SUJETOS RESPONSABLES POR VULNERACIÓN DE LAS NORMAS DE PROTECCIÓN DE DATOS. ESPECIAL REFERENCIA A LOS DATOS RELATIVOS A LA SALUD*

SUBJECTS RESPONSIBLE FOR VIOLATION OF THE RULES OF PROTECTION OF DATA HEALTH

Rev. Boliv. de Derecho Nº 30, julio 2020, ISSN: 2070-8157, pp. 40-75

* Trabajo realizado en el marco del Proyecto I+D+i «Retos investigación» del Programa estatal de I+D+i orientado a los Retos de la Sociedad del Ministerio de Ciencia, Innovación y Universidades: RTI2018-097354-B-100. «Contratos, transparencia y protección de datos en el mercado digital» (2019-2022)

Raquel GUILLÉN CATALÁN

ARTÍCULO RECIBIDO: 25 de mayo de 2020
ARTÍCULO APROBADO: 28 de mayo de 2020

RESUMEN: En el presente estudio se analiza quiénes son los distintos responsables por vulneración de las normas de protección de datos relativos a la salud, en particular en la situación de crisis sanitaria actual, tanto en el ámbito de la imposición de multas administrativas, como por la causación de daños y perjuicios.

PALABRAS CLAVE: Protección de datos, datos relativos a la salud, sujetos responsables, multas administrativas, daños y perjuicios.

ABSTRACT: *TThis study analyzes who are the different parties responsible for the infringement of rules of the health data, particularly in the current health crisis situation, both in the area of imposing of administrative fines and for causing of damages.*

KEY WORDS: *Data protection, health data, responsible subjects, administrative fines and damages.*

I. INTRODUCCIÓN.

El derecho fundamental de la protección de datos es el derecho que nos permite acceder, rectificar y cancelar la información almacenada y disponer de los propios datos personales, es decir, es el derecho a controlar la veracidad o exactitud de dichos datos, de impedir la difusión de éstos y de verificar su utilización para el fin autorizado[1], en suma, conocer el tratamiento que terceros hacen de nuestros datos[2], cobrando mayor relevancia cuando nos encontramos ante el tratamiento de datos sensibles relativos a la salud y sin duda, en la actualidad, en un tránsito hacia el tratamiento masivo de datos[3], el conocido como big data[4].

No obstante, en la situación actual en la que nos encontramos, conviviendo en un estado de alarma dictado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el mencionado estado de alarma para la gestión de la situación

1 Perez Luño, A.: *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1984, pp. 316- 375.

2 Solar Calvo, P.: "La protección de datos en la UE: recapitulación de novedades", *Revista Aranzadi Unión Europea*, núm. 1, 2017, pp. 76 y ss.

3 La Profª. Cobas señala que protección de los datos personales se ha extendido de manera galopante a otros conceptos como big data y minería de datos. Vid. Cobas Cobiella, Mª. E.: "Protección de los datos personales. Bases de datos. Big data. Un nuevo paradigma", en AA.VV.: *Los derechos fundamentales. Perspectiva entre América y Europa* (coord. por Cánovas González D. y Vega Cardona R. J.), UniAcademia Leyer, Bogotá, 2019, p. 122.

4 Concretamente el Prof. Vázquez De Castro señala que son tratamientos inteligentes y a gran escala de datos masivos o macrodatos. Vid. Vázquez De Castro, E.: "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 46, 2018, p. 52.

• Raquel Guillén Catalán
Profesora Titular de Derecho Civil de la Universitat de València. Doctora en Derecho por la Universidad de Valencia, con Sobresaliente Cum Laude y Premio extraordinario. En relación con la investigación, que se centra en la protección de datos, el derecho contractual, protección a los consumidores y ADRs, quisiera resaltar la publicación de cuatro monografías, así como numerosos capítulos y artículos en editoriales y revistas de reconocido prestigio (Revista Actualidad Jurídica Iberoamericana, Revista de Derecho Patrimonial, Revista de Derecho y Nuevas tecnologías, etc). He realizados contribuciones a congresos, nacionales e internacionales y participado en proyectos I+D+I, siendo IP en dos de ellos. Correo electrónico: raquel.guillen@uv.es.

de crisis sanitaria ocasionada por la COVID-19, y sus sucesivas prórrogas, donde existen limitaciones a la libertad de circulación, cabe plantearse si la protección de los datos puede verse alterada en atención a las excepcionales circunstancias, especialmente pensando en la continua recopilación de datos sensibles derivados de la crisis sanitaria actual, no sólo por las Administraciones públicas o instituciones sanitarias, sino también por las empresas a sus trabajadores e, incluso, por los propios ciudadanos hacia las empresas cuando realizan una entrevista de trabajo y manifiestan que son inmunes a la enfermedad o la creación de los llamados pasaportes sanitarios.

Al respecto la Agencia Española de Protección de Datos ha sido concluyente en su Informe 0017/2020 donde afirma literalmente que "la normativa de protección de datos personales, en tanto que, dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada"[5].

En la actualidad, la protección de datos se regula por 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 (RGPD). Así como, por Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) [6] que no sólo ha integrado algunas de las normas establecidas en el RGPD[7], sino que ha complementado la misma, atendiendo a que los Estados miembros debían precisar algunos aspectos que quedaban sin concretar en la normativa europea[8], dotando con ello de mayor seguridad jurídica[9].

5 Informe 0017/2020 de la Agencia Española de Protección de Datos, p. 1, disponible en https://www.aepd.es/es/documento/2020-0017.pdf.

6 Para mayor información sobre el iter parlamentario de la norma, véase, Martínez Vázquez, F.: "La tramitación parlamentaria de la Ley Orgánica de protección de datos personales y garantías de los derechos digitales", en AA.VV.: *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. por Rallo Lombarte, A.), Tirant Lo Blanch, Valencia, 2019, pp. 53-78.

7 Vid. García Mexía, P. L.: "La singular naturaleza jurídica del Reglamento General de protección de datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, pp. 25-26.

8 Junto con el objetivo mencionado, se debe señalar que la promulgación de la LOPDGDD también supuso completar el RGPD con medidas más eficaces y clarificar la normativa aplicable al derogar expresamente la LOPD. Vid. Amérigo Alonso, J.: "Objeto y ámbito de aplicación", en AA.VV.: *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. por Rallo Lombarte, A.), Tirant Lo Blanch, Valencia, 2019, p. 80.

9 Cobas Cobiella, Mª. E.: "Protección de los datos personales", cit., p. 129.

El citado Reglamento es aplicable en todos los Estados de la Unión Europea y pretende homogeneizar[10] la normativa en materia de protección de datos[11], impidiendo que exista disparidad de regulaciones en cada Estado miembro[12], así como reforzar los estándares de exigencia de su protección[13], finalidad de unificación y armonización que no cumplía la derogada Directiva[14].

La protección que se dispensa a través de la normativa señalada sería inútil si, a la vez, no se estableciera un régimen disciplinario que garantizase el cumplimiento de la legislación y la posibilidad de solicitar el resarcimiento de los daños producidos por el incumplimiento de la citada regulación, más, teniendo en cuenta, el impacto que tienen las tecnologías en el ámbito de la salud, ya no sólo por las innumerables ventajas que ofrecen, como la monitorización de algunas enfermedades o el desarrollo del big data para obtener un diagnóstico más personalizado[15], sino también por los nuevos retos a los que hacer frente.

Al respecto, piénsese, por ejemplo, en el desarrollo de las apps de salud[16], tanto aquellas que se utilizan para detectar enfermedades, para combatirlas creando aplicaciones de rastreo de contactos o de autodiagnóstico e incluso para contener epidemias en fases de desescalada, como para potenciar prácticas saludables, lo se denomina como Mobile Health[17], en la explotación no consentida de los datos biométricos o en los riesgos que plantea la implementación de la

10 Téngase en cuenta que mientras los reglamentos son normas vinculantes, las directivas únicamente establecen unos objetivos para todos los Estados miembros que deben trasponer a través de su propio ordenamiento jurídico. Vid. López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos*, Sepín, Madrid, 2017, p.63.

11 Uno de los objetivos del Reglamento era "evitar la fragmentación de los ordenamientos jurídicos de los Estados miembros en materia de protección de datos personales, especialmente en lo relativo al régimen sancionador". Vid. Martínez Vázquez, F.: "La tramitación parlamentaria…", cit., pp. 55-56.

12 Al respecto se debe tener en cuenta que una de las críticas a la Directiva 95/46/CE relativa a la protección de las personas físicas en lo respectivo al tratamiento de datos personales se refería a "la excesiva libertad con la que contaban los Estados miembros a la hora de establecer el correspondiente régimen sancionador". Corral Sastre, A.: "El régimen sancionador en materia de protección de datos en el Reglamento general de la Unión Europea", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, p.573.

13 Dopazo Fraguio, P.: "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos)", *Revista Española de Derecho Europeo*, núm. 68, 2018, pp. 115 y ss.

14 Cobas Cobiella, M. E.: "Protección de los datos personales", cit., p. 131.

15 El big data se caracteriza por la velocidad de su procesamiento de datos, y el volumen y la variedad de éstos. Vid. Vázquez De Castro, E.: "Titularidad y responsabilidad en la economía del dato", cit., p. 53. Es evidente los enormes beneficios que origina la utilización del big data, pues permite obtener, tratar y analizar una gran cantidad de datos con rapidez y agilidad, como, por ejemplo, en la lucha contra la COVID-19, puesto que nos ayudará a crear modelos estadísticos de datos sobre la expansión del virus e incluso de manera preventiva para detectar futuros rebrotes, puesto que, analizando a través de algoritmos un conjunto de datos, de forma automatizada darán lugar a unas correlaciones que son las que permitirán llegar a las conclusiones.

16 Ramón Fernández, F.: "La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico", *Revista métodos de información*, vol. 8, núm. 14, 2017, pp. 5-25.

17 Ramón Fernández, F.: "Discriminación por condiciones de salud. Protección de datos y consumidores: una reflexión tras la reforma de la Ley General para la defensa de los consumidores y usuarios", *Revista de Derecho Privado*, núm. 1, 2019, p. 52.

historia clínica digital[18], así como en la utilización del big data la falta de control por parte de los interesados de los datos[19], bien porque se encuentran accesibles al público o bien porque se extraen a través de las diversas herramientas instaladas en los distintos dispositivos electrónicos[20] y que posteriormente se vinculan de manera automatizada con otros datos, creando perfiles[21], en nuestro caso, perfiles de salud, sanitarios o epidemiológicos, aunque, si bien es cierto, esta potencial vertiente del tratamiento masivo de datos está mucho más desarrollada en el ámbito del consumo[22].

Esta preocupación sobre la utilización de la tecnología y los datos personales relativos a la salud, la ha puesto en evidencia, recientemente, la propia Unión Europea en su Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados y en la Comunicación de la Comisión al Parlamento europeo, al consejo económico y social europeo y al Comité de las Regiones "Una estrategia europea de datos" de 19 de febrero de 2020 donde afirma literalmente que "los ciudadanos tienen derecho, en particular, a acceder a sus datos personales en materia de salud y a controlarlos, así como a solicitar su portabilidad".

Con la actual pandemia de la COVID-19, las autoridades sanitarias de los distintos Estados miembros han tenido que hacer frente a la propagación del virus utilizando todas las herramientas que tenían a su alcance. Las tecnologías han desempeñado un papel relevante, tal y como afirma la propia Recomendación, pero su éxito dependerá, en gran medida, en la confianza que los ciudadanos tengamos en que las aplicaciones móviles garantizan una utilización de nuestros datos personales limitada a los fines concretos para los que han sido creadas.

Por todo ello, el presente artículo realiza un breve estudio de los sujetos, personas físicas o jurídicas, sobre los que se aplica el RGPD, dejando al margen

18 Para un estudio exhaustivo de la historia clínica digital y los datos personales, véase, entre otros, Cristea Uivaru, L: *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud,* Bosch, Barcelona, 2018; Florencia Cabrera, R.: "Historia clínica digital y la protección de datos personales, reflexiones humanísticas", en AA.VV.: *FODERTICS 7.0: estudios sobre derecho digital* (coord. por González Pulido, I.), Comares, Granada, 2019, pp. 33-39.

19 Romeo Casabona, C. M.: "Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada,* núm. extra 1, 2019, pp. 85-127.

20 Vázquez De Castro, E.: "Titularidad y responsabilidad en la economía del dato", cit., p. 54

21 No obstante, téngase en cuenta que la utilización d ellos citados algoritmos inteligentes "conlleva riesgos de discriminación, por lo que deben establecerse garantías procesales, transparencia y comprensión de la información". Vid. Ramón Fernández, F.: "Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?", *Diario La Ley*, núm. 9365, 25 de febrero de 2019, p. 3.

22 Cobas Cobiella, Mª. E.: "Protección de los datos personales", cit., p. 155

el debate sobre la responsabilidad de la vulneración de datos por robots[23], a los que los interesados pueden dirigir tanto tus reclamaciones por infracción de las normas de la citada norma europea, como la acción de indemnización por daños y perjuicios causados en el incumplimiento de la normativa de protección de datos como un mecanismo de resarcimiento del que disponen, haciendo especial hincapié no solo en la identificación de la diversa tipología de sujetos responsables, sino haciendo un planteamiento previo sobre el ámbito de aplicación de la normativa europea, así como la tipología de datos sensibles específicos sobre los que recae este estudio, dejando al margen tanto el estudio del régimen de infracciones o sanciones contemplado en la normativa europea y española, como los principios del sistema de responsabilidad contemplado en el RGPD y las características del ejercicio de la acción de responsabilidad correspondiente.

II. LOS DATOS RELATIVOS A LA SALUD.

1. Delimitación del término "dato personal".

El art. 4 RGPD señala que dato personal es toda información sobre una persona física identificada o identificable, tal y como se venía afirmando ya en la letra a) de su art. 2 de la deroga directiva[24].

No obstante, respecto a las personas identificables, el Considerando 26 RGPD señala que "para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física".

Además, precisa el legislador europeo que "para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos".

Por tanto, el mencionado criterio de probabilidad razonable de que se utilicen medios para identificar a una persona servirá para concretar la aplicación o no de la normativa de protección de datos, es decir, aunque los datos tratados sean de carácter personal resultará de aplicación la normativa relativa a la protección de datos únicamente cuando se empleen todos los medios que puedan ser

23 Ramón Fernández, F.: "Robótica, inteligencia", cit., p.8.

24 El citado precepto señalaba literalmente que se entendía por dato personal «toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

razonablemente utilizados y sin esfuerzos proporcionados para relacionar esas informaciones con las personas físicas identificables.

Por ese motivo, hay que tener presente que uno de los peligros señalados en la introducción de este artículo, la utilización del big data, desde el momento en que se realicen tratamientos de datos de forma anonimizada dejan de ser los datos de carácter personal y estaríamos fuera de lo previsto en la RGPD, ya que en el caso de que no sea posible identificar a un individuo o la identificación requiera esfuerzos desproporcionados, no será de aplicación la normativa de protección de datos[25], puesto que en el proceso de big data lo más importante no es la información concreta que pueda asociarse a una persona, sino la información en sí[26].

Así mismo, se debe hacer referencia que el citado precepto, como novedad introducida por el RGPD, señala, específicamente, como dato personal los siguientes identificadores: "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"[27].

Dicha lista es ejemplificativa y puede ser ampliada con cualquier otra información sobre una persona física identificada o identificable, es decir, aquella persona cuya identidad pueda determinarse, directa o indirectamente.

Debe analizarse juntamente con el Considerando 30 RGPD que establece que las personas físicas pueden ser asociadas a determinados identificadores en línea facilitados por sus dispositivos o aplicaciones, como las direcciones IP o las "cookies"[28] y que ello, combinado con otros datos recibidos por los servidores, puede suponer la elaboración de perfiles de las personas físicas e identificarlas[29].

25 Por tanto, cuando hay una relación entre un identificador y una persona serán de aplicación los principios de Protección de Datos. Vid. Arias Pou, M.: "Definiciones a efectos del Reglamento General de Protección de datos", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, p. 116.

26 Vázquez De Castro, E.: "Titularidad y responsabilidad", cit., p. 58.

27 "El Reglamento actualiza el listado de ejemplos que recogía la Directiva". Vid. Arias Pou, M.: "Definiciones", cit., p. 117.

28 En este sentido se pronuncia el apartado 2.2 de la Guía sobre el uso de las cookies de noviembre de 2019 de la Agencia Española de Protección de Datos.
Disponible en https://www.aepd.es/sites/default/files/2019-12/guia-cookies_1.pdf.

29 Vid. La STJUE de 1 de octubre de 2019 en relación con los requisitos del consentimiento válido del interesado para el tratamiento de datos personales y la obtención de su información personal mediante el establecimiento de cookies en su propio equipo informático. Sin entrar en el contenido de la sentencia mencionó el hecho que no hay consentimiento válido si se autoriza la utilización de cookies si se autoriza mediante una casilla por defecto.

2. Los datos especialmente protegidos. Especial referencia a los datos de la salud.

No todas las categorías de datos personales tienen la misma protección dentro de la normativa europea.

Se debe destacar la específica atención que realiza el legislador europeo a los denominados "datos especialmente protegidos" en el art. 9 RGPD, por afectar al núcleo más íntimo de la personalidad[30].

La normativa europea incluye dentro de la tipología de datos especialmente protegidos aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

El objetivo de este epígrafe es abordar, de manera sistemática, la noción de los datos de la salud clarificando qué tipología de datos incluimos en esa clasificación, con la finalidad de poder identificarlos para determinar su régimen jurídico aplicable y poder conocer si se han incumplido las obligaciones establecidas por la normativa para cada uno de los posibles sujetos responsables que veremos más adelante.

El apartado 15 del art. 4 RGPD contiene la definición de datos relativos a la salud, introduciendo de ese modo un término nuevo que no existía en la directiva derogada, estableciendo que son aquellos "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

Como se observa el legislador europeo pretende establecer un objeto delimitado con la finalidad de evitar ambigüedades que haga imprecisa la citada categoría de estos datos acotando específicamente qué información puede incluirse en la misma.

Concretamente, si atendemos a la literalidad del precepto, las informaciones que se incluyen en la categoría de datos relativos a la salud son aquellas referentes a la salud física o mental y los servicios de atención sanitaria[31].

30 Jove Villares, D.: "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización", *Revista Derecho y Salud*, núm. 1, 2017, p. 58.

31 Es decir, el dato de salud sigue refiriéndose a la salud pasada, presente y futura, y no creo que en su aplicación práctica tengamos ningún ejemplo de problemas prácticos en cuando al concepto. Vid. Pariente De Prada, J. I.: "Los Datos de Salud en el nuevo Reglamento Europeo de Protección de Datos", *I+S: informática y salud,* núm. 122, 2017, p. 13).

Como se observa no se ha optado por un elenco de datos, sino por una definición concreta[32]. Evidentemente, la recogida de los datos relacionados con la COVID-19 son datos de salud catalogados como categoría especial de datos, puesto que, por ejemplo, conforme a la interpretación del Considerando 35 RGPD se podría incluir como dato relativo a la salud "todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca 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", es decir, independientemente de quien sea la fuente de la información[33] e independientemente del medio a través del cual ha sido tratado, piénsese, por ejemplo, las redes sociales[34].

Junto con los datos relativos a la salud, es necesario mencionar por su especial protección y su relación con los datos relativos a la salud, los datos genéticos y los datos biométricos[35], aunque, dejando al margen las discusiones doctrinales sobre si éstos son un subtipo de datos relativos a la salud[36] o una categoría autónoma[37].

Se podría afirmar que la actual tendencia es entender a los datos genéticos como categoría diferenciada de los datos a la salud, atendiendo a que el RGPD los define de manera separada[38].

---

32 Al respecto señala que si se hubiera optado por un elenco de datos debería ser no taxativo. Vid. Jove Villares, D.: "Datos relativos a la salud", cit., p. 59.

33 Vid. Arias Pou, M.: "Definiciones", cit., p. 126.

34 Véase March Cerdá, J. C.: "Redes sociales, salud y pacientes", en AA.VV.: *Medios de comunicación y salud* (coord. por Del Pozo Cruz, J. T., Román San Miguel, A., Alcántara López, R. y Domínguez Lázaro, M. R.), Astigi, Sevilla, 2015, pp. 181-226.

35 Para mayor información sobre las diferencias entre los datos relativos a la salud y el resto de categorías señaladas, véase Pérez Gómez, J. M.: "La protección de los datos de salud" en AA.VV.: *Hacia un nuevo derecho de protección de datos* (coord. por Rallo Lombarte, A. y García Mahamut, R.), Tirant Lo Blanch, Valencia, 2015, pp. 621-668.

36 Al respecto véase. Ramón Fernández, F.: "Transparencia y protección de datos especialmente protegidos en genética y la salud desde el punto de vista civil y del buen gobierno", *Diario La Ley*, núm. 9281, 2018, pp. 1-15 o Álvarez Rigaudias, C.: "Tratamiento de datos de salud", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, pp. 172-176.

37 Por ejemplo, en el art. 5.1.g) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter señala que "En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética". No tanto desde un punto de vista doctrinal, donde siempre se ha procurado remarcar la singularidad de los datos genéticos, ya sea considerándolos como una tipología afín (Andreu Martínez, M. B., Pardo López, M. M. y Alarcón Sevilla, V.: "Hacia un nuevo uso de los datos de la salud", *Ius et Scientia*, vol. 3, núm. 1, 2017, p. 166).

38 Jove Villares, D.: "Datos relativos a la salud", cit., p.62.

El apartado 13) del art. 4 RGPD señala que se entiende por «datos genéticos», los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona[39], es decir, a través de un análisis cromosómico, un análisis del ADN o ARN, o elemento por el que se obtenga información equivalente[40].

Por su parte, el apartado 14) del citado precepto define los datos biométricos como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

El tratamiento de los datos relativos a la salud requiere como categoría especial de datos que se cumpla las previsiones establecidas en el art. 9 RGPD, es decir, queda prohibido dicho tratamiento con carácter general, salvo que se cumpla cualquiera de las excepciones establecidas en el apartado segundo del mencionado artículo. Por ejemplo, que el interesado dé su consentimiento explícito para el tratamiento de dichos datos personales; que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social; que el tratamiento 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; que el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; que el tratamiento es sea 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, entre otros.

Dicho precepto debe ponerse en relación con lo señalado en los Considerandos 53 y 54 RGPD, aún más si cabe en la situación de pandemia en la cual nos encontramos.

El tenor literal del Considerando 53 señala que "las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con

39 Según el art. 45 Ley 14/2007, de 3 de julio, de investigación biomédica se garantizará el derecho a la intimidad y el respeto a la voluntad del sujeto en torno a la información, confidencialidad de los datos genéticos de carácter personal.

40 Arias Pou, M.: "Definiciones", cit., p. 125.

fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública.

El Considerando 54 nos recuerda que el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública y matiza qué debe interpretarse por salud pública, remitiéndonos a la definición contenido en la letra c) del art. 2 del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, es decir, "todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad".

En consecuencia, si se prescinde del consentimiento de los interesados este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros, centros residenciales o entidades públicas o sanitarias, traten los datos personales con otros fines.

Paralelamente, el art. 9 LOPDGDD relativo a las categorías especiales de datos se remite al párrafo segundo del art. 9 RGPD y, además, contempla la posibilidad de que se establezcan requisitos adicionales relativos a su seguridad y confidencialidad para el tratamiento de datos de la salud amparados en una norma con rango de ley, en particular, cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte[41]. No obstante, por ahora, habrá que esperar la normativa reglamentaria.

41 Posibilidad amparada en el párrafo cuarto del art. 9 RGPD, en atención a las peculiares características que las singularizan. Vid. Jove Villares, D.: "Datos relativos a la salud", cit., p. 63

III. SUJETOS INCLUIDOS EN EL ÁMBITO DE APLICACIÓN DEL RGPD.

A continuación, se va a hacer referencia, a una serie de extremos que considero esenciales para poder entender con mayor precisión quienes pueden ser responsables ante la vulneración de las obligaciones establecidas en el RGPD[42].

Con el objetivo de conocer con exactitud quiénes serán los sujetos responsables de las infracciones y de los daños y perjuicios causados por el incumplimiento de las normas contenidas en el RGPD, se debe señalar que el Reglamento europeo ha dado un paso importante en relación a clarificar la cuestión relativa a la aplicación de la normativa europea de protección de datos a los encargados y responsables de los ficheros que estuvieran establecidos fuera de la UE, puesto que diferencia entre el ámbito de aplicación objetivo y territorial, con la finalidad de que las personas físicas no nos veamos privadas de nuestro derecho a la protección de datos.

Respecto a la primera cuestión concerniente al ámbito objetivo de aplicación, el art. 2 RGPD establece, en su párrafo primero, que el Reglamento "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Por un lado, al no hacer referencia el precepto expresamente a los datos de residentes en la Unión Europea se debe entender que se aplica a toda persona física, independientemente de su nacionalidad o residencia[43].

Por otro lado, respecto a qué tipo de tratamientos es aplicable el RGPD, el precepto citado literalmente menciona tanto los tratamientos automatizados, como los manuales, pero en este segundo supuesto la aplicación del Reglamento se limita a aquellos supuestos en que los datos se incorporaren o estén destinados a ser incluidos en un fichero[44].

Así mismo, se debe hacer mención expresa a la no aplicabilidad del RGPD cuando el tratamiento es efectuado por una persona física en el ejercicio de

42 Debe tenerse en cuenta que junto el Reglamento existen otra normativa europea que regula aspectos específicos en relación a la privacidad, como, por ejemplo, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) que, se prevé que, en breve, sea sustituía por el Reglamento del Parlamento europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónica. En relación con las dudas de conciliación entre las diversas normativas, véase López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos*, cit., pp. 60 y 77.

43 En esta línea se pronuncia el Considerando 14 RGPD que señala expresamente que "la protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales".

44 Así lo especifica el Considerando 15 RGPD.

actividades exclusivamente personales o domésticas[45], es decir, sin relación alguna a actividades profesionales o comerciales[46].

Con relación a la cuestión relativa al ámbito de aplicación territorial[47], el párrafo primero del art. 3 establece, con carácter general, que el RGPD se aplicará al "tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no".

Como se observa se hace referencia, primeramente, para la aplicación de la norma únicamente al lugar del establecimiento en la Unión Europea. En definitiva, tal y como señala previamente el Considerando 22, un establecimiento implica el ejercicio de manera efectiva y real de una actividad, independientemente de que sea una sucursal o una filial con personalidad jurídica, puesto que no es determinante la personalidad jurídica en la que ha sido constituida.

Además, se debe comentar la posibilidad de que los responsables o los encargados tengan más de un establecimiento en la Unión Europea, en cuyo caso se debe acudir al término de establecimiento principal que se define en el art. 4.16) RGPD[48].

A continuación, el párrafo segundo del art. 3 RGPD, a diferencia de la derogada redacción de la Directiva de protección de datos[49], señala que el tratamiento se aplica también al tratamiento de datos personales de interesados que residan en la Unión, realizado por un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con[50]:

45 Al respecto, el Considerando 18 RGPD pone, como ejemplo, la utilización por los propios ciudadanos de las redes sociales. Piénsese también en un repertorio de direcciones. Para más información, sobre el alcance de esta excepción y su interpretación jurisprudencial, véase Amérigo Alonso, J.: "Objeto y ámbito de aplicación", cit., pp. 97-98.

46 Por tanto, comparto la apreciación de la reconocida doctrina que esta exclusión no se aplicaría ante tratamientos que tuvieran interés oneroso. Vid. Uriarte Landa, I.: "Ámbito de aplicación material", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, p. 68.

47 Para un estudio del iter legislativo del precepto y un análisis comparado con la Directiva, Vid. Ripoll Carulla, S.: "Aplicación territorial del Reglamento", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, pp. 77-96.

48 La citada definición que delimita el concepto de establecimiento principal contribuye a identificar el establecimiento principal cuando el sujeto responsable cuente con establecimientos en más de un Estado miembro. Vid. Arias Pou, M.: "Definiciones", cit., pp. 116 y 130.

49 El art. 4.1.c) Directiva 95/46/CE señalaba que ésta era de aplicación cuando «el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en el caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea».

50 La redacción de este precepto pretende «superar la territorialidad del establecimiento para poner el foco en la residencia del interesado o afectado». Vid. Amérigo Alonso, J.: "Objeto y ámbito de aplicación", cit., p. 106.

la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a éstos se les requiere su pago[51]. Al respecto, aclara el propio RGPD que la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, no bastan para determinar la intención de ofrecer bienes y servicios, sino que debe atenderse a otros factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros[52];

el control de su comportamiento, en la medida en que éste tenga lugar en la Unión[53]. Para determinar si una actividad de tratamiento controla el comportamiento de los interesados, "debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes"[54].

Como se observa, el legislador europeo especifica y clarifica los criterios para determinar si se aplica la normativa europea de protección de datos a los residentes en la Unión Europea, cuando el responsable o encargado no lo sea, ya que deja de hacer mención a la ambigua expresión de la Directiva 95/46/CE, lo cual favorece la aplicación de la normativa de protección de datos[55], debiendo los distintos responsables de los tratamientos, independientemente de su ubicación, cumplir con la misma[56].

En esta línea se pronuncia el art. 30 LOPDGDD que establece que en los supuestos de aplicación del RGPD a los responsables o encargados del tratamiento no establecidos en la Unión Europea y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer

51 Para un mayor análisis de la modificación introducida por el RGPD respecto a la Directiva en este aspecto, véase López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos*, cit., pp. 106-107.

52 Vid. Considerando 23 RGPD.

53 Por tanto, se incluiría cualquier persona jurídica que fuera elegida para realizar el tratamiento, independientemente de su estructura societaria. Por ejemplo, una filial. Vid. Minero Alejandre, G.: "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario jurídico y económico escurialense*, núm. 50, 2017, p. 37.

54 Al respecto véase el Considerando 24 RGPD.

55 Piénsese, por ejemplo, en la aplicabilidad de la normativa europea a las redes sociales, puesto que muchas de ellas están ubicadas en terceros países fuera de la Unión. Vid. Gil Antón, A. M., *¿Privacidad del menor en internet?,* Aranzadi, Pamplona, 2015, p. 121.

56 En esta línea véase, Rallo Lombarte, A.: "España en la vanguardia de la Protección de datos: nuevos retos del Reglamento Europeo", en AA.VV.: *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de datos. Adaptado al Proyecto de Ley Orgánica de Protección de datos de 10 de noviembre de 2017* (coord. por López Calvo, J.), Wolters Kluwer, Madrid, 2018, p.79.

al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en la normativa europea.

Del mismo modo, en el supuesto de indemnización por daños y perjuicios por vulneración de la normativa de protección de datos, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

En consecuencia, se puede afirmar que el legislador europeo considera la problemática de la protección de datos como una cuestión global y no solo territorial y, por ello, el nuevo RGPD ha pretendido simplificar las dificultades que existían en la práctica para interpretar la aplicación de la normativa europea a los titulares de los ficheros no pertenecientes a la Unión Europea.

IV. EL RÉGIMEN DE RESPONSABILIDAD DE LOS SUJETOS INTERVINIENTES EN LA PROTECCIÓN DE DATOS.

En primer lugar, y antes de analizar en particular los diversos sujetos responsables ante la vulneración de la normativa de protección de datos, se debe precisar que el RGPD establece una doble vertiente de protección: las multas administrativas y las indemnizaciones por daños y perjuicios.

1. El régimen de infracciones y sanciones administrativas.

La aprobación del RGPD ha supuesto la introducción de numerosas novedades para hacer efectivo el cumplimiento de las obligaciones en materia de protección de datos.

En particular, respecto del régimen de infracciones y sanciones administrativas, el legislador europeo ya no enumera de manera exhaustiva cada conducta tipificada como tal, sino que se remite al incumplimiento de las obligaciones de cada uno de los sujetos responsables de las infracciones.

Sin olvidar, que el legislador europeo ha suprimido en el Reglamento la distinción de infracciones y sanciones en muy graves, graves y leves, aunque el legislador español la ha seguido recogiendo por tradición legislativa la citada diferenciación en la LOPDGDD.

No podemos dejar de mencionar que el Reglamento europeo tampoco despeja las dudas referidas al plazo de prescripción de las infracciones y de las sanciones, cuya laguna deberá ser suplida por las normativas de los Estados miembros[57].

57 En el ordenamiento jurídico español se debe acudir a los arts. 72, 73, 74 LOPDGDD respecto a la prescripción de las infracciones y al art. 78 LOPDGDD con relación a la prescripción de las sanciones.

Respecto a la cuantificación de las sanciones, aunque sin especificar una clasificación, distingue diversas sanciones dependiendo la vulneración concreta realizada por el sujeto responsable[58] y se debe resaltar la finalidad disuasoria del art. 83 RGPD al haber incrementado considerablemente las cuantías de las multas administrativas.

Así, por ejemplo, por una parte, el párrafo cuarto del citado precepto especifica las siguientes infracciones con su correlativa sanción que pueden alcanzar los diez millones de euros o si se trata de una empresa del 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior optándose por la de mayor cuantía:

- Las obligaciones del responsable y del encargado a tenor de los arts. 8, 11, 25 a 39, 42 y 43.

- Las obligaciones de los organismos de certificación a tenor de los arts. 42 y 43;

- Las obligaciones de la autoridad de control a tenor del art. 41, apartado 4[59].

Por otra parte, el párrafo quinto y sexto señalan las siguientes infracciones a las que se les aumenta la cuantía económica, hasta los veinte millones de euros o si es una empresa el 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, dependiendo de la gravedad de la infracción cometida, optándose por la de mayor cuantía:

- Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los arts. 5, 6, 7 y 9[60].

- Los derechos de los interesados a tenor de los arts. 12 a 22[61].

- Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los arts. 44 a 49;

- Toda obligación que adopten los Estados miembros en relación con situaciones específicas de tratamiento, como la conciliación entre la

58 Para conocer con mayor exactitud el tipo de infracciones que han sido sancionadas hasta la actualidad por la AEPD, véase el estudio exhaustivo de Royo V. y Méler, N.: "Multas impuestas por la AEPD en aplicación del RGPD: motivos y cuantías", *Diario La Ley*, 5 de septiembre de 2019, pp. 1-4.

59 Tal y como señala el Prof. Corral hay una defectuosa traducción del reglamento, puesto que al hablar de autoridades de control realmente se debería haber hecho referencia a los órganos de supervisión del cumplimiento de los códigos de conducta. Vid. Corral Sastre, A.: "El régimen sancionador, cit., p. 576.

60 Por ejemplo, las normas relativas a la licitud del tratamiento, las condiciones del consentimiento o el tratamiento de datos especiales.

61 Piénsese, por ejemplo, en las vulneraciones de los derechos de acceso, rectificación, supresión, portabilidad u oposición.

protección de datos y la libertad de información o el acceso a documentos oficiales, o el tratamiento del número nacional de identificación.

- El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control.

- El incumplimiento de las resoluciones de la autoridad de control.

Es necesario tener en cuenta que "el nuevo Reglamento establece un parámetro de cumplimiento que obliga a demostrar la existencia de diligencia debida por parte de los responsables y encargados, de forma que, si no existe, se estaría incumplimiento de facto el Reglamento"[62].

No obstante, un aspecto positivo que se debe resaltar de la aprobación del RGPD y a los efectos que aquí nos interesan, es el referente a los sujetos responsables de las infracciones que pueden ser sancionados, tal y como se puede deducir de lo ya señalado, puesto que ya no sólo responderán los encargados y los responsables del tratamiento, sino también los organismos de control y las autoridades de supervisión de los códigos de conducta, pero no se pronuncia específicamente sobre los organismos públicos infractores, quedando, por tanto, a la discreción de cada Estado miembro de su sanción.

Por tanto, a continuación, señalaremos brevemente cada uno de los sujetos anteriormente mencionados.

El art. 4.7 RGPD define al responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento", es decir, será considerado como responsable del tratamiento todo ciudadano, empresa u organismo que decida realizar un tratamiento de datos de carácter personal y decida sobre cómo debe realizarse el mismo, aunque no haya hecho él directamente la recogida de los datos[63].

Por el contrario, el apartado 8) del art. 4 RGPD entiende por encargado, aquella "persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento", es decir, toda persona que no siendo el titular del fichero realiza alguna función relacionada al tratamiento de los datos, pero actuando bajo las directrices o instrucciones del

62 Vid. López Álvarez, L. F.: "La responsabilidad del responsable", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, p. 291.

63 La cuestión principal para el responsable hace responsable del fichero es decidir para que se van a utilizar los datos y qué medio se van a emplear en los tratamientos que se van a realizar. Arias Pou, M.: "Definiciones", cit., p. 123.

responsable del tratamiento. Por ende, no tiene capacidad para decidir ni sobre los datos que recoge ni los medios que utiliza ni la finalidad a la que los destina[64].

Al respecto, el art. 33, párrafo segundo, LOPDGDD, clarifica todavía más dicha distinción, al concretar que "tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el art. 28.3 RGPD[65]", es decir, se puede afirmar la necesaria formalización de un contrato de prestación de servicios entre el responsable y el encargado[66], siempre y cuando no se enmarquen en la contratación del sector público, puesto que queda al margen de este precepto.

No obstante, aunque exista dicho contrato entre el sujeto responsable y el que debería ser calificado como encargado, este último será considerado responsable si actúa en su propio nombre y sin que los titulares de los datos personales observen que actúa en nombre de un tercero, es decir, del responsable del tratamiento.

Así mismo, el inciso del citado apartado añade que también tendrá la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

Junto con los responsables y los encargados de los tratamientos también serán responsables los representantes de éstos cuando no estén establecidos en el territorio de la Unión Europea, como se ha visto en el epígrafe anterior.

Así mismo, pueden también ser sujetos responsables terceros intervinientes, como los organismos de control y las autoridades de supervisión de los códigos de conducta.

Por un parte, el apartado 21 del art. 4 establece que la "autoridad de control" es la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el art. 51, es decir, de conformidad con el citado precepto aquel organismo público independiente que tiene la responsabilidad de "supervisar

64 Arias Pou, M.: "Definiciones", cit., p. 124.

65 El citado apartado establece que "el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable". Además, dicho contrato estipulará, entre otros aspectos, que el encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable".

66 Este contrato entre el responsable del tratamiento y el encargado del fichero representa una garantía que permite la utilización de los datos por las partes sin considerar que se ha producido la cesión de datos. Arias Pou, M.: "Definiciones", cit., p. 124.

la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión".

Por otra parte, el art. 41, párrafo primero, establece la posibilidad de que la autoridad de control acredite a otro organismo para que supervise el cumplimiento de un código de conducta que se haya elaborado con la finalidad de contribuir a la correcta aplicación de RGPD, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas, en virtud art. 40 RGPD.

Por último, considero que España, aunque ha perdido la oportunidad de sancionar económicamente a los organismos públicos cuando infringen la normativa de protección de datos, puesto que el art. 77 LOPDGDD únicamente establece el apercibimiento y la publicación de la resolución, dará ejemplo a través de la aplicación de las medidas sancionatorias previstas por la legislación vigente, especialmente con el inicio de medidas disciplinarias correspondientes frente a la persona física responsable de la infracción.

2. La indemnización por daños y perjuicios.

A) Reconocimiento del derecho.

Junto con el régimen sancionatorio mencionado, el art. 82 RGPD regula el derecho a la indemnización de los interesados por los daños y perjuicios causados como consecuencia de la infracción de las normas contenidas en el RGPD, así como de los actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y de las normas de los propios Estados Miembro, de conformidad con el Considerando 146 RGPD.

No obstante, se debe señalar que esta previsión indemnizatoria prevista en la norma europea, no es novedosa, puesto que ya se contemplaba en el art. 19 de nuestra derogada Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (LOPD) el derecho a la indemnización de las personas físicas como consecuencia del incumplimiento de lo dispuesto en la LOPD por parte del responsable o del encargado del tratamiento, siempre que se sufriera un daño o lesión en sus bienes o derechos a través de una acción por responsabilidad civil[67], que derivaba del mandato a los legisladores nacionales que se preveía en el art. 23 Directiva 95/46/CE para que reconociesen el derecho a indemnización.

67 El derogado art. 19 LOPD regulaba el "Derecho a indemnización", indicando que "Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación

Se debe precisar que, en la actualidad, la actual LOPDGDD, no hace referencia alguna al citado derecho de indemnización por vulneración de la normativa de protección de datos.

Aunque el RGPD es de obligado cumplimiento y directamente aplicable a cada Estado Miembro, no hubiera habido ningún inconveniente en que la legislación actual se hubiera pronunciado al respecto, al contrario, hubiera sido positivo, puesto que, al igual que sucede con el régimen sancionador, el RGPD no derogaría el régimen previsto en la normativa nacional, sino que lo desplazaría[68] a aquellos supuestos no incluidos en el ámbito de aplicación del Reglamento[69].

B) Sujetos responsables.

En relación con los sujetos responsables, se debe señalar que la obligación de indemnizar recae, de conformidad con el art. 82 RGPD, a todo "responsable o el encargado del tratamiento", como consecuencia de una infracción del Reglamento.

No obstante, hay que precisar que el contenido de la obligación de indemnizar de cada uno de los sujetos mencionados, derivada de los daños y perjuicios causados, difiere en uno y otro supuesto, aunque la finalidad última, en todo caso, como establece el Considerando 146, es que "los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos".

Por tanto, en atención a que ya hemos definido quién es el responsable y quien es el encargado del fichero, procederemos a ver las diferencias entre la responsabilidad de uno y otro en materia de resarcimiento de los daños y perjuicios que hayan podido causar por la vulneración de la normativa de protección de datos.

Al respecto el apartado segundo del citado precepto, establece que mientras el responsable responderá por los daños y perjuicios causados por la operación de tratamiento cuando ésta no cumpla la normativa, el encargado solo responderá "por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable".

reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".

68 El Prof. Corral señala literalmente que "el régimen sancionador que establece la Ley orgánica de protección de datos actual queda postergado a la aplicación de aquellos supuestos que queden fuera del ámbito de aplicación material del reglamento". Corral Sastre, A.: "El régimen sancionador", cit., p. 573.

69 Vid. Amérigo Alonso, J.: "Objeto y ámbito de aplicación", cit., p. 95.

No obstante, tanto el responsable como el encargado del tratamiento estarán exentos de responsabilidad si demuestran que no son responsables del hecho que causa el daño, en virtud de los establecido en el apartado 3 del art. 82 RGPD.

Amén de lo anterior, al encargado del tratamiento se le establece una responsabilidad limitada[70], puesto que únicamente responderá cuando no haya cumplido con sus obligaciones específicamente previstas para él o cuando haya actuado al margen o en contra de las directrices señaladas por el responsable del tratamiento.

En cambio, el responsable del tratamiento será responsable siempre que haya incumplido la normativa independientemente del tipo de actuación, y no sólo por sus propios actos, sino por los daños derivados de una infracción cometida por sus encargados del tratamiento[71].

Continuando con la presencia de otros sujetos en el tratamiento de los datos, piénsese en la posibilidad de que el encargado del tratamiento haya subcontratado la realización de sus funciones en el tratamiento. Dicha facultad está contemplada, a sensu contrario, en el apartado 2 del art. 28 RGPD que establece que "el encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable".

Por ende, si el responsable autoriza al encargado, éste podrá requerir la colaboración de otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable. En cuyo caso, en virtud del párrafo 4 del mencionado precepto, se impondrán a este otro encargado, mediante contrato, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado.

Sin embargo, y a efectos del sujeto responsable en caso de daños y perjuicios, es importante reseñar, que, en el supuesto de hecho reflejado, el RGPD, no establece la responsabilidad por hecho propio del encargado subcontratado, sino que el encargado inicial "seguirá siendo plenamente responsable ante el responsable del

70 Como señala el Prof. Rubí, aunque se haya previsto una responsabilidad limitada, *podrá beneficiar a los perjudicados para el resarcimiento de los daños causados, puesto que muchas funciones del tratamiento de datos son encargadas a grandes empresas con menores riesgos de insolvencia para resarcir el daño. Vid.* Rubí Puig, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil,* vol. V, núm. 4 (octubre-diciembre), 2018, *p. 65.*

71 Al respecto hay autores que señalan que "l*a responsabilidad del responsable no deriva de una eventual falta de diligencia en la selección o supervisión del comportamiento del encargado (culpa in eligendo, culpa in vigilando), sino de una asunción primaria de todos los daños que puedan ocasionarse a raíz de un tratamiento de datos personales en el cual haya definido sus fines y medios". Vid.* Rubí Puig, A.: "Daños por infracciones", cit. *p. 68. Por el contrario, hay otros autores que hacen referencia a que la responsabilidad es subjetiva, lo que incluye la culpa in vigilando. Vid.* Nieto Garrido, E.: "Derecho a indemnización y responsabilidad", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016, p. 561.

tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado".

No obstante, entiendo que, aunque la normativa europea no haga ninguna previsión al respecto de la responsabilidad civil del encargado subcontratado, podría ser responsables si se cumplen todos los requisitos del sistema general de responsabilidad civil extracontractual previsto en el Código Civil, puesto que el RGPD no deroga el sistema de responsabilidad civil previsto en nuestro ordenamiento jurídico.

C) Pluralidad de sujetos responsables.

En este apartado precisaremos cómo se articula la responsabilidad ante la concurrencia de varios responsables.

El apartado cuarto del art. 82 RGPD y el Considerando 146, señalan que "cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado participan en el mismo tratamiento", cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios.

No obstante, cuando el responsable o encargado del tratamiento haya pagado la totalidad de la indemnización por el perjuicio ocasionado, tendrá derecho a reclamar a los demás responsables la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, es decir, la normativa europea recoge la facultad de repetición de quien abona la indemnización contra los terceros responsables por la parte que les corresponda del daño causado.

En consecuencia, en el supuesto de que participen en la comisión del hecho dañoso varios de los sujetos anteriormente señalados, la responsabilidad será solidaria.

3. Los IPS como sujetos responsables en el tratamiento de datos personales.

En la actualidad, es de todos conocido el impacto que tienen las TICs en cualquier ámbito de la sociedad. La utilización de las nuevas tecnologías ha fomentado no solo la contratación de un modo global, sino nuevas formas de comunicación. Ello plantea el desarrollo de nuevos retos.

Concretamente, en nuestro caso, si las redes sociales respetan la normativa de protección de datos, especialmente en lo referente a los datos sensibles. Para ello, en primer lugar, se tendrá que delimitar la calificación de las redes sociales como prestador de la sociedad de la información, en aldeante ISP, para posteriormente, acotar el régimen jurídico de responsabilidad de éstos.

A) Delimitación del concepto de ISP.

Antes de señalar la posible consideración de sujeto responsable de los prestadores de servicios de la sociedad de la información, se debe delimitar qué se entiende por ISP.

En el art. 2 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, conocida como la Directiva sobre el comercio electrónico (en adelante, DCE) se define al ISP como "cualquier persona física o jurídica que suministre un servicio de la sociedad de la información".

Por tanto, a continuación, se debe limitar el concepto de "servicios de la sociedad de la información". La letra a) del mencionado artículo, en lugar de concretar el concepto de servicios de la sociedad de la información, nos reenvía a las definiciones del apartado 2 del art. 1 de la Directiva 98/34/CE, modificada por Directiva 98/48/CE.

No obstante, en la actualidad, las citadas Directivas han sido derogadas por la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

Concretamente, la letra b) del apartado primero del art. 1 de la citada Directiva, señala que se entenderá como servicio, "todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios"[72].

A continuación, delimita cada uno de los elementos del citado servicio prestado, puesto que debe ser a distancia, es decir, un servicio prestado sin que las partes estén presentes simultáneamente; por vía electrónica o un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético y , por último, a petición individual de un destinatario de servicios, lo que supone que el servicio prestado sea una transmisión de datos a petición individual.

72 Por ejemplo, no cabe duda de que "un servicio en Internet que consiste en facilitar el contacto entre vendedores y compradores de productos tiene, en principio, la consideración de un servicio en el sentido de la Directiva 2000/31". Vid. apartado 109 de la STJUE 12 julio 2011, asunto C-324/09, (TOL2.155.786).

Del análisis comparado de la anterior Directiva y de la vigente, se observa claramente que la Directiva (UE) 2015/1535 ha reproducido literalmente la definición del apartado 2 del art. 1 de la Directiva 98/34/CE, modificada por Directiva 98/48/CE, a la que hace referencia la DCE[73].

En este sentido se pronuncia la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, conocida como Ley de comercio electrónico, en adelante LSSICE.

Concretamente, en su anexo, en la letra a), se especifica que "los servicios de la sociedad de la información comprenden, todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario», pero también comprende «los servicios no remunerados por sus destinatarios en la medida en que constituyan una actividad económica para el prestador de servicios"[74].

En definitiva, se puede afirmar que los servicios de la sociedad de la información cubren una amplia variedad de actividades, desde la compraventa de productos online, pasando por el envío de comunicaciones comerciales, a los que ofrecen herramientas de búsqueda, acceso y recuperación de datos; o simplemente los servicios consistentes en transmitir información a través de una red de comunicación, de acceso a una red de comunicación o alojamiento de información suministrada por el destinatario del servicio[75].

Así mismo, y para dotar de mayor claridad la identificación de los posibles sujetos responsables ante la vulneración de la normativa de protección de datos, conviene distinguir entre los prestadores de servicios, a los intermediarios[76].

Al respecto, la letra b) del mencionado Anexo, define, de manera genérica, al servicio de intermediación, como el "servicio de la sociedad de la información por

73 Respecto a la citada definición debe también señalarse la interpretación realizada por la STJUE 11 septiembre 2014, asunto C-291/13, (TOL4.629.555), en su apartado 30. Concretamente, el Tribunal Europeo señala que "el artículo 2, letra a), de la Directiva 2000/31 debe interpretarse en el sentido de que el concepto de servicios de la sociedad de la información, definido en dicha disposición, incluye los servicios que ofrecen información en línea y por los cuales el prestador del servicio obtiene su remuneración, no del destinatario, sino de los ingresos generados por la publicidad que figura en una página de Internet".

74 Respecto a la no necesidad de que el servicio de la sociedad de la información esté remunerado, véase Andrés Moreno, J.: "Violación de los derechos de autor a través de redes P2P: ¿responsabilidad de los prestadores de servicios de la sociedad de la información o de los miembros de las redes?", *Revista La Propiedad Inmaterial*, núm. 14, 2010, p. 265.

75 Se entiende por "destinatario del servicio", de conformidad con la letra d) del art. 2 DCE, cualquier persona física o jurídica que utilice un servicio de la sociedad de la información por motivos profesionales o de otro tipo y, especialmente, para buscar información o para hacerla accesible y, en virtud del apartado d) anexo de la LSSICE, es aquella persona física o jurídica que utiliza, sea o no por motivos profesionales un servicio de la sociedad de la información.

76 Grimalt Servera, P.: "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en AA.VV.: *El derecho a la imagen desde todos los puntos de vista* (coord. por De Verda y Beamonte, J. R.), Thomson Reuters, Cizur Menor, 2011, p.170.

el que se facilita la prestación o utilización de otros servicios de la información o el acceso a la información"[77].

Así pues, son servicios de intermediación, la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicación, la realización de copia temporal de las páginas de Internet, el alojamiento de datos en los propios servidores o el acceso o recopilación de datos o de enlaces a otros sitios de Internet.

B) Régimen de responsabilidad de los ISP.

Este apartado pretende mencionar la responsabilidad de los prestadores de servicios, especialmente en su condición de intermediarios, por los daños causados por la vulneración de la normativa de protección de datos, atendiendo a la importancia que, en la actualidad, tienen las redes sociales por el volumen de datos que tienen a su alcance.

Al respecto el párrafo 4 del art. 2 RGPD establece que el Reglamento se aplicará sin perjuicio de lo establecido en la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, que ha sido traspuesta en la LSSICE. Concretamente, se deberá acudir a los arts. 12 a 15 de la Directiva y a los arts. 13 a 17 LSSICE que regulan el régimen de responsabilidad de los ISP[78].

En consecuencia, es importante señalar que los ISP serán sujetos de responsabilidad tanto de conformidad con el RGPD ante el incumplimiento de sus obligaciones si sus funciones son acordes a cualquiera de los términos generales de los sujetos intervinientes del RGPD y por los daños y perjuicios causados por

77 Como se observa claramente, la citada descripción sigue la línea previamente establecida por de la Ley Modelo de la CNUDMI sobre Comercio electrónico que señala en la letra e) de su art. 2 que "por «intermediario», en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él".

78 Para un estudio en profundidad de la responsabilidad de los ISP en su condición de intermediarios véase, entre otros, Busto Lago, J. M.: "La responsabilidad civil de los prestadores de servicios de intermediación en la sociedad de la información", *Actualidad Jurídica Aranzadi*, núm. 542, 2002, pp.1-6; Chaparro Matamoros, P.: "La normativa existente en materia de responsabilidad de los prestadores de servicios de la sociedad de la información", en AA.VV.: *Derecho al honor: Tutela constitucional, Responsabilidad Civil y otras cuestiones* (coord. por De Verda y Beamonte, J.R.), Aranzadi, Pamplona, 2015, pp. 243-269; Clemente Meoro, M. E.: "La responsabilidad civil de los prestadores de servicios de la sociedad de la información" en AA.VV.: *Responsabilidad civil y contratos en Internet. Su regulación en la ley de servicios de la sociedad de la información y comercio electrónico* (dir. por Clemente Meoro, M. E. y Cavanillas Mugica, S.), Comares, Granada, 2003, pp. 1-116; Grimalt Servera, P.: "La responsabilidad civil", cit., pp. 167-198; Peguera Poch, M.: "La exención de responsabilidad civil por contenidos ajenos en Internet", en AA.VV.: *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (coord. por Morales Prats, F. y Morales Garcia, O.), Aranzadi, Cizur Menor, 2002, pp. 25-66; Plaza Penadés, J.: "La responsabilidad civil de los intermediarios en Internet y otras redes (su regulación en el Derecho comunitario y en la LSSICE)", en AA.VV.: *Contratación y comercio electrónico* (coord. por Orduña Moreno, F. J.), Tirant Lo Blanch, Valencia, 2002, pp. 195-237 o Plaza Penadés, J,.: "La responsabilidad civil de los intermediarios en internet", en AA.VV.: *Principios de derecho de internet* (coord. por García Mexía, P. L), 2005, pp. 391-426.

su vulneración, como en su labor de prestadores de servicios de la información o intermediarios en virtud de su legislación específica.

De ese modo, se considerarán sujetos responsables de la vulneración de la normativa de protección de datos, cualquier ISP que se pueda calificar como responsable del tratamiento, como redes sociales o motores de búsqueda.

Respecto de los primeros, analizaremos en el siguiente epígrafe la Resolución R/01870/2017 de la AEPD que condenó a Facebook por la vulneración de la normativa de protección de datos por la comisión de diversas infracciones, entre ellas una relativa al tratamiento de daos relativos a la salud.

En relación con los motores de búsqueda, la STJUE de 13 de mayo de 2014, asunto C-131/12, se debe tomar como punto de referencia en la consideración de responsable del tratamiento a los motores de búsqueda[79].

El apartado 33 de la citada sentencia establece que "el gestor del motor de búsqueda es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de ésta y, por consiguiente, debe considerarse responsable de dicho tratamiento en virtud del mencionado artículo".

Además, añade la mencionada sentencia, en los apartados 36 y 37 que la actividad de los motores de búsqueda "desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos".

Por último, en relación con la corresponsabilidad en el tratamiento de los datos, es importante tener en cuenta lo señalado en el apartado 40 de la mencionada sentencia, donde el TJUE afirma que la determinación conjunta de los medios del tratamiento de los editores de sitios de Internet con los motores de búsqueda no elimina, en modo alguno, la responsabilidad del motor de búsqueda, ya que, que la facultad de determinar los fines y los medios del tratamiento de los datos personales puede realizarse sólo o conjuntamente con otros, como ya se establecía en el art. 2, letra d), de la derogada Directiva.

79 El objeto de la STJUE era determinar si se podían considerar responsables de los tratamientos a los motores de búsqueda, concretamente a Google, ya que a actividad de un motor de búsqueda consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente (apartado 41 de la citada STJUE).

C) El caso particular de Facebook.

Tal y como se ha mencionado anteriormente, se debe tener presente que las redes sociales, al igual que cualquier empresa que realiza recopilación de datos personales y crea ficheros con los mismos debe cumplir cada uno de los requisitos de la normativa española y europea de protección de datos.

En relación a si las redes sociales son sujetos responsables ante la vulneración de la normativa de protección de datos, se debe señalar como referencia, aunque fuera dictada conforme a la normativa anterior ya derogada, la Resolución R/01870/2017, derivado del procedimiento sancionador PS/00082/2017, condenó a Facebook Inc. a una multa de 300.000 €, por la infracción del art. 6.1 LOPD, en relación con el art. 5 y el art. 4, apartados 1 y 2 LOPD; a una multa de 600.000 €, por la infracción del art. 7 LOPD, en relación con el art. 5 y el art. 4, apartados 1 y 2 LOPD, y a una multa de 300.000 €, por la infracción del art. 4.5 LOPD, en relación con el art. 16 LOPD, en base a los argumentos que señalo a continuación.

La AEPD, en la citada Resolución, para poder imponer las correspondientes sanciones a Facebook, se pronunció, inicialmente, sobre las alegaciones de Facebook Inc. sobre su falta de responsabilidad en el tratamiento de los datos de los usuarios de Facebook en la Unión Europea, aduciendo que el dominio "facebook.es" está registrado a nombre de Facebook Ireland.

Tras analizar la AEPD si las conductas analizadas en el procedimiento instructor fueron llevadas a cabo por Facebook Inc. en el marco de las actividades de un establecimiento del responsable del tratamiento en territorio español o si se han empleado medios situados en España por parte de Facebook Inc., puesto que si no fuera de ese modo, no se aplicaría la LOPD, en virtud del párrafo primero del art. 2, se centra en las argumentaciones respecto a la comisión o no de las infracciones.

En primer lugar, la AEPD valora si Facebook cumple correctamente con el deber de información a los interesados cuando se recaban sus datos, que se recoge en el art. 5 LOPD[80].

La AEPD comprobó que Facebook no informaba a los usuarios de forma exhaustiva y clara sobre los datos que iba a recoger y los tratamientos que iba a realizar con ellos, sino que se limitaba a dar algunos ejemplos, pero la red

80 En particular, se comprobaba si Facebook cumplía la normativa de protección de datos al recabar el consentimiento de los menores, ya que éstos son los usuarios más habituales y vulnerables de las redes sociales. La Resolución señala que Facebook permite registrarse a menores que hayan cumplido 13 años de edad, pero, de los hechos probados, se corrobora que, ni se habilita ninguna opción para que los padres o tutores presten el consentimiento, ni los menores son informados de que no pueden recabarse datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, entre otros.

social recogía otros datos a través del uso de cookies, algunas de ellas de uso específicamente publicitario e incluso otras de uso declarado secreto, cuando navegan por páginas de terceros y que contienen el botón 'Me gusta'[81].

A continuación, se examina si el consentimiento se recababa de manera inequívoca, es decir, que no admitía lugar a dudas, y que permitía al interesado ejercer un control de sus datos. Con relación a este aspecto, en los hechos probados se establece que Facebook no obligaba a leer las condiciones de la política de privacidad para concluir el proceso de alta en la red social.

Por tanto, la AEPD considera que la información facilitada por Facebook a los usuarios no se ajusta a la normativa de protección de datos, lo cual constituye una infracción tipificada como grave en el art. 44.3.b LOPD.

En segundo lugar, en relación con la infracción del párrafo 5 del art. 4 LOPD que recoge el deber de cancelación, la AEPD consideró que Facebook no cumplía con las obligaciones establecidas por la LOPD y cometía una infracción tipificada como grave en el art. 44.3.c) LOPD, puesto que la AEPD comprobó que cuando un usuario configuraba sus opciones de privacidad para no recibir anuncios, la información recogida por Facebook a partir de sus hábitos de navegación no se eliminaba, sino que se retenía y se reutilizaba posteriormente asociada al mismo usuario, a pesar de haber dejado de ser útiles para el propósito para el que se recogieron[82].

En tercer lugar, en relación con la infracción del art. 7 LOPD, se debe señalar que la AEPD, en base a la investigación realizada, verificó que Facebook recogía datos especialmente sensibles, como ideología, sexo, creencias religiosas o salud.

En particular, respecto a los datos relativos a la salud, objeto de este trabajo, la AEPD comprobó que, en el perfil del usuario, en el grupo de información de "Acontecimientos importantes", existe un subgrupo específico de "Salud y bienestar" que permitía introducir información sobre la superación de una enfermedad o abandono de un hábito.

81 De manera específica la AEPD constató que la política de privacidad de Facebook contenía expresiones genéricas y poco claras y su política de privacidad estaba configurada de manera muy compleja en multitud de capas de forma que un usuario medio de las nuevas tecnologías no llegaba a ser consciente ni de los datos tratados ni de su destino.

82 Al respecto la Resolución señala que se había demostrado, respecto de cuentas que habían sido eliminadas por los propios usuarios y que, por tanto, se solicitaba la cancelación de los datos expresamente, que Facebook, a través de una cookie de la cuenta eliminada, no solo almacenaba la información de la misma, sino que continuaba recogiendo y tratando información durante un periodo de 17 meses. Sobre esta cuestión, la Profª. Vázquez Ruano prestaba atención a la vulneración de la protección de datos en aquellos supuestos en los que, tras la cancelación de un perfil de una red social, la información del citado perfil, aunque desactivado, seguía disponible a través de los motores de búsqueda. Vid. Vázquez Ruano, T., "La tutela de la información personal y el uso de las redes sociales", *Universitas: Revista de filosofía, derecho y política*, núm. 15, 2012, pp. 141-143.

Sobre esos aspectos, los usuarios de la red habían configurado determinados campos de interés como SIDA u obesidad, que permitían al incluir esos valores buscar entre los posibles valores o sugerir algunos valores en base a tipos predefinidos y, por tanto, discriminar la información en base a los mismos.

Además, la AEPD confirmó que los citados datos sensibles eran utilizados, entre otros fines, para diseñar campañas publicitarias que permitían seleccionar público objetivo en función de un perfilado realizado con los mencionados datos sensibles.

La Resolución señaló que, de conformidad con el art. 7 LOPD, la única base legal para tratar los datos especialmente protegidos es el consentimiento, que además ha de ser expreso y por escrito, puesto que no concurren las excepciones previstas en el apartado 2 del citado precepto y de los hechos probados se constató que, en ningún momento, se procedió a la recogida del consentimiento expreso y por escrito de los usuarios, puesto que Facebook, no establecía ningún régimen específico para el tratamiento de datos especialmente protegidos, sino que, por defecto, se tratan todos de la misma manera al pulsar un botón denominado "Terminado".

En definitiva, Facebook cometía una infracción muy grave tipificada en el art. 44.4.b. LOPD.

Además, se debe recordar la corresponsabilidad de Facebook junto con los administradores de las páginas web, tal y como reconoce la STJUE de 29 de julio de 2019.

Concretamente el supuesto de hecho analizado por la mencionada sentencia es que una empresa alemana de comercio electrónico insertó en su página web el botón "me gusta" de Facebook, que implicaba la transmisión de los datos personales del visitante del citado portal a Facebook sin su consentimiento y con independencia de si el citado visitante era miembro de la red social o de si pulsó el citado icono.

Ante esta situación una asociación alemana de defensa de los intereses de los consumidores demanda a la citada compañía y el Juez alemán que conocía el litigio presentó cuestión prejudicial al TJUE.

La STJUE precisa que la empresa alemana puede ser considerada responsable junto con Facebook de las operaciones de recogida y de comunicación de los datos personales, dado que puede considerarse que ambas determinan, conjuntamente, sus medios y sus fines, puesto que dichas operaciones de tratamiento se efectúan en interés económico para ambas, ya que mientras a la empresa alemana la

inserción del botón le permite optimizar la publicidad de sus productos, Facebook obtiene como contraprestación los datos personales de los visitantes de la web de la empresa alemana.

Por todo ello, la STJUE califica a los administradores de páginas web corresponsable de determinadas operaciones de tratamiento de datos de los visitantes de su sitio, como la recogida de datos y su transmisión a tercero, en el caso que nos ocupa concretamente a Facebook, debiendo cada uno de los corresponsables del tratamiento deben cumplir con la normativa de protección de datos.

Por último, para finalizar con la consideración de Facebook como sujeto responsable de la protección de datos, debemos mencionar que, en la actualidad, se ha admitido a trámite la demanda colectiva de responsabilidad civil presentada por la OCU contra Facebook por vulneración de la normativa de protección de datos, donde se solicita una indemnización por el daño moral causado por la cesión de datos personales a Cambridge Analytica, sin tener el consentimiento de los titulares de dichos datos[83].

V. CONCLUSIONES.

La aprobación del RGPD ha supuesto, desde mi punto de vista, un avance de la salvaguarda del derecho fundamental de protección de datos, puesto que el nuevo modelo de protección de datos aprobado por el legislador europeo supone, en primer lugar, cumplir con su finalidad armonizadora dotando de un mismo régimen jurídico de protección de datos a todos los Estados miembros.

En primer lugar, esta nueva regulación nos permite concretar qué datos o informaciones se incluyen en datos tan sensibles como los relativos a la salud, a los biométricos y a los genéticos.

Además, el RGPD unifica las normativas nacionales, ya no únicamente regulando el régimen de infracciones y sanciones, sino estableciendo de manera uniforme la acción de indemnización por daños y perjuicios por la vulneración de la normativa de protección de datos.

En segundo lugar, el RGPD favorece al titular de los datos personales las acciones frente a los sujetos responsables tanto en materia de multas administrativas, como de responsabilidad civil.

83 Téngase en cuenta que el art. 80 RGPD permite a los interesados a ejercitar el derecho a ser indemnizado a través de un mandato a una entidad, organización o asociación sin ánimo de lucro y cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales.

Mientras en el primer caso no solo hay un incremento considerable de la cuantía económica de la sanción administrativa, sino también una ampliación de los sujetos infractores, en el segundo supuesto relativo a la responsabilidad civil por los daños y perjuicios, el RGPD distingue claramente los sujetos, responsables y encargados, y la delimitación de su ámbito de responsabilidad estableciendo que el responsable que participe en la operación de tratamiento responderá de los daños y perjuicios que se cause y el encargado del tratamiento únicamente responderá cuando no haya cumplido las previsiones del RGPD o haya actuado al margen, o en contra, de las instrucciones legales del responsable.

Así mismo, se debe mencionar la importancia del establecimiento de una responsabilidad solidaria en caso de que existan varios sujetos responsables de los daños y perjuicios, por las ventajas que ello conlleva de no tener el perjudicado que delimitar la parcela de responsabilidad de cada uno de ellos, pudiendo demandar a uno de ellos por la totalidad, viéndose resarcido completamente por ello.

Además, el titular de los datos puede ejercitar su derecho al resarcimiento por los daños y perjuicios causados por la vulneración de la normativa de protección de datos, puesto que puede reclamar la misma a través de una entidad, organización o asociación sin ánimo de lucro.

En consecuencia, aunque la tendencia actual es un crecimiento vertiginoso del uso de los datos relativos a la salud por las potenciales utilidades que las nuevas tecnologías nos permiten, con el aumento de los riesgos que ello conlleva, el RGPD mantiene un plus de protección inherente a su categoría de datos especialmente sensibles requiriendo un consentimiento expreso y por escrito.

No obstante, habrá que esperar si se promulga en el ordenamiento jurídico español una normativa específica de condiciones adicionales para el tratamiento de datos genéticos, biométricos o relativos a la salud, que nos lleve a poder afirmar que nos encontramos con una nueva categoría de datos cuya protección esté reforzada estableciendo un marco de garantías capaz de hacer frente eficazmente a todos los desafíos que presenta esta cuestión, logrando un equilibrio entre la protección de la persona, su privacidad y la necesidad del desarrollo tecnológico.

Sin olvidar que, en situaciones excepcionales como la crisis sanitaria actual, donde los datos personales relativos a la salud resultan de interés público, los sujetos responsables deberán ser todavía más precavidos con la utilización de nuestros datos, estableciendo qué datos deben tratarse y por quién, así como la finalidad del tratamiento de los datos de manera clara y específica, para contribuir al seguimiento y la contención de la actual pandemia por parte de las autoridades sanitarias nacionales y europeas, pero velando por el respeto de la normativa de protección de datos.

BIBLIOGRAFÍA

ANDREU MARTÍNEZ, M. B., PARDO LÓPEZ, M. M. y ALARCÓN SEVILLA, V.: "Hacia un nuevo uso de los datos de la salud", *Ius et Scientia*, vol. 3, núm. 1, 2017.

ÁLVAREZ RIGAUDIAS, C.: "Tratamiento de datos de salud" en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por PIÑAR MAÑAS, J. L.), Reus, Madrid, 2016.

AMÉRIGO ALONSO, J.: "Objeto y ámbito de aplicación", en AA.VV.: *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. por RALLO LOMBARTE, A.), Tirant Lo Blanch, Valencia, 2019.

ANDRÉS MORENO, J.: "Violación de los derechos de autor a través de redes P2P: ¿responsabilidad de los prestadores de servicios de la sociedad de la información o de los miembros de las redes?", *Revista La Propiedad Inmaterial,* núm. 14, 2010.

ARIAS POU, M.: "Definiciones a efectos del Reglamento General de Protección de datos", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por PIÑAR MAÑAS, J. L.), Reus, Madrid, 2016.

BUSTO LAGO, J. M.: "La responsabilidad civil de los prestadores de servicios de intermediación en la sociedad de la información", *Actualidad Jurídica Aranzadi,* núm. 542, 2002.

CHAPARRO MATAMOROS, P.: "La normativa existente en materia de responsabilidad de los prestadores de servicios de la sociedad de la información", en AA.VV.: *Derecho al honor: Tutela constitucional, Responsabilidad Civil y otras cuestiones* (coord. por DE VERDA Y BEAMONTE, J. R.), Aranzadi, Pamplona, 2015.

CLEMENTE MEORO, M. E.: "La responsabilidad civil de los prestadores de servicios de la sociedad de la información" en AA.VV.: *Responsabilidad civil y contratos en Internet. Su regulación en la ley de servicios de la sociedad de la información y comercio electrónico,* (dir. por CLEMENTE MEORO, M. E. y CAVANILLAS MUGICA, S.), Comares, Granada, 2003.

COBAS COBIELLA, M. E.: "Protección de los datos personales. Bases de datos. Big data. Un nuevo paradigma" en AA.VV.: *Los derechos fundamentales. Perspectiva entre América y Europa* (coord. por CÁNOVAS GONZÁLEZ D. y VEGA CARDONA R. J.), UniAcademia Leyer, Bogotá, 2019.

CORRAL SASTRE, A.: "El régimen sancionador en materia de protección de datos en el Reglamento general de la Unión Europea", en AA.VV.: *Reglamento General*

de Protección de Datos. Hacia un nuevo modelo europeo de privacidad (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

Cristea Uivaru, L: *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud,* Bosch, Barcelona, 2018.

Dopazo Fraguio, P.: "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos)", *Revista Española de Derecho Europeo,* núm. 68, 2018.

Florencia Cabrera, R., "Historia clínica digital y la protección de datos personales, reflexiones humanísticas", en AA.VV.: *FODERTICS 7.0: estudios sobre derecho digital* (coord. por González Pulido, I.), Comares, Granada, 2019.

García Mexía, P. L.: "La singular naturaleza jurídica del Reglamento General de protección de datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

Gil Antón, A. M.: *¿Privacidad del menor en internet?,* Aranzadi, Pamplona, 2015.

Grimalt Servera, P.: "La responsabilidad civil de los prestadores de servicios de la sociedad de la información", en AA.VV.: *El derecho a la imagen desde todos los puntos de vista* (coord. por De Verda y Beamonte, J. R.), Thomson Reuters, Cizur Menor, 2011.

Jove Villares, D.: "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización", *Revista Derecho y Salud,* núm. 1, 2017.

López Álvarez, L. F.: "La responsabilidad del responsable", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos,* Sepín, Madrid, 2017.

March Cerdá, J. C.: "Redes sociales, salud y pacientes" en AA.VV.: *Medios de comunicación y salud* (coords. por Del Pozo Cruz, J. T., Román San Miguel, A., Alcántara López, R. y Domínguez Lázaro, M. R.), Astigi, Sevilla, 2015.

Martínez Vázquez, F.: "La tramitación parlamentaria de la Ley Orgánica de protección de datos personales y garantías de los derechos digitales", en AA.VV.:, *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de*

diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (coord. por Rallo Lombarte, A.), Tirant Lo Blanch, Valencia, 2019.

Minero Alejandre, G.: "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario jurídico y económico escurialense,* núm. 50, 2017.

Nieto Garrido, E.: "Derecho a indemnización y responsabilidad", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

Pariente De Prada, J. I.: "Los Datos de Salud en el nuevo Reglamento Europeo de Protección de Datos", *I+S: informática y salud,* núm. 122, 2017.

Peguera Poch, M.: "La exención de responsabilidad civil por contenidos ajenos en Internet", en AA.VV.: *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (coord. por Morales Prats, F. y Morales Garcia, O.), Aranzadi, Cizur Menor, 2002.

Pérez Gómez, J. M.: "La protección de los datos de salud" en AA.VV.: *Hacia un nuevo derecho de protección de datos* (coord. por Rallo Lombarte, A. y García Mahamut, R.), Tirant Lo Blanch, Valencia, 2015.

Perez Luño, A.: *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1984.

Plaza Penadés, J.:

- "La responsabilidad civil de los intermediarios en internet", en AA.VV.: *Principios de derecho de internet* (coord. por García Mexía, P. L), 2005.
- "La responsabilidad civil de los intermediarios en Internet y otras redes (su regulación en el Derecho comunitario y en la LSSICE)", en AA.VV.: *Contratación y comercio electrónico,* (coord. por Orduña Moreno, F. J.), Tirant Lo Blanch, Valencia, 2002.

Rallo Lombarte, A.: "España en la vanguardia de la Protección de datos: nuevos retos del Reglamento Europeo", en AA.VV.: *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de datos. Adaptado al Proyecto de Ley Orgánica de Protección de datos de 10 de noviembre de 2017* (coord. por López Calvo, J.), Wolters Kluwer, Madrid, 2018.

Ramón Fernández, F.:

- "Discriminación por condiciones de salud. Protección de datos y consumidores: una reflexión tras la reforma de la Ley General para la

defensa de los consumidores y usuarios", *Revista de Derecho Privado*, núm. 1, 2019.
- "La protección de datos en las aplicaciones móviles de diagnóstico de enfermedades genéticas. Un estudio jurídico", *Revista métodos de información*, vol. 8, núm. 14, 2017.
- "Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?", *Diario La Ley*, núm. 9365, 25 de febrero de 2019.
- "Transparencia y protección de datos especialmente protegidos en genética y la salud desde el punto de vista civil y del buen gobierno", *Diario La Ley*, núm. 9281, 2018.

Ripoll Carulla, S.: "Aplicación territorial del Reglamento", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

Rodríguez Ayuso, J. F.: *Figuras y responsabilidades en el tratamiento de datos personales*, Bosch, Barcelona, 2019.

Romeo Casabona, C. M.: "Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud", *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada,* núm. extra 1, 2019.

Royo V. y Méler, N.: "Multas impuestas por la AEPD en aplicación del RGPD: motivos y cuantías", *Diario La Ley*, 5 de septiembre de 2019.

Rubí Puig, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil,* vol. V, núm. 4 (octubre-diciembre), 2018.

Solar Calvo, P.: "La protección de datos en la UE: recapitulación de novedades", *Revista Aranzadi Unión Europea*, num.1, 2017.

Uriarte Landa, I.: "Ámbito de aplicación material", en AA.VV.: *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (dir. por Piñar Mañas, J. L.), Reus, Madrid, 2016.

Vázquez Ruano, T., "La tutela de la información personal y el uso de las redes sociales", *Universitas: Revista de filosofía, derecho y política*, núm. 15, 2012.

Vázquez De Castro, E.: "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 46, 2018.