente, del II Encuentro Iberoamericano sobre Protección de Datos Personales de 2003 derivó la Declaración de La Antigua (Guatemala) de 2003 de los países participantes y convocados reconocieron la protección de datos como derecho fundamental, sobre el que es creciente su "interés, preocupación y compromiso. Si bien, reconocieron que, en Iberoamérica, continúan produciéndose situaciones que impiden o dificultan el ejercicio efectivo de tal derecho", constatando la necesidad de impulsar medidas para garanticen un elevado nivel de protección de datos y de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes, en el respeto a los derechos fundamentales de los intereses de sus respectivos países, garanticen una protección adecuada en todos los Países Iberoamericanos. Tales

restructura y al producirse transferencias internacionales de datos a países de la UE. De hecho, para reforzar la mutua y continua colaboración entre los Países Iberoamericanos, se constituyeron en la *Red Iberoamericana de Protección de Datos* y declararon que "en el marco legal e institucional de sus respectivos países, realizarán, dentro de sus respectivas competencias, los esfuerzos necesarios para que la protección de datos personales sea impulsada en el seno de la Conferencia Iberoamericana, en la certeza de que así se promoverá la difusión y concienciación de tan importante derecho fundamental". Es en la citada Red Iberoamericana de Protección de Datos donde se intercambian buenas prácticas entre los principales actores del sector privado y público, con las principales agencias de protección de datos de los países iberoamericanos[176], con el objetivo de avanzar en la creación del régimen normativo en protección de datos[177].

- Otra evidencia que se ha reforzado es la relativa a que, **más de cinco años después de la entrada en vigor y aplicación del RGPD, siguen existiendo empresas que no se han adaptado a la normativa, otras que se han adaptado al cumplimiento de la normativa de protección de datos sin profundizar o en un plano meramente "formal"** (probablemente para

marcos normativos deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los instrumentos internacionales. Recuperado de: http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf (fecha de consulta: 2023). En ese mismo año, la XIII Cumbre Iberoamericana de jefes de Estado y de gobierno, en Santa Cruz de la Sierra (Bolivia), en noviembre 2003, derivó en la Declaración de Santa Cruz de la Sierra de 2003, que vuelve a reconocer la protección de datos como un derecho fundamental. Asimismo, son conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidos en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos.

[176] María H. Santos en Latinoamérica sigue los pasos de España en protección de datos, legal, cinco días. Recuperado de: https://cincodias.elpais.com/cincodias/2017/07/25/legal/1500978248_131866.html, (fecha de consulta: 2023).

[177] Igualmente, destaca el XV *Encuentro Iberoamericano de Protección de Datos en Santiago de Chile* organizado por la Red Iberoamericana de Protección de Datos del Consejo para Transparencia Chilena en junio de 2017, en él se aprobaron y presentaron los "*Estándares de Protección de Datos para los Estados Iberoamericanos*". En este encuentro se debatieron temas relacionados con el ejercicio efectivo de la privacidad, como el derecho a la desindexación o el uso de tecnologías de vigilancia. Se celebran a tal fin "Encuentros", periódicos, aunque lo relevante respecto a protección de datos es que año tras año se ha ido reforzando el reconocimiento del carácter fundamental del derecho a la protección de datos personales y que, han ido reconociendo que la falta de normativa sobre protección de datos de algunos países supone un riesgo o peligro para usuario.

exonerarse de posibles sanciones o cumplir de cara a la cara visible y a favor de su reputación), lo que no es conforme el espíritu del RGPD y de la cultura de cumplimiento en privacidad de protección de datos y la responsabilidad proactiva. Así, se ha evidenciado la existencia de otras empresas que se adaptaron en su día, pero las novedades y nuevas orientaciones de las autoridades de control o del EDPB precisan la actualización de la adecuación, o de los procedimientos a los que afecte (por ejemplo, en materia de cookies[178]). Casi seis años después de la entrada en vigor y aplicación del RGPD siguen incrementando los tratamientos ilícitos, así como que los casos y las modalidades de tratamientos ilícitos de datos se siguen repitiendo.

En conexión con lo anterior, se ha evidenciado que **se sigue sancionando a las empresas por las mismas causas de incumplimiento en la materia y en aspectos esenciales de cumplimiento de la normativa**, tal y como ponen de manifiesto las sanciones de Autoridades de Control de protección de datos impuestas desde el año 2018 (en que entró en vigor y aplicación el RGPD y se inició la presente investigación) a la actualidad, de las que se han trasladado por orden cronológico las más relevantes en las Tablas incluidas con sanciones relevantes ordenadas por orden cronológico.

- A modo de ejemplos de **instrumentos para cumplir y demostrar cumplimiento con la normativa de protección de datos** se ha evidenciado que pueden ser los siguientes: la llevanza como responsable y como encargados del tratamiento de un RAT con el contenido mínimo previsto en el artículo 30 del RGPD (nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del DPO; fines del tratamiento, categorías de interesados y de datos personales; categorías de destinatarios, los plazos de conservación; en su caso las transferencias internaciones y las medidas técnicas y organizativas de seguridad del artículo 32 RGPD) o de una forma más completa. Dicho RAT tiene que estar actualizado, siendo lo recomendable con carácter anual y cada vez que sea necesario; de tal forma que en caso de que se proceda a la modificación,

[178] Recuperado de: https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-right-access-and-letter-cookie-consent_en; https://www.aepd.es/documento/guia-cookies.pdf (fecha de consulta: 2023).

eliminación o adición de los datos que sean necesarios. Por ejemplo, si termina la relación con un encargado de tratamiento o se deja de realizar cesiones de datos, debe reflejarse en el RAT.

También, se ha demostrado que son esenciales la concienciación y formación periódica, así como disponer e implantar textos legales adaptados a la empresa u organización que se trate, como Políticas de protección de datos y de Cookies, Guías o Manuales de protección de datos, procedimientos (como de gestión y notificación de brechas de seguridad, videovigilancia, de gestión del ejercicio de derechos), así como Códigos de buenas prácticas en protección de datos. Otros mecanismos destacados son los procedimientos de gestión del riesgo y de evaluación de impacto en tratamientos de datos personales y del nivel de riesgo de vulneración a la protección de datos[179].

- En cuanto al **ordenamiento jurídico español**, se ha evidenciado (en el Apartado 4) que la **protección de datos configura un derecho fundamental, autónomo e independiente** consagrado en el texto constitucional; que tal y como ha reiterado el TC, se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero.

  Así mismo, se ha constatado que **el derecho a la protección de datos configura un derecho no absoluto, por lo que se generan convergencias con otros derechos fundamentales** (como con el derecho a la libertad de información), por lo que han reflejado las principales consideraciones sobre el juicio de ponderación de derechos cuando convergen varios derechos fundamentales. **En estos supuestos de conflicto se viene manteniendo la pertinencia de realizar un juicio de ponderación de derechos**, correspondiendo realizar una ponderación de los derechos en conflictos en el caso en concreto.

  De otro lado, se ha constatado que **la LOPDGDD 3/18 constituyó un hito jurídico** que vino a "adaptar" la normativa europea partiendo, además, del

[179] Recuperado de: https://www.aepd.es/es/guias-y-herramientas/guias (fecha de consulta: 2024).

principio de plena aplicabilidad de internet a los derechos y libertades reconocidos, como a la vida, la seguridad o a la libertad religiosa y los prestadores de servicios contribuirán a garantizar su aplicación **reconociendo un elenco de nuevos derechos y garantías digitales** (facultades de acceso universal, asequible y de calidad a internet, del testamento digital, de desconexión digital del trabajador y de la educación digital, analizadas en profundidad en la publicación que constituye el Capítulo II).

De la citada Ley **se ha destacado su regulación de los principios de protección de datos y derechos en materia de protección de datos en línea y de forma similar a los previstos en la normativa europea** (licitud, exactitud, transparencia e información, además de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición). Por otro lado, que **regulaba una serie de disposiciones aplicables a tratamientos concretos, como los sistemas de información crediticia, tratamientos con fines de videovigilancia, los sistemas de exclusión publicitaria o los sistemas de información de denuncias internas** regulados de forma específica por la citada *Ley de Canal de Denuncias o Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.*

Además, se ha evidenciado que dicha normativa nacional dedica un apartado a regular la AEPD, el **procedimiento en caso de posible vulneración de la normativa de protección de datos y el régimen sancionador**, distinguiendo entre infracciones consideradas "muy graves" (como el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 RGPD), "graves" (como no disponer del registro de actividades de tratamiento establecido en el artículo 30 RGPD). Como infracciones "leves", se prevén el incumplimiento de la obligación de documentar cualquier violación de seguridad.

- Respecto al **elenco de los citados nuevos derechos y garantías digitales que reconoce la LOPDGDD 3/18 en su Título X, se ha evidenciado que más que una nueva generación de derechos, configuraron facultades ligadas a los derechos fundamentales a la protección de datos y a la intimidad**

personal y familiar; así como que **su efectividad puede presentar limitaciones** en la práctica, porque su reconocimiento ha de completarse con medidas de apoyo y financieras efectivas, así como con garantías de control por parte de las autoridades competentes. También, por la falta de trayectoria doctrinal y jurisprudencial consolidada, precisando ser interpretados y concretado su contenido por parte de los órganos judiciales y autoridades competentes; y trasladados a medidas y protocolos de cumplimiento concretos a concretar por parte de las empresas e instituciones.

- Al margen de lo anterior, se ha constatado una **especial tutela de los menores de edad en el entorno digital**, trayéndose a colación de manera ilustrativa la Resolución de la AEPD de agosto de 2023[180], en la que sancionó a una inmobiliaria con 6.000 euros por publicar fotos de un inmueble con imágenes de menores. Dos fotografías de la cocina del inmueble permitían ver cuatro fotos de menores; otra, de un dormitorio, retratos de estas.

- Adicionalmente, se ha constatado que **en el año 2023 se publicó la Ley 11/2023, en transposición de varias Directivas de la UE, el 8 de mayo de 2023, que introdujo varias modificaciones en la LOPDGDD 3/18**, como la ampliación de la duración máxima de las actuaciones previas de investigación de 12 a 18 meses y del procedimiento sancionador de 9 a 12 meses y se añade un nuevo apartado que prevé la posibilidad de que, a condición de que se demuestre haber adoptado medidas para cumplir con la norma aplicable, la AEPD archive la reclamación y adopte soluciones correctivas, alternativas o más moderadas, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos previstos.

- Para finalizar, se ha reforzado la evidencia de que **los incumplimientos de la normativa sobre protección de datos se producen en todos los sectores y por diversos motivos. El riesgo de sanción de las empresas de todos los ámbitos y tamaños podría ser el mismo que antes de la regulación del RGPD, la diferencia es que ahora las sanciones son más en número, siendo esta tendencia al alza**, como se refleja, por ejemplo, en las Memorias

[180] Recuperado de: https://www.aepd.es/es/documento/ps-00526-2022.pdf (fecha de consulta: 2023)

que con carácter anual publica la AEPD. Así la tendencia es que **la cuantía de las sanciones en materia de protección de datos sea mayor, recayendo la carga de la prueba de demostrar el cumplimiento en el responsable del tratamiento, de ahí, la importancia de no solo cumplir sino guardar una trazabilidad y documentarlo**, generando las oportunas evidencias del cumplimiento.

- En línea con lo anterior, se ha evidenciado el **incremento de sanciones por vulneración de la normativa de protección de datos a nivel internacional, europeo y español, siendo además la tendencia al alza** como se ha indicado y como se refleja en las Memorias que con carácter anual publica la AEPD, respecto a las que se ha llevado a cabo el análisis de las dos últimas Memorias anuales de la AEPD de 2021 y 2022, y de las que se ha extraído las siguientes consideraciones:

  - En el año 2022 se gestionaron un mayor número de notificaciones de brechas de seguridad respecto al año anterior, un total de 1751 notificaciones y, se generaron 31 requerimientos a los responsables; lo que se prevé ha seguido al alza y así se considera quedará reflejado en la Memoria anual de 2023 que se publicará próximamente.

  - Una de las principales preocupaciones del entorno digital es la relacionada con el acceso por menores a dispositivos móviles, al periodo que los utilizan y los servicios de internet que acceden[181].

  - Los principales desafíos para la privacidad son el uso de la IA por los poderes públicos y empresas privadas, el tratamiento de datos a una escala desconocida hasta ahora, planteando el uso de "espacios de datos" como un modelo de tratamiento de gran complejidad organizativa y tecnológica, así como el escalado en la diversidad de categorías de datos procesadas, número de sujetos afectados, ámbitos involucrados, intervinientes y otros.

[181] En esta línea se ha publicado el 14 de diciembre de 2023 un Decálogo de Principios. Verificación de edad y sistemas de protección de personas menores de edad ante contenidos inadecuados. Recuperado de: https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf (fecha de consulta: 2023).

- Han incrementado el número de reclamaciones en el ámbito *online*, más de un 40% con respecto a 2020, hasta situarse en casi un 20% del total de reclamaciones registradas[182]. Si en la Memoria de 2021 las reclamaciones recibidas en la AEPD alcanzaron una cifra sin precedentes, con un total de 13.324, superando las 10.324 reclamaciones presentadas en el año 2020. El número de reclamaciones resueltas ha sido también extraordinario, y un 35% superior al año anterior; en la Memoria de 2022 se informa que la tasa de reclamaciones resueltas frente a reclamaciones recibidas se ha mantenido en el entorno del 100 %. Se especifica un total de 14.3937 reclamaciones resueltas.

- Se observa un aumento del número de multas impuestas por la AEPD, si bien el importe total se reduce debido a una disminución en el número de grandes procedimientos resueltos durante este último año frente a lo sucedido el año pasado.

- Las top áreas de actividad con mayor número de reclamaciones recibidas serían: Servicios de internet, video vigilancia, publicidad (excepto o correo no deseado), ficheros de morosidad, reclamación de deudas, Comercios, transporte y hostelería, Administración Pública, Sanidad, Entidades financieras/acreedoras y publicidad a través de email o móvil, junto a la contratación fraudulenta y sanidad.

- Los seis temas con mayor importe total en 2022 de multas son servicios de internet, publicidad (excepto *spam*), asuntos laborales, brechas de datos, contratación fraudulenta y telecomunicaciones. Se ha evidenciado cómo las empresas de telecomunicaciones siguen siendo sancionadas por mala praxis al realizar duplicados de tarjeta SIM o eSIM o tarjeta virtual, a través de suplantación de identidad o casos de *sim swapping*; por la realización de llamadas comerciales a individuos que se ha opuesto a las mismas y/o están registrados en la lista de exclusión publicitaria; por no contar con medidas suficientes de seguridad para evitar una suplantación de identidad

[182] En particular, los hechos se refieren, en una proporción importante, a la difusión no consentida de datos personales en sitios web, particularmente en redes sociales y servicios equivalentes de la sociedad de la información, y a la desatención de las solicitudes de supresión dirigidas a los prestadores de servicios, que en no pocas ocasiones presentan deficiencias informativas en sus políticas de privacidad.

y realizar portabilidad sin verificar el consentimiento; o por el tratamiento ilícito de datos al renovar una promoción sin el consentimiento del cliente y contra su decisión.

La misma tendencia se ha observado en el sector financiero, las entidades financieras siguen siendo sancionadas por reclamar mediante entidades de recobro, deudas a entidades bancarias que quedaron anuladas por sentencia judicial o por utilizar datos de terceras personas sin permiso para crear cuentas bancarias a menores e ingresar el dinero de una herencia.

- De forma paralela, se ha evidenciado que **el aumento de las cifras de cibercriminalidad,** habiéndose sofisticado tanto las amenazas como los ciberataques y variado sus agentes, configurando factores esenciales de negocio a la vez que unas de las principales preocupaciones de la sociedad actual, especialmente en países desarrollados y en desarrollo; **y el uso generalizado de las TIC, las redes sociales, la red de internet, la IA y el resto de las herramientas digitales, generan nuevos escenarios en los que se generan nuevos retos y desafíos** para la protección de datos, a la vez que aumenta la preocupación social por la importancia de respetar y hacer respetar este derecho fundamental y cumplir la normativa reguladora. se ha puesto de manifiesto la tendencia de aumento de las vulneraciones en materia de protección de datos, sino también de las cifras de cibercriminalidad.

- Derivado de lo anterior, se ha constatado la **necesidad de seguir trabajando en una cultura global de cumplimiento de la normativa protección de datos y de tutela y garantía de este derecho, armonizada y con homogeneidad regulatoria**. La importancia del cumplimiento de las exigencias y principios de protección de datos se debe producir en todos los ámbitos y niveles, así como la necesidad de establecer medidas de seguridad y salvaguarda, sin olvidar las medidas de control periódicos y auditorías[183].

  De forma paralela, se ha reforzado la evidencia de que **la tutela de los datos personales y de los derechos digitales sigue configurando uno de los**

[183] Consisten en realizar pruebas para detectar posibles vulnerabilidades que pudieran poner en riesgo la seguridad, disponibilidad, integridad y confidencialidad de los sistemas informáticos y de los datos almacenados en ellos, o la capacidad de detección y respuesta ante incidentes de seguridad.

retos actuales en todos los ámbitos y en particular, del Derecho Constitucional, debiendo ser el objetivo común compartido seguir promocionando la cultura de la protección de datos, la responsabilidad proactiva de cumplimiento y la concienciación en el respeto de los derechos digitales con la finalidad de que sean respetados y percibidos por la sociedad como una necesidad inherente a la dignidad humana.

En este punto, se hace una doble referencia, por un lado, al término *compliance* o cumplimiento normativo[184], que en el sector de protección de datos se refiere a los procedimientos, medidas, buenas prácticas adoptadas por las compañías y organizaciones en general, para identificar y clasificar los riesgos operativos y legales a los que están expuestos en este sector específico de protección de datos. Ello con el objeto de establecer el conjunto de mecanismos para prevenir, mitigar y reaccionar frente a estos riesgos, como puede ser un incidente de seguridad o filtración de datos; o el incumplimiento de nombrar DPO en aquellos casos que según la norma es obligatoria.

Los pasos serían primero, identificar riesgos concretos, segundo, monitorizar y detección de los riesgos para prevenir, tercero, resolver para eliminar los riesgos que se han dado y cuarto, asesoramiento continuo de esos riesgos detectados y poner soluciones. Por otro lado, a la seguridad de la información[185] entendida como el conjunto de políticas, procedimientos y medidas preventivas y reactivas que afectan a la seguridad del tratamiento de los datos en cualquier formato, ya sea electrónico, papel, verbal, etc. y en cualquier etapa de su uso, recopilación, almacenamiento, procesamiento, transmisión y borrado.

[184]Entendido como el "conjunto de procedimientos y de buenas prácticas adoptados por las compañías, organizaciones, y demás personas jurídicas, a los efectos de poder identificar y clasificar los riesgos operativos y los de carácter legal a los que se enfrentan, y, así poder establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos". Recuperado de: https://confilegal.com/20200227-compliance-y-proteccion-de-datos-dos-caras-de-la-misma-moneda/ (fecha de consulta: 2023).

[185] De hecho, siendo el objetivo mantener los datos y la información personal de una organización seguros se hace uso o son de aplicación los principios de confidencialidad, integridad y disponibilidad, lo que se conoce como la Tríada CIA, a los que se añade los principios de trazabilidad, autenticidad y no repudio, que garantiza al receptor de una comunicación que el mensaje fue originado por el emisor y le previene que este niegue el envío de esa comunicación.

Por último, se evidencia que el término *compliance* está íntimamente relacionado con el de protección de datos y que no solo se lleva a cabo de forma técnica sino a través de políticas y procedimientos de confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los sistemas de información (es la capacidad de demostrar o probar la participación de las partes en una comunicación).

II.- En un segundo bloque se refleja que, todo lo anterior, se ha precedido de una breve aproximación a la noción de derechos humanos y su proceso de reconocimiento (Apartado 1), mediante los procesos de positivación, generalización, internacionalización, a los que se añadió el de especialización; evidenciándose que el reconocimiento de los derechos humanos, y en particular del derecho a la protección de datos, deriva de un progresivo desarrollo a nivel internacional, europeo y nacional español. Así, se ha reforzado la evidencia de que la protección de datos no tiene el carácter tan novedoso como aparentaba tener cuanto entró en vigor y aplicación el RGPD, aunque sí que marcó un antes y un después, pues fue a partir de entonces cuando se comenzó a dar la relevancia oportuna a este derecho en todas las áreas, los sectores y niveles, incluidos los ciudadanos.

En línea con lo anterior, se ha reforzado la evidencia que el derecho a la protección de datos tal y como lo conocemos y entendemos en la actualidad es resultado de un importante desarrollo y se ha revalorizado con la publicación y posterior entrada en vigor y aplicación del RGPD en el ámbito europeo; así como con la imposición de sanciones por vulneración de la normativa que han sido conocidas a nivel mediático en el ámbito internacional, europeo y español (como ocurrió con la sanción de gran calado social impuesta a *Facebook* en 2018 derivada de la cesión ilícita de datos personales por parte de la red social *Facebook* a la empresa *Cambridge Analytica)*. En su virtud, se ha ido generando un creciente interés en la tutela en relación con la protección de datos y la privacidad, configurando actualmente, junto con la ciberseguridad y la Inteligencia Artificial, las principales preocupaciones en todos los sectores.

Otra de las evidencias más destacadas de este primer apartado y en conexión con lo anterior, es que el reconocimiento de un ámbito privado de la persona física susceptible de ser legalmente protegido frente a toda injerencia arbitraria encuentra su origen hace

más de setenta años en el marco del Derecho Internacional. No obstante, no fue hasta mediados de los años ochenta cuando el derecho a la protección de datos pasó a ser considerado una facultad con sustantividad propia, independiente y autónoma del derecho a la intimidad personal y familiar, al que inicialmente se entendía unido. Esta consideración como derechos independientes y autónomos es la que se mantiene en la actualidad, entendiéndose que así debe mantenerse.

III.- Por último, en un tercer bloque se ha concretado el concepto de protección de datos personales, así como su delimitación del derecho fundamental a la intimidad personal y familiar por su distinta función, distinto objeto y contenido; y se han expuesto unas nociones básicas sobre el juicio de ponderación de derechos en caso de convergencia de derechos *in fine* (Apartado 5). En resumen, se ha evidenciado que **ambos derechos fueron positivados en la segunda mitad del siglo XX en el ordenamiento jurídico español, pero tras una evolución jurisprudencial se fueron configurando como independientes y autónomos, así como no absolutos, que comparten su carácter de derecho fundamental y el objetivo de ofrecer una eficaz protección constitucional de la vida personal y familiar.**

No obstante, se ha evidenciado que están **estrechamente interrelacionados por lo que en determinados supuestos pueden generarse dificultades o convergencias** sobre si el derecho en cuestión es uno u otro[186]. Así, el derecho a la **protección de datos es transversal, tiene confluencia y proyección en áreas de convergencia con otros derechos fundamentales, como los derechos a la tutela judicial efectiva, intimidad personal y familiar, derecho a la salud o derecho a la información y a la comunicación; siendo necesario hacer una ponderación de derechos**, siempre poniendo atención en no poner en riesgo los derechos y libertades de terceros.

Al hilo de lo anterior, se ha evidenciado que **son frecuentes las convergencias de derechos fundamentales, respecto a lo que se ha desarrollado el juicio de ponderación de derechos** en el caso en concreto. De hecho, se ha evidenciado

[186] Igual ocurre con los términos protección de datos y privacidad, pues a veces se habla de privacidad de forma más genérica, pero a nivel jurídico esta se podría situar entre la intimidad y la protección de datos que, insistimos no es lo mismo. La privacidad es subjetiva, para una persona puede ser dato íntimo como su fe, su número de cuenta bancaria o su correo electrónico; pero para otras no y lo exponen públicamente.

que, **en la convergencia en el ámbito penal entre protección de datos y derecho a la información veraz, el TC viene otorgando una prevalencia al derecho a la información veraz**, que no opera de forma automática, sino que habrá de ser valorada atendiendo a las circunstancias del caso en concreto.

Finalmente, se ha reafirmado la evidencia de que la **protección de datos y ciberseguridad configuran los principales retos a los que se enfrentan las empresas, los profesionales y la sociedad** en general. La protección de los datos personales no es una opción, sino un objetivo común compartido. **La tutela de los datos personales y de los derechos digitales sigue configurando uno de los retos actuales en todos los ámbitos y en particular, del Derecho Constitucional, debiendo ser el objetivo común compartido seguir promocionando la cultura de la protección de datos, la responsabilidad proactiva y la concienciación en la salvaguarda de los derechos digitales con la finalidad de que sean respetados y percibidos por la sociedad como una necesidad inherente a la dignidad humana, uno de los fundamentos del orden y de la paz social para evitar discriminaciones geográficas, pues la protección de datos es un asunto transnacional.**

A modo de corolario, la concienciación y la educación en materia de protección de datos, privacidad y seguridad de la información. La formación y la concienciación transparente y clara en todos los sectores y niveles resulta fundamental en el objetivo de una cultura global sobre protección de datos. Resulta trasladable a este ámbito la conocida frase “La educación es el arma más poderosa que puedes usar para cambiar el mundo” (Nelson Mandela).

Resumen y discusión del Capítulo II: "Aproximación a los nuevos derechos y garantías digitales reconocidos en la 3/2018".

En este Capítulo, de carácter más innovador y el primero que conforma la primera publicación del Compendio de la tesis, se ha reflejado el régimen jurídico en el sistema español en materia de protección de datos en relación con **el reconocimiento de un elenco de derechos y garantías digitales consagrados en el Título X de la LOPDGDD 3/18, cuyo reconocimiento explícito supuso un hito en el ordenamiento jurídico español**, como se ha mencionado anteriormente en el resumen y discusión del Capítulo I.

En resumen, se ha reforzado la evidencia de que la LOPDGDD 3/18 parte del reconocimiento del principio general de plena aplicabilidad en internet de la totalidad de los derechos y libertades consagrados en la CE y en los Tratados y Convenios Internacionales en los que España es parte. De ahí que, **todo usuario de los medios digitales mantiene en el entorno digital sus derechos, como el derecho a la vida, a la seguridad personal, a la libertad de expresión e información, a la intimidad, a la imagen, al honor, al secreto de las comunicaciones o a la protección de sus datos personales.** Aunque la LOPDGDD 3/18 va más allá, encomendando a los prestadores de servicios de la sociedad de información y a los proveedores de internet que contribuyan a garantizar la aplicación de los derechos reconocidos.

Sin embargo, **siguiendo la línea del RGPD, tampoco establece un catálogo de medidas concretas tendentes a garantizar tal aplicación de forma eficaz, correspondiendo a cada ente valorar e instaurar las medidas o herramientas oportunas y efectivas para cumplir con protección de datos, con la responsabilidad proactiva y con el reto del citado principio de plena aplicabilidad.**

En cuanto a los diecisiete derechos y garantías digitales reconocidos por la LOPDGDD 3/18, se han agrupado en tres secciones. Primero, los reconocidos en el entorno digital; segundo, los que se refieren a una especial protección al menor de edad, en su consideración de colectivo vulnerable y de mayor riesgo; y tercero, los derechos reconocidos en el ámbito laboral.

- Tras un análisis más a fondo de estos, en el **entorno digital** se ha evidenciado el reconocimiento del derecho al acceso universal, asequible y de calidad a internet independientemente de cualquier condición personal, social o económica; el derecho a la neutralidad de internet para que los prestadores de servicios de internet oferten sus servicios de forma transparente y sin discriminación a los usuarios por motivos técnicos o económicos; y del derecho a la seguridad digital para que las comunicaciones por medios digitales se transmitan y reciban de forma más segura posible y los usuarios sean informados de sus derechos.

  Adicionalmente, se ha reconocido el derecho a solicitar a los responsables de redes sociales y servicios equivalentes la rectificación de contenidos difundidos por terceros que vulneren los derechos al honor, la intimidad y a la libertad de comunicar y recibir libremente información veraz; y a solicitar la actualización de informaciones en medios de comunicación digitales cuando la información original no se adecue o refleje la situación actual por circunstancias posteriores a su publicación causándole un perjuicio. También, ha reconocido el derecho al olvido en búsquedas de internet y redes sociales y servicios equivalentes, junto al derecho a la portabilidad de los datos en dichas redes por el que se puede instar a sus prestadores recibir y transmitir los contenidos facilitados o que lo transmitan directamente a otro prestador indicado.

  Además, se ha evidenciado el reconocimiento del derecho a la educación digital con carácter inclusivo, en el uso de los medios digitales seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y particularmente, con el respeto de la intimidad personal y familiar y la protección de datos. En esta línea, en el marco universitario incluía la garantía en los planes de estudio de títulos habilitantes, formación en el uso y seguridad de los medios digitales y en garantía de los derechos en internet; e incluso que la Administraciones incorporen materias sobre la garantía de los derechos digitales y protección de datos en los temarios de pruebas selectivas a cuerpos superiores y a aquellos que traten datos.

  Se ha destacado el testamento digital en el reconocimiento de la facultad de toda persona de disponer el uso y destino de sus bienes digitales y la regla

general de que los vinculados al fallecido por razones familiares o, de hecho, así como sus herederos estén legitimados al acceso a los contenidos gestionados por los prestadores de servicio de la sociedad de información sobre los fallecidos, así como decidir su uso, destino o supresión. Salvo prohibición previa del fallecido expresa o que se establezca legalmente.

- En cuanto a la **especial protección de los menores en internet**, se ha evidenciado que la LOPDGDD 3/18 prevé que sus progenitores o representantes legales han de procurar un uso equilibrado y responsable de los medios digitales para garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos. Esta se protege hasta el punto de prever la intervención del Ministerio Fiscal en casos de uso o difusión de imágenes o datos personales de menores en redes sociales y servicios equivalentes que pudieran implicar intromisiones ilegítimas en sus derechos fundamentales, de cara a instar medidas cautelares y de protección oportunas.

  Destaca también, la evidencia de que, aunque se establezca en 14 años la edad para consentir válidamente el tratamiento de datos personales, corresponde a sus padres o representantes legales el ejercicio de derechos hasta la mayoría de edad. En general se evidencia que sigue la línea del RGPD y de la Ley Orgánica 1/1996 de protección jurídica del menor, así como que encomienda al Gobierno la aprobación de un Plan de Actuación para promover la formación difusión y concienciación para dicho uso seguro y responsable.

- En lo que respecta al **ámbito laboral**, se ha evidenciado el aumento del uso de las herramientas digitales, así como la necesidad de tutelar el bien jurídico de la intimidad de los trabajadores y su dignidad. Se ha analizado el reconocimiento del derecho a la intimidad en el uso de dispositivos digitales en el lugar de trabajo puestos a disposición por el empleador, con derecho a acceder al contenido derivado de su uso a los únicos efectos del control laboral y garantizar la integridad de los dispositivos. Sin embargo, esta facultad está limitada por el respeto de los derechos del trabajador y previa información clara expresa e inequívoca al respecto.

> Así mismo, se ha referenciado el reconocimiento del derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos, y ante el uso de sistemas de geolocalización, que han de respetar los estándares mínimos del derecho a la intimidad y establecer medidas adecuadas para respetarlo. También se ha destacado el reconocimiento al derecho a la desconexión digital para garantizar el respeto de los tiempos de descanso, permisos y vacaciones del trabajador, que no sería respetado en ciertos trabajos que requieren disponibilidad completa.

Aunque es de reconocer la importancia del reconocimiento de los derechos y garantías digitales, se ha concluido que **más que un nuevo catálogo de facultades, constituiría un elenco de facultades esenciales titularidad de la persona física que se encuentran ligadas a los derechos fundamentales a la protección de datos y a la intimidad.** Además, se ha puesto en evidencia que su implementación puede presentar problemas al no gozar de la trayectoria doctrinal y jurisprudencial en comparación con la de otros derechos, requiriendo un grado de determinación y concreción de su contenido por las autoridades competentes; así como que su reconocimiento positivo deviene insuficiente si no se acompaña de medidas de garantía, apoyo y financiación por las autoridades competentes para hacerlos efectivos.

A mayor abundamiento, al no establecerse medidas y protocolos para hacerlos eficaces, correspondería a cada ente establecer las que considere razonables, pudiendo dar lugar a divergencias interpretativas que supongan distintos niveles de protección de los derechos y garantías digitales. Además, se ha evidenciado la necesidad de que precisan ser ampliados y actualizados para proteger los derechos fundamentales de los ciudadanos conforme se vayan generando necesidades de tutela antes las innovaciones y la evolución tecnológicas.

Por último, **se ha reforzado la evidencia de que, aunque se han producido grandes avances en la tutela del derecho a la protección de datos y de los derechos digitales, sigue siendo preciso seguir trabajando en la formación y la promoción de la cultura de la protección de datos y de los derechos digitales, la responsabilidad proactiva y la concienciación en la salvaguarda de los derechos**

digitales con la finalidad de que sean respetados y percibidos por la sociedad como una necesidad inherente a la dignidad humana.

Resumen y discusión del Capítulo III: "Protección de datos personales en la Administración de Justicia española. Protocolo de Comunicación de la Justicia 2018".

En este Capítulo, que conforma la segunda publicación del Compendio de Publicaciones, se ha evidenciado que **en el ámbito judicial también son objeto de tratamiento datos personales de los intervinientes en los procedimientos judiciales por parte de jueces y tribunales, así como la Oficina judicial** que les sirve de soporte y apoyo. Así, en la Administración de Justicia española, jueces y tribunales tratan, en el ejercicio de su potestad jurisdiccional y dentro de su competencia, numerosos datos personales de los intervinientes en los procesos judiciales, surgiendo la obligación de asegurar la protección de su información personal, especialmente de las categorías sensibles de datos; toda vez que las consecuencias del tratamiento de datos ilícito, al margen de la normativa y de la ética, son perjudiciales y de difícil reparación, la vulneración del derecho fundamental a la protección de datos personales y el incumplimiento de la normativa sobre protección de datos.

También, se ha demostrado que **la protección de datos tiene un régimen jurídico particular en este ámbito, consistente fundamentalmente en la aplicación, junto a la normativa europea, de las especialidades de la LO 6/1985 del Poder Judicial en todos los órdenes judiciales (LOPJ), salvo en el orden penal en el que resulta de aplicación la Directiva 2016/690, y en España, su transposición por la Ley Orgánica 7/2021** (con carácter posterior a la publicación del artículo, de ahí que no se haga referencia a la misma), estando mientras tanto vigentes los artículos 22 y siguientes. y sus disposiciones de desarrollo de la LOPD 15/1999.

Se ha evidenciado que dicho régimen particular consiste, fundamentalmente en que **los tribunales han de mantener los ficheros necesarios para la tramitación adecuada de los procesos, así como los que se precisen para la adecuada gestión, con respeto a las garantías y derechos establecidos en la normativa de protección de datos**. Así mismo, **se distinguen ficheros jurisdiccionales**, en cuyo

caso el tratamiento se limitará a los datos en tanto se encuentran incorporados a los procesos de que conozcan y su finalidad se relacione directamente con el ejercicio de la potestad jurisdiccional (es decir, las resoluciones judiciales) **y los no jurisdiccionales,** que son los que constan en procedimientos gubernativos tramitados por juzgados y tribunales. Por ende, las particularidades consisten en que se distinguen dos tipos de ficheros de datos tratados por los órganos judiciales u Oficina Judicial en relación con los incorporados a los procesos de que conozcan: jurisdiccionales y no jurisdiccionales.

Respecto al tratamiento de los primeros, se ha evidenciado que **no se aplica el consentimiento del interesado como base de legitimación**, sino que se acude al resto de las bases previstas en el art. 6 RGPD, normalmente, el ejercicio de la potestad jurisdiccional (misión en interés público u obligación legal), sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba. Así, se ha constatado que rige el principio de licitud y se exigen las bases de legitimación del art. 6 RGPD, aunque no sería necesario el consentimiento para que los tribunales traten datos en el ejercicio de su potestad jurisdiccional, sino que esta legitima el tratamiento de datos en ficheros jurisdiccionales. Lo anterior, como se indicaba, sin perjuicio de lo que dispongan las reglas de la validez de la prueba, teniendo que acudir a la Ley de Enjuiciamiento civil y criminal según se trate.

Igualmente, se ha evidenciado **la corresponsabilidad de los ficheros jurisdiccionales de las Administraciones Públicas competentes en materia de dotación de medios materiales a la justicia y que el CGPJ es la autoridad de control de cumplimiento de la normativa de protección de datos en la administración de justicia española** (en relación con los ficheros jurisdiccionales); **mientras que para los no jurisdiccionales será la AEPD**. Además, se prevé que la AEPD prestará al CGPJ la colaboración que precise, pudiendo adoptar medidas reglamentariamente para garantizar el cumplimiento de medidas de seguridad conforme a la normativa de datos respecto a los tratamientos con fines no jurisdiccionales.

A la par, **se ha puesto en conexión el derecho de protección de datos con el derecho a la libertad de información mediante el análisis de las principales medidas y recomendaciones que el Protocolo de Comunicación de la Justicia de**

2018, elaborado por la Oficina de Comunicación del CGPJ, que evidencia que la actividad de los órganos judiciales genera información judicial de gran interés social y periodístico, especialmente en el ámbito penal; que los ciudadanos son titulares del derecho a la protección de sus datos, pero también del derecho a la libertad de información veraz por cualquier medio de comunicación, en relación con el principio constitucional de publicidad de actuaciones, por lo que en el ejercicio de este último cumplen un papel esencial los medios de comunicación.

Se han indicado medidas y recomendaciones en el citado Protocolo para garantizar el derecho a la información derivada de los tribunales de forma eficaz, clara veraz, objetiva y responsable, con respeto a los derechos de los implicados en los procesos judiciales, especialmente en el orden penal, tanto en fase de instrucción (como que las Oficinas de Comunicación pueden facilitar la información y resoluciones de asuntos relevantes, previa autorización del juez instructor, siempre que no se trate de diligencias de sumario y no perjudique a la finalidad de secreto sumarial), como en fase de juicio oral, en el que se evidencia que el proceso judicial se convierte en público desde se declara judicialmente el fin de la fase de instrucción; sin restricciones de acceso a la vista y a la información, salvo en casos excepcionales señalados por la ley.

- Adicionalmente, se ha evidenciado en esta fase de juicio oral, que, en cuanto a los funcionarios que intervienen en la vista, rige la LO 1/1982 sobre Protección Civil del Derecho al honor, la intimidad y la propia imagen, según la que el derecho a la propia imagen no impedirá su captación o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. Así mismo se ha evidenciado que España es uno de los países con mayor transcendencia informativa en la retransmisión de juicios, siendo muestra de ella la retransmisión completa y en directo del Juicio del *Procés* en el Tribunal Supremo; lo que contribuye se evidencia a la transparencia y a que la sociedad conozca y valore la relevante labor del Poder Judicial.

- En cuanto a la fase de publicación de las resoluciones judiciales, según el texto constitucional serán siempre motivadas y se pronunciarán en audiencia

> pública. En el ámbito penal la LOPJ establecía, además, que serán depositadas en la Oficina Judicial y se permitirá a cualquier interesado el acceso al texto y según el art. 235 bis LOPJ. Sin perjuicio de lo establecido legalmente, se prevé la posibilidad de acceso al texto íntegro o a determinados extremos o a otras resoluciones durante el proceso, únicamente previa disociación de los datos personales y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o garantía del anonimato, como víctimas o perjudicados.

Otra importante evidencia es que la LOPJ permite al poder judicial y a los letrados de la Administración de Justicia adoptar las medidas necesarias para la supresión de datos de los documentos a los que las partes pueden acceder durante la tramitación del proceso, siempre que no sean necesarios para garantizar su derecho a tutela judicial efectiva. Además, prevé que el acceso a las sentencias o a ciertos extremos también puede quedar restringido cuando pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o garantía del anonimato a las víctimas o perjudicados, cuando proceda, así como para evitar que sean usadas con fines contrarios a las leyes.

En esta línea, en los envíos a los medios de comunicación se les advertirá de su responsabilidad en la difusión de datos en la resolución judicial, de acuerdo con el criterio establecido por los órganos técnicos afectados y el DPO del CGPJ. En todo caso, se prevé que será de aplicación la normativa de protección de datos que contenga la citada resolución judicial adjunta, que no podrán ser cedidos ni comunicados con fines contrarios a las leyes.

En virtud de lo anterior, **se ha reforzado la evidencia de que la protección de datos es un objetivo común compartido, siendo conveniente** (consecuencia de las reformas legales y de las tendencias europeas) **elaborar una regulación sistemática completa, desarrollada de protección de datos en el ámbito jurisdiccional**, pues el actual régimen formado por varios artículos con remisión a otras normas deviene insuficiente. Además, los casos de filtraciones de datos en el ámbito judicial tienen el efecto de incidir directamente en la percepción de la ciudadanía de la justicia como mejorable y cuestionan el tratamiento de los datos en la Administración de Justicia.

Finalmente, se ha demostrado que **la elaboración de Protocolos de Comunicación de la Justicia**, como el de 2018 (o el más reciente y posterior a la publicación, de 2020), con recomendaciones concretas para que la información judicial llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados, **favorecen la garantía de los derechos y principios implicados** (información, publicidad de actuaciones, tutela judicial efectiva, intimidad, honor, protección de datos, imagen) convivan de forma pacífica.

A modo de actualización, se refleja que se publicó en España la Ley Orgánica 7/2021 que trasponía la Directiva 2016/690, de que, posteriormente a la publicación del citado artículo, se publicó El **Protocolo de Comunicación de la Justicia 2020**[187], presentado por el presidente del Tribunal Supremo y del CGPJ al Pleno del órgano de gobierno de los jueces el 28 de mayo de 2020, que constituye el texto vigente actualmente. Supuso la actualización del anterior, al incorporar un Capítulo dedicado a la publicidad de las actuaciones judiciales en el marco de las medidas de prevención de contagio por la pandemia COVID-19 adoptadas en las sedes judiciales; con el objetivo de seguir garantizando que la información que genera la actividad de Juzgados y Tribunales llegue al ciudadano, igualmente, de forma eficaz, clara, veraz, objetiva y responsable, con absoluto respeto a los derechos y observancia de los deberes de todos los implicados en procedimientos judiciales.

[187] Recuperado de: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Protocolo-de-Comunicacion-de-la-Justicia/ (fecha de consulta: 2024).

Resumen y discusión del Capítulo IV "El derecho fundamental a la protección de datos personales en el ámbito penal".

El Capítulo IV contiene la tercera de las publicaciones, reflejando las principales particularidades de protección de datos en el proceso penal, evidenciándose que en estos también existen una gran cantidad de datos relativos a los sujetos intervinientes, en la mayoría relevantes para la investigación criminal y la prueba, que han de ser necesariamente objeto de tratamiento por las autoridades competentes.

Cabe destacar que se ha reforzado la evidencia de que el orden penal es el de mayor interés social y mediático, evidenciándose también que la particularidad del régimen jurídico de protección de datos en el proceso penal consiste en que no se aplica directamente el marco normativo general de protección de datos al que se ha hecho referencia, sino que éste se aplica de forma supletoria. En cambio, sí tiene aplicación directa la Directiva 2016/680, que regula de forma específica el tratamiento de datos de personas físicas por autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones.

De otro lado, se ha evidenciado que, aunque tiene aspectos en común con la normativa general (principios básicos de protección de datos de licitud, adecuación, pertinencia y necesidad de los fines perseguidos), en algunos de sus preceptos permite la posibilidad de que en la concreta regulación de cada derecho el Estado pueda adoptar medidas que restrinjan el derecho. En particular cuando obstaculice investigaciones o procedimientos judiciales u oficiales o perjudique la prevención, detección, investigación o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; o implique un riesgo para la seguridad pública, nacional o de los derechos y libertades de terceros.

En España, se ha evidenciado que transcurrieron varios años hasta que se materializó la transposición de la citada Directiva, a través de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[i] seguía vigente la normativa interna española interpretada a la luz de la Directiva. Esta recogía que los ficheros creados por las Fuerzas y cuerpos de seguridad del Estado que contengan datos personales debían ser objeto de registro

permanente y que, por regla general, la recogida y tratamiento de datos para fines policiales sin consentimiento del afectado se limita a los supuestos y categorías de datos necesarios para la prevención de un peligro real para la seguridad pública o la represión de infracciones penales.

Adicionalmente, se ha constatado que **se restringe más el tratamiento de datos sensibles a únicamente cuando sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de la legalidad de la actuación administrativa o la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos judiciales.** Igualmente, que el tratamiento de datos en ficheros policiales está sujeto a límites y garantías, como ocurre con los judiciales, destacando que se prevé su cancelación cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento, atendiendo especialmente a criterios como la edad del afectado, el carácter de los datos y la necesidad de mantenerlos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Respecto al tratamiento de datos de condenas e infracciones penales o medidas de seguridad por Administración de Justicia, abogados o procuradores, se evidencia que solo puede llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la UE o de los Estados miembros que establezca las garantías adecuadas para los derechos y libertades de los interesados. También, de conformidad con el CP, el condenado que haya extinguido su responsabilidad penal tiene derecho a obtener del Ministerio de Justicia la cancelación de sus antecedentes penales, que dejen de constar en el Registro Central de Penados y Rebeldes cuando hayan transcurridos los plazos establecidos (art. 136 CP), cuyas inscripciones no son públicas.

Del análisis de la protección de datos como garantía en el proceso penal y en la actuación investigadora criminal, se evidencia que protección de datos y Derecho penal están sujetos a límites, en su sentido subjetivo al *ius puniendi* del Estado, estando restringido por las garantías de respeto a los derechos de la dignidad humana, los principios de legalidad, culpabilidad, intervención mínima o el de *non bis in ídem*.

Se ha demostrado que **la protección de datos opera como una garantía en el proceso penal** (como ocurre en fase de instrucción penal con las diligencias de sumario, que serán reservadas; o fase de juicio oral con las excepciones a la publicidad de los actos cuando, por ejemplo, le exijan razones de seguridad guarden público o la adecuada protección de los derechos fundamentales de los intervinientes). Así, se prevé que se podrá acordar la adopción de medidas para la protección de la intimidad de la víctima y de sus familiares, como la prohibición en todo caso de la divulgación o publicación de información relativa a la identidad de víctimas o menores.

También, se ha constado **que la protección de datos personales constituye una garantía en la actividad investigadora criminal y probatoria**, porque las autoridades competentes (que tratan datos para los fines de esclarecer hechos delictivos, determinar los intervinientes u obtener pruebas) han de tener la máxima observancia y respeto de los derechos fundamentales. En esta línea, se ha evidenciado que cuando la prueba se ha obtenido con vulneración del derecho la protección de datos o los derechos y libertades fundamentales no surtirá efecto, lo que no significa que los hechos averiguados sean falsos, no existan o no puedo decirse si son reales o no. Como ha puesto de manifiesto nuestro TS, la vulneración del citado derecho en relación con el investigado abre una grieta en la estructura del proceso penal y puede generar efectos contaminantes respecto de las pruebas obtenidas de forma ilícita y en lo que concierne a otros actos conectados con las mismas.

Del análisis de los delitos de descubrimiento y revelación de secretos en el CP, y sus tipos agravados, se ha evidenciado que el bien jurídico tutelado es la intimidad en su sentido más amplio como facultad de autodeterminación informativa, lo que puede llevar a confusión con el derecho a la protección de datos como facultad de control de la información personal, aunque se trata de dos derechos distintos y autónomos.

De otro lado, se evidencian las problemáticas de que puede considerarse que su tipificación podría exceder del principio de última *ratio* del derecho penal, teniendo en cuenta que los datos ya se tutelan por regulación específica. Además, pueden llegar a suponer la imposición de penas realmente gravosas para el derecho a la libertad personal, pudiendo llegar a prisión de cuatro a siete años por el delito de revelación de datos reservados personales que configuren un tipo agravado, como de datos sensibles o ser de un menor o persona de necesidad especial, realizado con fin

lucrativo. Otras problemáticas evidenciadas son que el consentimiento del sujeto pasivo conlleva la atipicidad de la conducta, que para su persecución requiere previa denuncia, y la regla del perdón el ofendido o su representante legal, que extingue la acción penal (lo que puede propiciar que se sigan realizando las conductas al no recibir las consecuencias negativas de su conducta).

Aunque esto ha sido matizado por los tribunales en el sentido de que es una regla general y hay que se ha excluido cuando se afecte a intereses generales, lo que explica que en esos casos tampoco sea precisa denuncia previa. Así mismo, contiene referencia a protección de datos y prevención de delitos, siendo en la práctica frecuentes los concursos de delitos de descubrimientos y revelación de secretos, así como con otros e intrusión informática, amenazas, coacciones, de acosos, calumnias e injurias, violencia de género, suplantación de identidad o estafas, entre otros.

Por tanto, **en el ámbito penal, protección de datos proyecta incidencia y múltiple repercusión, configurando una garantía en todas las fases del proceso penal** -orden jurisdiccional de mayor interés social y mediático- y en la actividad investigadora criminal. El tratamiento ilícito de datos constituye una infracción de la normativa sobre protección de datos, pero también puede suponer la comisión de uno o varios delitos, especialmente de los previstos en el Título X del Libro II en el CP (arts. 197 y siguientes), que pueden llegar a ser sancionados con hasta siete años de prisión. Estos dos ámbitos de tutela operan en sus ámbitos de competencias respectivas.

Un tratamiento ilícito que no fuese considerado delictivo por órganos judiciales, sí podría constituir una infracción a la normativa sobreprotección de datos. Las principales cuestiones problemáticas en los delitos de descubrimiento y revelación de secretos son las relativas al bien jurídico tutelado, la gravedad de las penas previstas para sus infractores y aquellas derivadas de necesidad de denuncia para su persecución y del efecto del perdón del ofendido.

Son **frecuentes los delitos de descubrimiento y revelación de secretos, y en general los tratamientos ilícitos de datos, concurran y favorezcan la comisión de otros delitos**, como de estafa, de ciberacoso, de suplantación de identidad, o los denominados delitos de *phising* y *carding*; es necesario tomar medidas tanto para evitar cometer estos delitos, como para prevenir ser víctimas, especialmente en

relación con los menores de edad, sometidos a mayores riesgos, por lo que han de ser especialmente protegidos.

Se ha reforzado la evidencia de que en el contexto actual **siguen aumentando las cifras de cibercriminalidad**, habiéndose evidenciado la sofisticación tanto las amenazas como los ciberataques y variado sus agentes[188] (ciberestafas, ciberacoso, ciberbullying, *phishing-car*, *phishing bancario, vishing*). Para hacer frente, se considera necesario tomar medidas para evitar cometer y ser víctimas de estos delitos, especialmente en el caso de los menores de edad al considerar que tienen un mayor riesgo, tal y como especificaba la *Guía de la AEPD sobre protección de datos y prevención de delitos* que se recuerda contiene medidas como, por ejemplo, apostar por la educación digital y frente a ciberdelitos, evitar facilitar información a través de internet a desconocidos, así como no hacer una sobreexposición de la información personal como medida de tutela.

Como último enfoque, se ha evidenciado que **la información emanada de procesos penales contiene datos que requieren un equilibrio entre los derechos de protección de datos y libertad de información veraz**. También, la necesidad de **seguir ahondando en la salvaguarda del derecho a la protección de datos y en la promoción de una cultura global de protección de la información personal y la privacidad**. Además, siendo el orden jurisdiccional penal el de mayor interés social y mediático, se conexionan ambos derechos, siendo habitual su confluencia, otorgando el TC una prevalencia al derecho a la libertad de información veraz por su capacidad para formar una opinión pública libre, indisoluble unida al pluralismo del Estado democrático; prevalencia que ha aclarado no opera de forma automática, sino solo en casos en los que no concurran otros factores en los que lleve a primar la intimidad, el honor o la propia imagen o la protección de datos.

[188]Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html.

Resumen y discusión del Capítulo V: "Protección de datos personales en el sector sanitario, en el contexto del derecho a la salud y de la digitalización impulsada por la pandemia COVID-19"

Por último, en el Capítulo V se ha comprobado que **la protección de datos tiene particularidades también en el ámbito sanitario**, en el que los datos de salud se consideran de carácter sensible y, por ende, susceptibles de una tutela adicional, por el efecto o las graves consecuencias que pueden ser del todo irreparables. En resumen, se han diferenciado conceptos esenciales, como los de datos genéticos y biométricos, y se ha manifestado que en el ámbito de la salud también el uso de medios digitales avanza a un ritmo sin precedentes; digitalización que se ha impulsado tras la pandemia COVID-19 y la situación excepcional de emergencia sanitaria en la que derivó a nivel global, que tuvo una repercusión en muchos derechos fundamentales, destacando el de protección de datos.

El **sector sanitario se encuentra inmerso en un proceso de adaptación a las nuevas tecnologías, tanto los medios, como todos los agentes que en él interactúan, impulsado exponencialmente con la crisis sanitaria derivada de la pandemia COVID-19**. Así, el uso de Internet, las TIC y la IA en el ámbito sanitario está en constante evolución, marcando la irrupción de la pandemia COVID-19 un punto de inflexión en el aumento de su utilización y poniendo a prueba las garantías del derecho a la protección de datos y también a la intimidad.

De otro lado, se ha constatado que **la telemedicina tiene múltiples ventajas para los pacientes, profesionales, centros y sistemas sanitarios; pero también conlleva retos**, como la falta de concienciación, formación, interoperabilidad, recursos económicos y financieros y legislación uniforme; el desigual acceso y uso de las TIC, la falta de cultura tecnológica o sensibilización de profesionales sanitarios y pacientes; la prácticamente inexistente regulación en la materia y que la mayoría de proveedores de servicios se encuentran fuera del Espacio Económico Europeo.

Igualmente, se ha evidenciado que la aplicación de la tecnología en las Historias Clínicas se considera un arma fundamental para identificar, entre otras, todos los tratamientos y patologías del usuario, la medicina preventiva, el desarrollo de líneas

epidemológicas, estadísticas de riesgos de amplios sectores poblacionales, prevenir incidencias futuras en la salud de la población; y para planificar sistemas de atención primaria. Aunque su uso también tiene ciertos riesgos que es preciso tener en cuenta y establecer cautelas. En conexión con lo anterior se he demostrado que **la Historia Clínica del paciente funciona como elemento fundamental de la asistencia y prestación sanitaria, dejando constancia de los datos que bajo criterio médico permitan ese conocimiento veraz y actualizado del estado de salud de la persona**. Información considerada fundamental para el conocimiento veraz y actualizado del estado de salud del paciente. Así mismo, se ha comprobado que la aplicación de medios digitales a la HC se valora positivamente por los usuarios de sanidad, e incluso un arma fundamental para identificar todos los tratamientos y patologías del usuario, para la medicina preventiva, desarrollar líneas epidemológicas o generar estadísticas de riesgos.

Adicionalmente, se ha evidenciado que **se aplican en este sector los mismos principios en materia de protección de datos, con las particularidades** (como las relativas al derecho de información, de limitación del plazo de conservación o al de limitación de la finalidad, pues el tratamiento ulterior de los datos con fines de archivo en interés público, de investigación científica o histórica o estadístico no se consideran incompatibles con los fines iniciales). También, que se prohíbe como regla general el tratamiento de datos de salud, salvo cuando concurran las circunstancias previstas (como que sea necesario para proteger intereses vitales del interesado). Igualmente, aplica la excepción del apartado 4 del artículo 9 RGPD de que los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, respecto al tratamiento de datos genéticos, biométrico o sobre salud; evidenciándose que no se logra de forma completa el objeto el RGPD de armonización en la materia.

Se ha evidenciado la **evolución de la telemedicina o *ehealth*** en los últimos años en los que la digitalización ha transformado el sector de la salud, y a su impulso derivado de la pandemia COVID-19, que generó la publicación de normativa durante la pandemia y la toma de medidas, como la aplicación de asistencia COVID-19, la obligación de exhibición del pasaporte COVID-19 u otras como la toma de temperatura o las aplicaciones de información voluntaria de contagios o cámaras infrarrojos para lecturas masivas de temperatura generaron debate respecto a los derechos y

libertades de las personas físicas y en particular, de la protección de datos personales y la normativa reguladora.

Al hilo de lo anterior, se ha evidenciado que aunque la Pandemia COVID-19 supuso un impulso en la digitalización del sector sanitario, también conllevó la implementación de medidas que afectaron y pusieron a prueba la protección de datos de los ciudadanos y supusieron restricciones, como la toma de temperatura públicas, aplicaciones informáticas para rastrear contactos estrechos de los casos con contagiados basada en interés público de controlar la difusión de la pandemia y de garantizar la asistencia sanitaria. Se mantuvo la regulación y los principios constitucionales españoles y las normas que se desarrolla, pero ha cambiado la preocupación sobre el control de los datos y la percepción de los desafíos en materia de privacidad.

En definitiva, se ha constatado que la telemedicina ha generado la revalorización del derecho a la salud, junto a otros derechos a raíz de la pandemia, lo que a su vez se ha reflejado en jurisprudencia convencional y constitucional (que contienen pronunciamientos integrándolo en el derecho fundamental a la vida).

Como último enfoque, respecto a la **telemedicina**, en sus tres dimensiones principales de teleconsulta, telemonitorización y teleformación, se han demostrado sus principales ventajas para los profesionales sanitarios, los pacientes y los centros sanitarios, como la reducción de tiempos de espera, costes o favorece la conciliación laboral-personal y familiar; pero también sus barreras en general y desde el punto de vista de protección de datos, como que se está en adaptación, faltando formación educación, junto a la falta de interoperabilidad, recursos financieros y falta de legislación uniforme y disposiciones legales específicas de protección de datos en el sector salud. Junto el desigual acceso y uso de las TIC, la brecha digital, la falta de cultura tecnológica o sensibilización de profesionales sanitarios o pacientes.

Al respecto de lo anterior, se ha demostrado que la LOPDGDD 3/18 detalla los responsables y encargados que han de proceder a la designación obligatoria de DPO, pero existe una falta de marcos legales uniformes entre los diferentes países, siendo problemático además la existencia de normativa autonómica propia configurando sistemas normativos. Otra barrera es la de que la mayoría de los proveedores que

prestan servicios se encuentran fuera del Espacio Económico Europeo, configurando transferencias internacionales que han de ser remediadas y controladas para que se garantice un nivel de protección similar que el europeo.

De otro lado, se ha evidenciado que existen otros **temas relevantes que también tienen impacto en protección de datos, como el IOT o las implicaciones de la IA y que generan continuos retos en materia de privacidad y protección de datos, que pueden suponer riesgos para la seguridad de la información y su uso indebido por parte de terceros**, así como el riesgo de los datos, muchos de ellos sensibles, siendo necesario el establecimiento de un sistema de garantías adicionales de protección de los datos sensibles.

Para finalizar, se ha reforzado igualmente la evidencia de que, **a pesar de que se han dado grandes pasos dado hacia la plena introducción de las TIC y nuevas tecnologías en el ámbito sanitario, es preciso seguir implementando mejoras**, especialmente respecto la interoperabilidad de los sistemas tecnológicos utilizados en las diferentes Comunidades Autónomas en el sistema sanitario español; así como fomentando y concienciando en la importancia de la privacidad y protección de los datos personales en todos los niveles.

Conclusiones

Conclusiones

A continuación, se exponen las principales conclusiones derivadas de la investigación, el análisis y posterior reflexión en torno al derecho a la protección de datos personales y su proyección en áreas de convergencia con otros derechos fundamentales sobre el que versa la presente tesis, en cumplimiento de los objetivos de la misma.

1ª El reconocimiento de un ámbito privado de la persona física susceptible de ser legalmente protegido frente a toda injerencia arbitraria encuentra su origen hace más de setenta años en el marco del Derecho Internacional. No obstante, fue a mediados de los años ochenta cuando el derecho a la protección de datos pasó a ser considerado un derecho con sustantividad propia, independiente y autónomo del derecho a la intimidad. De ahí, que se concluya que el derecho a la protección de datos personales de la persona física, en su concepción actual, deriva de una progresiva evolución normativa y social a nivel internacional y europeo, que se revalorizó con la entrada en vigor y aplicación del RGPD en el año 2018, y la LOPDGDD 3/18 en España.

2ª Actualmente, el derecho a la protección de datos constituye un derecho fundamental único, independiente y autónomo, de carácter transnacional y transversal, que atañe o se relaciona en múltiples ámbitos, y que en la práctica converge con otros derechos fundamentales, como puede ocurrir con el derecho a la libertad de información veraz. Dado que son frecuentes las convergencias de derechos fundamentales, se ha desarrollado el denominado "juicio de ponderación de derechos" y se ha evidenciado que cuando confluyen los derechos a la protección de datos y a la información veraz en el ámbito penal, el Tribunal Constitucional español viene otorgando una prevalencia al derecho a la información veraz. No obstante, se ha aclarado que dicha prevalencia no opera de forma automática, sino que habrá de ser valorada atendiendo a las circunstancias del caso en concreto.

3ª El RGPD supuso un hito jurídico en materia de protección de datos, introduciendo grandes novedades respecto a la normativa anterior, entre las que destacan el hecho de que otorga una protección tecnológicamente neutra, su aplicabilidad directa y el establecimiento de un catálogo de principios básicos (licitud, lealtad, transparencia, limitación del plazo de conservación, minimización de datos, entre otros), algunos de los cuales ya se recogían en normas anteriores a nivel internacional y europeo, aunque sí que introdujo otros novedosos como el derecho a la portabilidad. En conexión con ello, se ha evidenciado la influencia de la normativa europea sobre protección de datos en otros continentes y países, destacando haber sido y ser referente en el marco de protección de datos en América Latina, donde la protección de datos es tan diversa como los países que la forman, con realidades sociales, económicas, políticas y culturales muy diferentes.

4ª Igualmente, la LOPDGDD 3/18 constituyó otro hito jurídico pues vino a "adaptar" la normativa europea partiendo, además, del principio de plena aplicabilidad de internet a los derechos y libertades reconocidos; y contemplando que los prestadores de servicios contribuirán a garantizar su aplicación reconociendo además, un elenco de nuevos derechos y garantías digitales (facultades de acceso universal, asequible y de calidad a internet, del testamento digital, de desconexión digital del trabajador y de la educación digital, entre otras). No obstante, se ha evidenciado que más que una nueva generación de derechos, estos configuraron una serie de facultades ligadas a los derechos fundamentales a la protección de datos y a la intimidad; así como que su efectividad puede presentar limitaciones en la práctica.

5ª Desde el punto de vista de protección de datos, es igual de importante cumplir con la normativa como poder acreditar o evidenciar el cumplimiento. Para ello, se ha evidenciado la existencia de múltiples y diversos instrumentos, como la llevanza de un RAT con el contenido mínimo previsto en el RGPD y actualizado de forma periódica y cada vez que sea necesario; la concienciación y formación periódica en la materia a todos los niveles (en este sentido se concluye que el factor humano es y será el eslabón más importante dentro de la cadena de confidencialidad y ciberseguridad). Otras medidas destacables serían las de disponer e implantar textos legales adaptados a la empresa u organización que se trate (Políticas de protección de datos

y de Cookies, Guías o Manuales o procedimientos, Códigos de buenas prácticas, así como procedimientos de gestión del riesgo y de evaluación de impacto en tratamientos de datos personales y del nivel de riesgo de vulneración a la protección de datos.

6ª De la aplicación de protección de datos en el ámbito judicial se ha evidenciado, por un lado, que también son objeto de tratamiento datos de los intervinientes en los procedimientos judiciales y que, en la Administración de Justicia española, se tratan numerosos datos de los intervinientes en los procesos judiciales, surgiendo la obligación de asegurar la protección de su información personal.

7ª En conexión con la anterior conclusión, se ha evidenciado que, en el ámbito de la Administración de Justicia española, la protección de datos tiene un régimen jurídico particular consistente fundamentalmente en la aplicación, junto a la normativa europea de las especialidades de la LOPJ; salvo en el orden penal en el que resulta de aplicación la Directiva 2016/690, y en España, su transposición por la Ley Orgánica 7/2021. Otras de las particularidades son la diferenciación entre ficheros jurisdiccionales y no jurisdiccionales, como aquellos que constan en procedimientos gubernativos tramitados; así como que rige el principio de licitud aunque no sería necesario el consentimiento para que los tribunales traten datos en el ejercicio de su potestad jurisdiccional, sino que esta legitima el tratamiento de datos en ficheros jurisdiccionales, sin perjuicio de lo que dispongan las reglas de la validez de la prueba, teniendo que acudir a la Ley de Enjuiciamiento civil y criminal según se trate.

8ª Se ha constatado que en el ámbito judicial español los tribunales han de mantener los ficheros necesarios para la tramitación adecuada de los procesos, así como los que se precisen para la adecuada gestión con respeto a las garantías y derechos establecidos en la normativa de protección de datos. Además, se ha evidenciado la corresponsabilidad de los ficheros jurisdiccionales de las Administraciones Públicas competentes en materia de dotación de medios materiales a la justicia y que el CGPJ es la autoridad de control de cumplimiento de la normativa de protección de datos en la administración de justicia española (en relación con los ficheros jurisdiccionales); mientras que para los no jurisdiccionales es la AEPD.

9ª La actividad de los órganos judiciales genera información judicial de gran interés social y periodístico, especialmente en el ámbito penal, concluyéndose que la elaboración de Protocolos de Comunicación de la Justicia, con recomendaciones concretas para que la información judicial llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados, favorecen la garantía de los derechos y principios implicados convivan de forma pacífica.

10ª Una de las principales particularidades del régimen jurídico de protección de datos en el proceso penal consiste en que no se aplica directamente el marco normativo general de protección de datos, sino supletoriamente. Además, el tratamiento de datos en ficheros policiales está sujeto a límites y garantías, destacando que se prevé su cancelación cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento, atendiendo especialmente a criterios como la edad del afectado, el carácter de los datos y la necesidad de mantenerlos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

11ª La protección de datos configura una garantía tanto en el proceso penal (como en fase de instrucción penal con las diligencias de sumario, que serán reservadas; o fase de juicio oral con las excepciones a la publicidad de los actos cuando, por ejemplo, le exijan razones de seguridad guarden público o la adecuada protección de los derechos fundamentales de los intervinientes) como en la actuación investigadora criminal y probatoria, evidenciándose que la protección de datos y el Derecho penal están sujetos a límites, en su sentido subjetivo al *ius puniendi* del Estado, estando restringido por las garantías de respeto a los derechos de la dignidad humana, los principios de legalidad, culpabilidad, intervención mínima o el de *non bis in ídem*. De hecho, las autoridades competentes han de tener la máxima observancia y respeto de los derechos fundamentales y cuando la prueba se ha obtenido con vulneración del derecho la protección de datos o los derechos y libertades fundamentales no surtirá efecto, lo que no significa que los hechos averiguados sean falsos, no existan o no puedo decirse si son reales o no.

12ª La protección de datos tiene particularidades también en el ámbito sanitario y se aplican en este sector los mismos principios en materia de protección de datos, con las particularidades propias, como las relativas al derecho de información, de limitación del plazo de conservación o al de limitación de la finalidad, pues el tratamiento ulterior de los datos con fines de archivo en interés público, de investigación científica o histórica o estadístico no se consideran incompatibles con los fines iniciales.

13ª Aunque se han producido grandes avances normativos y sociales a nivel internacional, europeo y español, así como progresos sociales en la tutela y garantía del derecho a la privacidad y protección de datos, se concluye que aún queda trabajo por hacer para conseguir un cumplimiento real y transnacional de la normativa, potenciar una conciencia en todos los niveles y en general, una cultura global sobre protección de datos, armonizada y con homogeneidad regulatoria.

14ª En conexión con lo anterior, se ha evidenciado que el RGPD logró únicamente de forma parcial con su objetivo de homogeneización al dejar un cierto margen en algunos puntos a la legislación nacional (como la determinación de la edad del menor para prestar su consentimiento al tratamiento de datos). De ahí que, a su vez, se ha demostrado la necesidad de una especial protección homogénea de los menores de edad en todos los ámbitos, junto a una mayor atención y tutela por ser considerados menos conscientes de los riesgos, las consecuencias, y las garantías y derechos en materia de protección de datos.

15ª Casi seis años después de la entrada en vigor y aplicación del RGPD, se ha evidenciado que siguen existiendo empresas que no se han adaptado a la normativa y otras que se han adaptado al cumplimiento de la normativa de protección de datos sin profundizar o en un plano meramente “formal”, lo que no es conforme el espíritu del RGPD y de la cultura de cumplimiento en privacidad de protección de datos y la responsabilidad proactiva. De forma paralela se ha constatado que siguen incrementando los tratamientos ilícitos, así como que los casos y las modalidades se siguen repitiendo, dado que se ha evidenciado que se sigue sancionando a las

empresas por las mismas causas de incumplimiento en la materia y en aspectos esenciales de cumplimiento de la normativa.

16ª La protección de datos y la cibercriminalidad se siguen encontrando entre las principales preocupaciones en la época actual, configurando además un factor esencial de negocio en todas las empresas independientemente de su tamaño. Se ha constatado que son frecuentes los delitos de descubrimiento y revelación de secretos, y en general los tratamientos ilícitos de datos, concurran y favorezcan la comisión de otros delitos (como de estafa, de ciberacoso, de suplantación de identidad, o los denominados delitos de *phising* y *carding*, entre otros) siendo necesario tomar medidas tanto para evitar cometer estos delitos, como para prevenir ser víctimas, especialmente en relación con los menores de edad. Actualmente saber protegerse en el entorno virtual y proteger de forma adecuada los datos que se tratan es fundamental para el buen desarrollo de negocio y la confiabilidad de los interesados (clientes, empleados, etc.). Aunque se puede decir que la ciberseguridad afecta en mayor o menor medida a las empresas según su nivel de dependencia tecnológica.

17ª El riesgo de sanción de las empresas de todos los ámbitos y tamaños podría ser el mismo que antes de la regulación del RGPD, la diferencia es que ahora las sanciones son más en número, siendo esta tendencia al alza como se refleja en las Memorias que con carácter anual publica la AEPD, siendo las últimas las de 2021 y 2022.

18ª El uso de Internet, las TIC y la IA está en constante evolución, marcando la irrupción de la pandemia COVID-19 un punto de inflexión en el aumento de su utilización y poniendo a prueba las garantías del derecho a la protección de datos y también a la intimidad. Aunque la Pandemia COVID-19 supuso un impulso en la digitalización de todos los sectores, y en particular del sector sanitario, también supuso la implementación de medidas que afectaron y pusieron a prueba la protección de datos de los ciudadanos y supusieron restricciones. Se ha constatado que se mantuvo la regulación y los principios constitucionales españoles y las normas que se

desarrolla, pero ha cambiado la preocupación sobre el control de los datos y la percepción de los desafíos en materia de privacidad.

19ª A pesar de que se han dado grandes pasos dado hacia la plena introducción de las TIC y nuevas tecnologías en todos los ámbitos, y en particular en el ámbito sanitario, se concluye que es preciso seguir implementando mejoras, especialmente respecto la interoperabilidad de los sistemas tecnológicos utilizados en las diferentes Comunidades Autónomas en el sistema sanitario español; así como fomentando y concienciando en la importancia de la privacidad y protección de los datos personales en todos los niveles.

20ª La telemedicina, en sus tres dimensiones principales de teleconsulta, tele monitorización y teleformación, tiene grandes ventajas para los profesionales sanitarios, los pacientes y los centros sanitarios; pero también sigue teniendo barreras en general y desde el punto de vista de protección de datos, como que se está en adaptación, faltando formación educación, junto a la falta de interoperabilidad, recursos financieros. Junto el desigual acceso y uso de las TIC, la brecha digital, la falta de cultura tecnológica o sensibilización de profesionales sanitarios o pacientes.

A modo de **comentarios y conclusiones finales**, se considera que se han cumplido los objetivos generales y específicos del presente proyecto investigador que comenzó en el año 2018, así como resuelto sus interrogantes tanto los iniciales como los surgidos durante el periodo investigador.

Igualmente, se ha constatado que la metodología empleada y las adaptaciones que se han considerado necesario realizado durante el periodo investigador han sido efectivas para responder a las preguntas de la investigación. Aunque inicialmente, como se refleja en los Planes de Investigación, se proyectaba únicamente sobre el ámbito judicial, posteriormente se fue modelando conforme surgían nuevas preguntas o ideas en el proceso de investigación, ampliándose los ámbitos de proyección a las implicaciones de protección de datos en el ámbito penal, así como en el sector de la salud.

Adicionalmente, los resultados generan una gran reflexión e impacto real y actual, siendo útiles en el ámbito jurídico y académico y además, dejan abierta la posibilidad y aportan la sugerencia de seguir investigando en las hipótesis planteadas. Entre las futuras líneas de investigación, se considera que puede tener interés para la comunidad jurídica y académica seguir llevando a cabo trabajo de investigación en otras áreas de proyección del derecho a la protección de datos, como puede ser el ámbito civil o el ámbito del sector bancario o de seguros, entre muchos otros, puesto, como se ha evidenciado, el derecho a la protección de datos es un derecho transversal y global.

Otras de las posibles futuras líneas pueden consistir en estudios comparativos sobre la aplicación de la normativa europea sobre protección de datos en varios países de la UE, como pueden ser Irlanda, Portugal, Italia, Alemania y España para ver si se está produciendo un acercamiento en el objetivo de armonización del RGPD, de cara a encontrar puntos de encuentro y posibles mejoras y avances en la regulación en esta materia.

La innovación del presente trabajo se refleja en las publicaciones que lo compendian, especialmente las de los Capítulos III a V, pues existen numerosas publicaciones, pero ninguna realiza un estudio similar desde la óptica y tal y como se lleva a cabo en la presente tesis con la proyección del derecho fundamental a la protección de datos en los ámbitos antedichos, en los que se producen la convergencia entre derechos fundamentales. Además, se considera una forma de delimitar objetivos claros de la tesis y poner foco en temas concretos en las que se detecta la necesidad e interés de estudio, dejando para una eventual investigación posterior otros derechos fundamentales, no menos relevantes, sobre los que podría analizarse la posible convergencia.

También se considera innovador el formato de presentación de tesis por compendio en Ciencias Sociales y Jurídicas, en el campo del Derecho, puesto que es más ordinario encontrar este tipo de tesis en otros campos de conocimiento, como el de Ciencias Sociales, Políticas, del Comportamiento y de la Educación o de Ciencias de la Educación o en Ciencias naturales e ingenierías en general. Se ha optado por este formato pues se considera muy ventajoso, principalmente, porque permite la formación integral en el periodo de doctorado no solo en su área sino también a

través de las publicaciones académicas, revistas y libros de reconocido prestigio y de impacto en el sector, recibiendo una formación de una visión 360º, con la consecuente experiencia y competencias adicionales añadidas.
En línea con lo anterior, se plantea y considera deseable encontrar programas que, desde distintos niveles pudieran incidir en particular en la formación y protección de la privacidad y de los datos personales, la seguridad de la información y prevenir o minimizar los riesgos derivados de tratamientos ilícitos de datos, en un modo similar al que se reconoce lleva a cabo el INCIBE a través de cursos gratuitos en modalidad online sobre estas temáticas dirigidos a la ciudadanía en general y a docentes.

Finalmente, se considera que la actual investigación se sitúa en esta línea de trabajo a la que modestamente quisiera contribuir, incidiendo en que la protección de la privacidad y de los datos personales no es una opción, sino un objetivo común compartido, configurando la tutela de los datos personales y de los derechos digitales junto a la seguridad de la información unos de los retos de la sociedad actual.

Además, como mirada al futuro, se prevé el aumento de las cifras de cibercriminalidad, del uso generalizado de las TIC, las redes sociales, la red de internet; la evolución de las técnicas de IA (con los consiguientes peligros para los derechos y libertades de las personas física que supone) y el resto de las herramientas digitales. Por ende, se advierte que se seguirán generando nuevos escenarios en los que surgen nuevos retos y desafíos para la protección de datos, la privacidad y la ciberseguridad, aunque se prevé que también seguirá aumentando la preocupación social por la importancia de respetar y hacer respetar este derecho fundamental y cumplir la normativa reguladora. También, se prevé que se sigan produciendo con mayor frecuencia las convergencias de derechos en los que el derecho a la protección de datos será el auténtico protagonista (lo que no quiere decir que siempre debe prevalecer), con sus consiguientes ponderaciones de derechos según el caso en particular.

Referencias

Referencias

- Adsuara Varela, B., "El nuevo Reglamento General de Protección de Datos". Recuperado de: https://www.youtube.com/watch?v=U2thY0yEsIE.
- Álvarez-Pallete, J.M. “Informe Sociedad Digital en España”, Fundación Telefónica, 2019, pág. 8; y “La Sociedad de la Información en España”, Ariel S.A. y Fundación Telefónica, 2016, págs. 5 y ss.
- Amérigo Alonso, A., “El Real Decreto-Ley de protección de datos: una imprescindible solución temporal”, en *Revista del Colegio Notarial de Madrid*, 2018.
- Aparicio Salom, J., “Estudio sobre la protección de datos”, Aranzadi.
- Bratza, N. y Giakomopoulos, C. y Voordhoof, D., “Human rights challenges in the digital age: judicial perspectives”, ISBN 978-92-871-8998.
- Bueno de Mata, F. “Justicia y derecho en datos”, Tirant lo Blanch, 2023. Recuperado de: https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788411973496.
- Caridad Sebastian, M. y Ayuso García, M.D., “Situación de la brecha digital de género y medidas de inclusión en España”, Investig. Bibliog, vol. 25, núm. 55, México, 2011, págs. 227-252.
- “Sección Espacio Europeo de protección de datos”, Tercer trimestre de 2022, La Ley.
- Colmenero Guerra, J.A., “La protección de datos en la Administración de Justicia”, Portal Iberoamericano de Ciencias Penales, Instituto de Derecho Penal Europeo e Internacional, Universidad de Castilla- La Mancha. Recuperado de: http://www.cienciaspenales.net.
- Colmenero Guerra, “el derecho a la autodeterminación informativa” II Jornadas de estudio sobre protección de datos y derechos fundamentales”, Instituto Vasco de Administración Pública (IVAP),1991, págs. 304 y ss.

- Corazón Mira, R., “Algunas reflexiones sobre la protección de datos personales en el ámbito judicial”.

- Cremades López de Teruel, F.J., “Protección de datos y Poder Judicial”, Diario la Ley, 2018.

- Cuervo Álvarez, J., “Autodeterminación informativa”, 2014. Recuperado de: http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/#1.1.%20ASPECTOS%20GENERALES.

- De La Torre Reyes, T., “Evolución Histórica, concepto y fundamentación de los Derechos Humanos”, Módulo I, Universidad de Colima, 2008, pág. 30.

- Delgado Martín, J., “Investigación y prueba tecnológica en todas las jurisdicciones”, 2º Edición, Wolters Kluwer, 2018.

- Durán Rivacoba, R. y Castilla Barea, M. y Garrote Fernández Díez, I. y Grimalt Servera, P. y Martín García Ripoll M. y Navarro Castro, M. y Asociación de Profesores de Derecho Civil y Santos Morón, M.J. y García Garnica, M del C. y Plana Arnaldos, M y Díez Soto, C.M. y González Pacanowka, I., “Protección de datos personales”, Tirant lo Blanch, 2020. Recuperado de https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788490333907.

- Fernández Acevedo, J., Conferencia Centro de Empresarios de Jaén, 2018.

- Frossini, E. “Libertad, Igualdad, Internet”, ISBN:978-84-9190-756-5, Tirant lo Blanch, Ciudad de México, 2018, págs. 9 y 41. Traducción al español el libro publicado en italiano en 2016, pág. 22.

- García Almeida, A. y Medina Sánchez, N. y Castillo, Singh, C., “La brecha entre el primer y el tercer mundo en la actualidad” en *Revista Información Científica*, núm. 50.2, 2006, pág. 3.

- García Amado, J.A. “Conflictos de Derechos, Problemas Teóricos y Supuestos Prácticos”, Tirant lo Blanch, 2019.

- García Mahamut, R. “El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales”, Tirant lo Blanch.

- García Mahamut, R. y Mallén, T. y Pauner Chulvi, C. “Las cláusulas específicas del reglamento general de protección de datos en el ordenamiento jurídico español”, Tirant lo Blanch, 2021. Recuperado de: https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788413973524.

- Gene Spafford, “Mejores frases sobre seguridad informática”. Recuperado de: https://protegermipc.net/2017/04/04/las-mejores-frases-sobreseguridad-informatica/.

- Guía Rápida Protección de Datos. Aplicación del RGPD, Francis Lefevre, 2019, págs. 9 y ss.

- Gómez Montero, A., “Exposición sobre obsolescencia de los derechos” en Congreso de la Asociación de Constitucionalistas Españoles, 2018.

- Hernández Leal, E.J. y Duque Méndez, N.D. y Moreno Cadavid, J., “Big Data: una exploración de investigaciones, tecnologías y casos de aplicación”, en *Revista TecnoLógicas*, vol. 20, nº. 39, 2017.

- Hernández López, J.M. “Protección de datos personales Infracciones y sanciones penales”, Tirant lo Blanch, 2021. Recuperado de: https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788413979212.

- Hernández, M. “La geolocalización ante el COVID-19 como primera línea de defensa”, 2020. Recuperado de: https://www.diariojuridico.com/la-geolocalizacion-ante-el-covid-19-como-primera-linea-de-defensa/.

- Hidalgo Cerezo, A. “The data protection of minors. Special reference to its exceptions in health and educations fields”, La Ley 9926/2017 Derecho de Familia, núm. 15.

- H. Kelsen, “Principios de Derecho Internacional Público”, El Ateneo, Buenos Aires, 1965, (trad. de H. Caminos y E. C. 1952, Hermida del original *Principles of International Law*, Rinehart & Co., Nueva York,), págs. 124 y 125.

- “Informe sobre Medición de la Sociedad de la Información”, Resumen ejecutivo elaborado por la Unión Internacional de Telecomunicaciones, Ginebra, 2018,

págs. 2-3. Recuperado de: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-S.pdf.

- Kaiser, B. “La dictadura de los datos. La verdadera historia desde dentro de Cambridge Analytica”, Roharpercollins Publishe.

- Lera López, F. y Hernández Nanclares, N. y Blanco Vaca, C. “La “brecha digital” un reto para el desarrollo de la sociedad del conocimiento”, 2003.

- Manual Derecho Constitucional para preparación oposición de acceso a la Carrera Judicial y Fiscal, Carperi S.L, 2014.

- Marcos Ayjón, M. La protección de datos de carácter personal en la justicia penal. J. M., Bosch.

- Martínez Martínez, R., “Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública”, Diario La Ley, nº 9604, Sección Doctrina, 2020.

- Martínez Martínez, R., “El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto, AA.VV, Valencia, 2019, págs. 311-342.

- Megías Quirós, J.J., Recuperado de: http://revistas.ucm.es/index.php/ANDH/article(viewFile/ANDH0202110515A/20978.

- Moreno Bobadilla, A. y Serrano Maillo, M.I., “El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad”, Tirant lo Blanch, 2021.

- Murillo De la Cueva, L., “La confidencialidad de los datos personales: garantías el proceso judicial. La protección del derecho de intimidad de las personas (fichero de datos)”, Cuadernos de Derecho Judicial (XIII), CGPJ, Madrid, 1998, pág. 232.

- Muñoz García, C. “Regulación de la Inteligencia artificial en Europa. Incidencia en los regímenes jurídicos de protección de datos”, Tirant lo Blanch. Recuperado de: https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788411973434.

- Pacho Blanco, X. y Cabra Apalategui, J.M. y Hernández Marín, R. y Ordás Alonso, M. y García Amado, J.A., Segura Ortega, M. y Gutiérrez Santiago, R. y Sendín Mateos, J. y León Alonso, Marta. F. y Rodríguez Toubes Muñiz, J. y Pérez Bermejo, J. y Bonorino Ramírez, P.R. y Gutiérrez Santiago, P. y Ricoy Casas, R. y Rodríguez Boente, S. y Gimeno Presa, M. Argumentación Jurídica y Conflictos de Derechos, Tirant lo Blanch, 2021.

- Paz Canales, M. "Protección de datos en América Latina, urgente y necesaria", 2017.

- Peces Barba, Martínez, G., "Derecho Positivo de los Derechos Humanos", Colección Universitaria, Editorial Debate, Madrid, 1987.

- Pérez Luño Robledo, E.C., "El procedimiento de habeas data: el derecho procesal ante las nuevas tecnológicas", Dykinson, 2017.

- Pérez Luño, A.E., "Derechos Humanos, Estado de Derecho y Constitución", Tecnos, Madrid, 2010. pág. 50.

- Pérez Sola, N., "Diálogo entre Tribunales".

- Puerto Mendoza, A. "Derecho Digital, fundamentos básicos" Dikynson, 2019. Recuperado de: https://www.dykinson.com/libros/derecho-digital-fundamentos-basicos/9788445439524/.

- Puyol Montero, J. "La figura del delegado de protección de datos (DPD). Adaptado al Reglamento (UE) 2016/679 (RGPD) a la LO 3/2018, de 5 de diciembre (LOPDGDD) y al esquema de certificación de la Agencia Española de Datos", Aferre.

- Puyol, J. "Libro de test delegación de protección de datos (DPO) Dominio II", Tirant lo Blanch.

- Recio M., "Día de la Protección de Datos: El Convenio 108 y tus datos personales". Recuperado de: http://www.lawyerpress.com/blogs/LPe_Miguel_Recio_11.html.

- Recuerda Girela, M. A. “Tecnologías disruptivas”, Regulando el futuro, Aranzadi.

- Revenga Sánchez, M., “Regeneración Democrática y Reforma constitucional”, en Revenga Sánchez, M; Porras Nadales, A y Ruiz Rico-Ruiz, G. (Coord.), Tirant Lo Blanch, Valencia, 2017, pág.13.

- Rodríguez Ayuso, J.F. “Control externo de los obligados por el tratamiento de datos personales”, Bosch.

- Rodríguez Ayuso, J.F. “Figuras y responsabilidades en el tratamiento de datos personales”, Bosch.

- Rodríguez Ayuso, J.F. “Privacidad y Coronavirus: aspectos esenciales”, Dykinson, ISBN: 978-84-1324-795-3, 2020.

- Rodríguez Ayuso, J.F. “La protección de datos es una responsabilidad social”, Diario Responsabilidad. Recuperado de: https://diarioresponsale.com/opinion/26143-la-proteccion-de-datoses-una-responsabilidad-social.

- Rodríguez Cativiela, E.J. “El derecho al olvido: otra vuelta de tuerca”, en *Revista del Colegio Notarial de Madrid*, 2018.

- Rodríguez Zapata, J. “Teoría y práctica del Derecho Constitucional”, Tecnos, Madrid, 1996, pág. 296.

- Román Díaz, M. “La Declaración Universal de los derechos del hombre y sus conceptos de libertad e igualdad: una aproximación axiológica desde el prisma Bobbiano”, en *Revista de Ciencias Económicas*, 2011, pág.14.

- Rubio Llorente, F. “Derechos fundamentales, derechos humanos y Estado de Derecho”, en Punset Blanco, R. y Bastida Freijedo, F. y Varela Suanzes-Carpegna, J. (dirs.) “Fundamentos. Cuadernos monográficos de Teoría del Estado”, Derecho Público e Historia Constitucional, Junta General del Principado de Asturias, pág. 212

- Ruiz Robledo, A. “El régimen general de los derechos fundamentales, Compendio de Derecho Constitucional español”, Tirant Lo Blanch, Valencia, 2006.

- Schmarzo, B. “Big data, el poder de los datos”, Anaya Multimedia-Anaya Interactiva.

- Schneier, B. “Data Is a Toxic Asset, So Why Not Throw It Out?”, 2016, Recuperado de: https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html

- Sempere Samaniego, J., La Ley Privacidad 3090/2023, núm. 15, Sección Crónica de Corresponsales.

- Serrano García, J. “La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia”, Ediciones Bomarzo.

- Vega Iracelay, J. “The fundamental right to data protection in the Covid-19 pandemic: public emergency law, emergency or legal normality?”, La Ley Privacidad 5668/2021, Nº 8, Sección El Foro de la Privacidad, Wolters Kluwer.

- Viguri Cordero, J.A. y García Mahamut, R. y Mallén, T. y Pauner Chulvi, C. “La implementación del reglamento general de protección de datos en España y el impacto de sus cláusulas abiertas”, Tirant lo Blanch, 2023. Recuperado de: https://biblioteca.tirant.com/cloudLibrary/ebook/info/9788411478502.