ULP Law Review | Revista de Direito da ULP
Vol. 14, n.º 1
doi: 10.46294/ulplr - rdulp.v14i4.7472

La Influencia de las Nuevas Tecnologías en la Protección de Datos Personales en el Marco de la Epidemia Covid-19

Maria Teresa Heredero Campo[1]

Abogada

1. Introducción

En un contexto genérico podemos decir que "datos" se han recabado desde hace mucho tiempo, tal vez, sin que nos percatásemos de la relevancia que acabarían teniendo en este tiempo presente. Pensemos por ejemplo, en los primeros datos que obtiene el Estado a través de los denominados censos de población que datan de la época del imperio romano y se mantienen hasta el siglo XVIII (en España el primer censo es de 1768)[2]. Incluso, cuando hablamos genéricamente de datos, a muchas personas le vienen al pensamiento los libros de la iglesia o libros parroquiales, de los que la institución dispone para apuntar determinados acontecimientos importantes en la vida los creyentes, así encontramos libros de bautismo, de matrimonio y de defunciones, que no han quedado ajenos a los problemas que suscita la petición de cancelación de los datos que en ellos se contienen a requerimiento de la persona que desease eliminarlos. Aún hoy día hay quienes

[1] Abogada y Doctora en Derecho por la Universidad de Salamanca.

[2] En ese año el Conde de Aranda pide a los párrocos que recopilen datos relativos a la población: edad, sexo y estado civil. Sin embargo, el primer recuento, según los estadistas, oficial (es decir, que utilizó técnicas estadísticas modernas) fue el de Floridablanca de 1787, elaborado a partir de cuestionarios enviados a los intendentes de las distintas provincias y demarcaciones del reino a quienes se les requería para fijar cada una de las poblaciones de su zona. Los alcaldes eran responsables de los datos de sus habitantes que recabasen. El listado fue publicado por la Real Imprenta de Madrid en el año reseñado, bajo el título *Censo español ejecutado de Orden del Rey, comunicada por el Excelentísimo Señor Conde de Floridablanca, Primer Secretario de Estado y del Despacho,* y fue modificado y ampliado en 1789.

agotan como último recurso dirigirse a estas vetustas "bases de datos" para intentar encontrar información sobre sus antepasados[3].

Dando un salto en el tiempo, el primer sistema de gestión de bases de datos electrónico lo encontramos 1968[4], época en la que se mejoró la usabilidad de los ordenadores, pero también empezaron a plantearse serios problemas de afectación de derechos. En este sentido MILLER señaló, de forma pionera, el peligro potencial que suponía el uso de estos equipos cara a lesionar derechos tan importantes como la intimidad, el honor o la imagen, entre otros, incluido el conocido hoy en día como derecho a la protección de datos. WESTIN corroboró esta posición advertida por MILLER en 1972, año en el que publicó una monografía en la que alertaba sobre los usos lesivos que podía acarrear el uso de la informática[5]. Y es que desde que aparecieran Internet, los teléfonos inteligentes y las aplicaciones, cada vez más prolíferas, los problemas se han incrementado considerablemente.

Tanto los documentos que se han ido creando en el seno de las instituciones europeas, como discrecionalmente las normativas internas de cada país, son considerados como el verdadero origen del movimiento legislativo en materia de protección de datos, y suponen un giro en la regulación de esta materia creando nuevos derechos no contemplados anteriormente que confieren al titular de los mismos un amplio margen para decidir sobre sus datos personales. Además, estos movimientos fruto de la preocupación por la evolución tecnológica, que se inician en Europa, recogen ya muchos de los principios que aún hoy

[3] Un primer hito en protección de datos lo podemos situar en 1935 cuando el presidente Roosevelt aprueba la *Social Security Act* (Aprobada por el Congreso el 14 de agosto de 1935. Fue la primera ley federal de los EE.UU. que establecía una normativa de una administración pública destinada a sostener un Estado de bienestar), con el fin de tener actualizada la información relativa a los trabajadores, (asistencia sanitaria, pensiones, etc.). Este primer intento sirvió para constatar que los medios técnicos para crear este tipo de herramientas eran escasos y puso en la palestra la necesidad de crear bases de datos organizadas y fáciles de ser actualizadas.

[4] En esos años, concretamente en 1965, L. Roberts y T. Merril, conectaron por primera vez dos ordenadores que se podían transmitir información entre ellos a través de una línea de teléfono, dando origen a ARPANET, que en 1970 ya ponía (además de usos militares) a disposición del usuario correo electrónico y transferencia de datos de ficheros, primero dentro de EE.UU. y posteriormente (a partir de 1973) las conexiones fueron ya de carácter internacional.

[5] A. R. MILLER, "Personal privacy in the computer age: The challenge of a new technology and information oriented society", *Michigan Law Review*, vol. 67, núm. 6 (1969): 1089-1246.
ALLAN F. WESTIN Y MICHAEL A. BAKER, *Data banks in a free society: computers, recordkeeping and privacy* (New York: Quadrangle, 1972).

continúan vigentes en los distintos ordenamientos internos y por supuesto en el marco normativo europeo, tales como: la calidad de los datos (que deben ser exactos y puestos al día, así como adecuados a la finalidad para la que se recogen)[6], la obtención de datos por medios legales, la adopción de medidas de seguridad en los ficheros, los derechos de acceso, cancelación, etc.

La evolución continua, y la Comunidad Económica Europea (CEE), en 1981, tratando de dar respuesta a esta nueva realidad aprueba el *Convenio del Consejo de Europa para la protección de las personas, respecto al tratamiento automático de datos personales* (Convenio 108), piedra angular en la forma de contemplar la materia relativa a protección de datos y que dio lugar posteriormente a recomendaciones sectoriales.

Es importante subrayar el artículo 8 del Convenio por cuanto se refiere no solo al reconocimiento del derecho que tienen los interesados a conocer los datos que les conciernen, sino la posibilidad de que estos sean modificados o incluso cancelados, cuestiones que otras leyes propias de ordenamientos internos ya contemplaban, poniendo de relieve la facultad que tiene a su disposición el titular de derechos de poder acudir a la jurisdicción que corresponda cuando se produzca una transgresión de sus derechos.

Además, algunos de los pronunciamientos del Tribunal Europeo de Derechos Humanos (TEDH) en materia de protección de datos, se han apoyado en los argumentos interpretativos de este artículo del que se pueden extraer una serie de principios que se podrían resumir en los siguientes:

- *Principio finalista*: la creación de un banco de datos siempre debe venir precedida por una razón que justifique la recogida de los mismos.
- *Principio de pertinencia de los datos*: lo que significa que los datos registrados han de guardar relación con el objetivo para el que fue creado el fichero.

[6] La primera norma ISO publicada sobre normas de calidad de datos fue la ISO 8000 de 2011, en ella además de clarificar que los datos de calidad no suponen un lujo sino que deben ser un requisito operativo, normativo y legal, quedó consagrado el estándar internacional de calidad de los datos cuya finalidad principal es la de ser utilizado para especificar la calidad de los datos que se intercambian. Bajo esta misa línea de trabajo la ISO 8000-150 se centra en los principios fundamentales de la gestión de la calidad de los datos maestros; también se ocupa de cuestiones relacionadas con los procesos y requisitos de implementación, de intercambio de datos y de procedencia.

- *Principio de utilización no abusiva*: esto sucede si los datos se usan para un fin distinto del anunciado originariamente.

- *Principio del derecho de olvido*: superada la finalidad para la que fueron recabados, los datos no deben conservarse.

- *Principio de lealtad*: la recopilación de información ha de realizarse por medios lícitos.

- *Principio de exactitud*: siendo el responsable del banco de datos el que debe comprobar la exactitud de los datos facilitados por el titular y siendo igualmente responsable de su actualización[7].

- *Principio de publicidad*: obligación de que exista un registro público de ficheros automatizados.

- *Principio de acceso individual*: todo individuo tiene derecho a conocer, y extensivamente a rectificar si son erróneos o inexactos, los datos que le conciernen y que son objeto de algún tratamiento automatizado. Y en caso de solicitarlo a obtener una copia de los mismos.

- *Principio de seguridad*: las bases de datos deben estar protegidas.

Se asume así mismo el compromiso de establecer un régimen de recursos y sanciones para los que incumplan los principios mencionados, enunciado, aunque no desarrollado, en el artículo 10 del Convenio.

Recuperamos en este punto la *Carta de los Derechos Fundamentales de la Unión Europea,* texto de referencia para la identificación de los contenidos en materia de derechos humanos en la UE. Más concretamente su artículo 8, que contempla la importancia de la protección de datos expresando el derecho que tiene a la misma toda persona en la parte que dichos datos le conciernan. En el segundo apartado del citado artículo, se hace referencia a que los datos han de ser tratados de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo

[7] Como dijeron V. MAYER-SCHÖNBERGER, y CUKIER: *La exactitud requiere datos cuidadosamente seleccionados, no olvidemos que en la era del Big Data, los datos se caracterizan por ser una fuente de innovación y de nuevo valor económico.* V. MAYER-SCHÖNBERGER, Y K. CUKIER, *Big Data, la Revolución de los datos masivos* (Madrid: Turner, 2013), 12.

previsto por la ley. Así mismo, recordándonos los términos contemplados en la Resolución 45/95, reconoce el derecho que toda persona tiene a acceder a los datos que la conciernan y a su rectificación[8]. El legislador remata el precepto en su apartado tercero declarando que el respeto de estas normas quedará sujeto al control de una autoridad independiente.

En la actualidad, la normativa comunitaria de referencia es el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 *relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE. El Reglamento General de Protección de Datos (RGPD)*, tiene como objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar[9].

2. Concepto de dato personal

En España, la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDyGDD), no ofrece una definición del término "dato de carácter personal", por lo que en base a la complementariedad que les caracteriza, si queremos una definición específica debemos acudir a la ofrecida por el legislador en el artículo 4 del RGPD y que es la que sigue:

Toda información sobre una persona física identificada o identificable[10] *(«el interesado»); se considerará persona física identificable toda persona cuya identidad*

[8] Documento accesible a través del siguiente enlace: http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf (último acceso: 21/10/2020).

[9] La corrección de errores del Reglamento fue publicada en el DOUE de 4 de mayo de 2016 y se encuentra accesible a través del siguiente enlace: https://www.boe.es/doue/2018/127/L00003-00007.pdf (último acceso: 21/10/2020).

[10] Mucho se ha escrito sobre identidad e identificación, a este respecto interesa destacar que por *identidad* en nuestro contexto se entiende el conjunto de rasgos o características propias de una persona que la distinguen del resto, p. ej. características relativas a su fisonomía o datos biométricos que hacen que cada individuo sea único. Por *identificación,* entendemos el acto de identificar, es decir, verificar que una persona es quien dice ser, y para ello es factible el uso de distintos mecanismos, algunos apuntados en la propia definición de dato personal cuando se refiere p. ej. al nombre y apellidos, al número de DNI, o a la Tarjeta de Identificación Profesional (TIP).

pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[11]

Lo importante por lo tanto es que el dato vertido permita la identificación del sujeto al que se refiere dicha información[12], es decir, el titular, que como ya ha quedado apuntado va a tener a su disposición ciertas facultades que le van a permitir acceder, rectificar, cancelar u oponerse al tratamiento de dichos datos, debiendo añadir que para que sean cedidos el responsable del fichero deberá recabar su consentimiento.

Dicho término debe ser considerado de forma amplia para que pueda adaptarse a la sociedad actual y por tanto al uso de las nuevas tecnologías. Con ello se pretende que el concepto alcance incluso a la persona cuyo nombre se desconoce, pero cuyo perfil completo se tiene[13], y que por lo tanto puede acabar siendo identificada con toda precisión conforme a dichos datos[14]. La derogada *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD) incluía, al amparo de dicho término, toda información de carácter numérico, alfabético, gráfico, fotográfico, acústico o de cualquier otro tipo. Otro aspecto importante es que los datos no han de ser de carácter privado o íntimo, basta que se refieran a cualquier aspecto de la persona.

[11] Según venía contemplado en el artículo 3 letra a) de la derogada LOPD, por dato de carácter personal se entendía cualquier información concerniente a personas físicas identificadas o identificables. Como ha quedado advertido, la nueva normativa, la LOPDyGDD, no da una definición como tal de dato personal, debiendo tomar en consideración la ofrecida por el RGPD.

[12] En este sentido ARIAS POU, haciendo acopio de la definición dada por el legislador advierte que el concepto de dato personal es bastante amplio dado que en él se incluye *cualquier información concerniente a personas físicas identificadas o identificables*. MARÍA ARIAS POU, "Definiciones a efectos del Reglamento General de Protección de Datos," en *Reglamento General de Protección de Datos*, dir. JOSÉ PIÑAR MAÑAS (Madrid: Reus, 2016), 117 y ss.

[13] El disponer de un dato tan aparentemente insignificante como el correo electrónico de una persona puede permitir el llegar a conocer su identidad de forma precisa, pues aunque no sea una dirección elaborada a partir de datos propios como el nombre o apellidos, que suele ser algo común en la práctica, podemos llegar de forma exacta e inequívoca de quién se trata a través de su dirección IP, por este motivo, actualmente se considera dentro de la identificación de dato de carácter personal la IP o los datos de localización.

[14] J. A. MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación de datos de carácter personal* (Madrid: Civitas, 2003): Cap. I, 27 y ss.

En consecuencia, la *Agencia Española de Protección de Datos* (AEPD) propone a este respecto, haciendo una interesante puntualización, que no sea necesario que el dato identifique directamente a la persona, sino que sirva para su identificación junto con otros elementos (identificabilidad) a la hora de considerar el concepto de dato personal[15].

2.1 ¿Qué se entiende por dato sensible?

Tal como se desprende del Considerando 15 del RGPD, *especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.*

Desde el punto de vista material y de forma muy resumida, se entiende por *datos sensibles* aquéllos que más directamente se refieren sea a la esfera personal e íntima que merecen una especial protección.

Lo que en realidad desvela tal concepción es una categoría de datos que necesita ser protegida de manera especial, datos especialmente protegidos, que podemos encontrar en diferentes fuentes. Este tipo de datos se revelan cuando se trata información relativa a: *ideología, afiliación sindical, creencia, religión, origen racial, salud, vida sexual y los relativos a infracciones tanto penales como administrativas*[16].

---

[15]Agencia Española de Protección de Datos (AEPD), http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/aepd_dpa_es.pdf (último acceso: 21/10/2020).

[16] El tratamiento de ficheros que contengan datos de este tipo debe estar dotado de un sistema de seguridad de nivel alto. Para entender a qué nos referimos hemos de saber que el tratamiento de ficheros de datos debe contemplar ciertas medidas de seguridad en función de los datos que se contengan en ellos. Así pues, encontramos tres niveles de seguridad, siendo estos acumulativos (nivel básico, nivel medio y nivel alto) según la naturaleza de la información tratada y almacenada en los mismos, atendiendo a la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información almacenada.
El primero de los niveles es el *Nivel Básico de seguridad* de los ficheros: se aplicará entre otros, a ficheros que traten datos identificativos y como ya hemos advertido al ser acumulativos se aplicarán a todos los ficheros que les corresponda el nivel medio y alto de seguridad (p. ej.: nombre, domicilio, teléfono, DNI, número de afiliación a la seguridad social, correos electrónicos, datos bancarios, edad, fecha de nacimiento, sexo, nacionalidad, etc.); El *Nivel Medio de seguridad*: se aplicará a ficheros que contengan datos de solvencia patrimonial, operaciones financieras y de crédito (p.ej.: datos relativos a hábitos de consumo, datos de seguridad social, solvencia patrimonial y crédito, antecedentes penales, sanciones administrativas, pruebas psicotécnicas, currículums, etc.); Por último el *Nivel Alto de seguridad*: se aplica a ficheros que contienen datos especialmente protegidos (p.ej.: ideología, afiliación sindical y política, religión y creencias, origen racial, salud, alimentación, bajas laborales, vida y práctica sexual, etc.).

La preocupación por la protección de los datos sensibles ya había quedado advertida por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en sus Directrices de 1980, concretamente por el grupo de expertos *ad hoc* sobre las barreras a los Datos Transfronterizos y la Protección de la Privacidad que trabajaban cooperando con el Consejo de Europa y la Comunidad Europea. Sobre este tema se debatió si debía existir un conjunto de datos que fueran reconocidos a nivel universal como sensibles, pero no fueron inicialmente capaces de determinar qué datos podían quedar incluidos en este conjunto dejando de forma residual simplemente una mención en la segunda parte sobre principios básicos de aplicación nacional en el apartado 7 por cuanto se refería a la limitación de la recogida de datos, en el que de forma genérica se indicaba que debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos. Así mismo, en el Memorándum Explicativo[17], en los apartados 19, 50 y 51, se detallan las siguientes cuestiones: en primer lugar, surgió la duda de si las Directrices debían ser generales o estructurarse en función de los distintos tipos de datos, admitiendo que posiblemente no fuera viable identificar una serie de datos que se considerasen sensibles universalmente. El apartado 50, basándose en los principios contemplados en los apartados de 7 a 14, haciendo hincapié en la forma de recabar datos, de tratarlos (es decir, cómo se van a procesar), su naturaleza, contexto… en definitiva fija ciertos límites en la fase de recopilación de los datos y los requisitos relativos a los métodos de recogida de datos. En este punto se habla de la posibilidad de enumerar los tipos de categorías de datos que son sensibles por sí mismos y cuya recogida debería restringirse o incluso prohibirse (p. ej. datos sobre la raza, creencia religiosa, antecedentes penales, etc.). Apunta que ningún dato es por sí mismo "privado" o "sensible" pero puede llegar a serlo por su contexto y uso. Por último el 51 alude a la discusión mantenida por el Grupo de Expertos sobre una serie de criterios de sensibilidad tales como el riesgo de discriminación, pero no le fue posible definir ningún conjunto de datos que pudieran verse universalmente

[17] Organización para la Cooperación y el Desarrollo Económico, *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales,* 23 de septiembre de 1980, disponible en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (último acceso: 21/10/2020).

como sensibles lo que trae como consecuencia que el apartado 7 afirme de forma general que deberían ponerse límites a la recogida de datos personales dejando en manos de los legisladores los criterios limitativos de cara a evitar la recogida indiscriminada de este tipo de datos. Entendemos que, pese a no indicar nada concluyente al respecto, los límites se refieren a los principios que se vienen manejando en el campo de la protección de datos siendo p. ej. la calidad de los datos o la finalidad, a la que se refiere cuando habla de destinar los datos especialmente sensibles según las tradiciones y actitudes existentes en cada país.

El artículo 7 de la derogada LOPD disponía de una lista cerrada en la que se incluían todas las categorías aludidas. Como es lógico pensar, cada una de ellas disponía a su vez de un grado de protección diferente. Hay quienes dentro de la misma, hacían diferenciación entre datos sensibles, supersensibles y sensibilísimos[18], pero lo habitual es referirse a los grados de protección como datos sensibles de primera y de segunda categoría.

En todo caso lo que sí parecía claro es que eran datos que tenían una trascendencia directa sobre el derecho a la intimidad siendo éste el factor que determinaba la necesidad o no de la especial protección.

La característica principal es que para tratar estos datos era necesario recabar el consentimiento del titular de los datos[19], debiendo prestarse éste de forma expresa y por

[18] Entre ellos, TONIATTI quien haciendo alusión a los datos "supersensibles" o "sensibilísimos" se refiere a aquellos datos en los que el ordenamiento jurídico, en su regulación, llega al extremo de privar al interesado del acceso directo a los mismos y limita su actuación respecto a los típicos instrumentos de control dirigidos al ejercicio del derecho de acceso, rectificación, cancelación, olvido, etc. Este autor concluye que este tipo de datos personales, clasificables desde el punto de vista material como ordinarios o sensibles, se presentan principalmente en archivos que tienen finalidades tales como la protección del orden público y la seguridad nacional, aunque también tienen cabida aquellos datos que afectan a la esfera íntima en materia sanitaria. R. TONIATTI, "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", *RVAD Revista Vasca de Administración pública,* Núm. 29 (1991): 139. Accesible en versión digital a través del siguiente enlace:
https://dialnet.unirioja.es/servlet/articulo?codigo=85373 (último acceso: 21/10/2020).

[19] En el artículo 6 de la LOPD hace referencia en su apartado primero a que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que legalmente se disponga otra cosa.

escrito tal como marcaba el apartado 2 del artículo 7 de la citada Ley[20].

El resto de apartados del artículo 7 establecían una serie de elementos a tener en cuenta:

En el apartado 3 de la hoy derogada LOPD, el legislador ponía de manifiesto que los datos de carácter personal que hicieran referencia al *origen racial, a la salud y a la vida sexual* pudiendo ser recabados, tratados y cedidos sólo cuando, por razones de interés general, así lo dispusiera una ley o el afectado consintiera expresamente. Quedaban prohibidos (tal como establecía el apartado 4) los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelasen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. Y por último en el apartado 5 hacía referencia a que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podían ser incluidos en ficheros de las Administraciones públicas competentes según marcasen las normas reguladoras respectivas[21].

Con respecto a los datos sensibles, en materia de protección de datos en la UE, la Comunicación del Consejo de 4 de noviembre de 2010, relativa al *enfoque global de la protección de los datos personales en la Unión Europea*[22], se planteó entre sus objetivos,

[20] A efectos de dejar constancia el tipo de consentimiento y de datos contemplados, reproducimos a continuación el tenor literal del artículo 7.2 de la derogada LOPD que decía: "Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado."

[21] El legislador se reservó el punto 6 del citado artículo 7 de la LOPD para establecer dos salvedades. La primera excepción permite que los datos que quedaban relacionados en los apartados anteriores pudieran ser objeto de tratamiento si era necesario para prevenir o para diagnósticos médicos, así como para la prestación de asistencia sanitaria o tratamiento, o para la gestión de servicios sanitarios, debiendo realizarse por profesionales sanitarios y manteniendo el deber de secreto profesional o de realizarse por otra persona que esta estuviera sujeta a una obligación de secreto equivalente. En segundo lugar, contempla que también pueden ser tratados los datos sensibles si fuera necesario de cara a salvaguardar el interés vital del afectado o de un tercero, en el supuesto de que el afectado estuviera física o jurídicamente incapacitado para prestar válidamente su consentimiento.

[22] Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones,* COM (2010) 609 final. Bruselas: 4.11.2010, https://eur-

la protección de los datos sensibles (*los que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad*), sin embargo, la constante evolución tecnológica hace necesario revisar las disposiciones existentes relativas a los datos sensibles, con el fin de determinar si es conveniente someter otras categorías de datos a esta normativa y precisar aún más las condiciones aplicables a su tratamiento[23].

Se abre aquí el campo de los *datos genéticos,* que pese a que inicialmente no se mencionan expresamente como una categoría de datos sensibles la ley ahora los contempla en el artículo 4 del RGPD definiéndolos como aquellos datos personales, obtenidos a partir del análisis de una muestra biológica, relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre esa persona en relación con su fisiología o su salud.

No es el único tipo de datos de los que nos habla el citado artículo del RGPD pues también se refiere a los *datos biométricos,* bajo cuya categoría se encuentran los datos personales que se obtienen a partir de un tratamiento técnico específico (p. ej.: imágenes faciales o datos dactiloscópicos -huellas dactilares-, otometrías, rasgos grafológicos, etc.), y que proporcionan información relativa a las características físicas, fisiológicas o conductuales de una persona permitiendo que se confirme la identificación única de dicha persona. Se suma la última categoría de datos señalados por el legislador en el apartado décimo quinto del Reglamento dedicado a los datos de salud, pudiendo ser datos relativos a la salud física o mental de una persona física. Una cuestión relevante a efectos del presente artículo, es que se incluyen datos sobre la prestación de servicios de atención sanitaria que revelen información sobre el estado de salud.

También podríamos hacer alusión a los *datos relativos a la filiación política*; en este tipo de información se pueden incluir las opiniones políticas de los ciudadanos, de los que mucho se ha hablado en los últimos tiempos a colación del recurso que presentó el 5 de marzo de 2019 (recurso de inconstitucionalidad núm. 1405/2019), el Defensor del Pueblo

lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0609&from=ES (último acceso: 21/10/2020).

[23] La Comisión considera necesario precisar aún más y armonizar las condiciones que deben cumplirse para realizar el tratamiento de determinadas categorías de datos sensibles.

contra el artículo de la *Ley de Régimen Electoral General* (LOREG) que permitía la recopilación de datos personales por parte de los partidos políticos en el marco de sus actividades electorales concernientes precisamente en las opiniones políticas que las personas hubieran publicado en redes sociales[24]. A este respecto el TC concluye en la STC 76/2019, de 22 de mayo[25], que procede declarar inconstitucional el artículo 58 bis 1 de la LOREG, introducido por la LOPDyGDD[26].

El artículo 2 de la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 sobre la privacidad y las comunicaciones electrónicas,* habla por ejemplo de *datos de tráfico* entendiendo por tales según viene expresado en la norma: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma.

También, en la misma norma, encontramos la categoría de *datos de localización* que son los datos tratados en una red de comunicaciones electrónicas que indiquen la posición

[24] El artículo anulado decía en su tenor literal que la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

[25] ECLI:ES:TC:2019:76; publicada en el BOE núm. 151, de 25 de junio de 2019.

[26] Concretamente el punto dos de la disposición final tercera indica que se añade un nuevo artículo 58 bis sobre utilización de medios tecnológicos y datos personales en las actividades electorales, concretando que la recopilación de datos personales relativos a las opiniones políticas de las personas que efectúen los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas. Y permite, tal como viene recogido en el apartado segundo, que los partidos políticos, coaliciones y agrupaciones electorales puedan utilizar datos personales que obtengan en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral. Puntualiza que el envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrá la consideración de actividad o comunicación comercial. Añade que las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. Y por último, en esta nueva configuración advierte que se deberá facilitar al destinatario un modo sencillo y gratuito en el que pueda ejercer su derecho de oposición. Noticias accesibles también a través de los siguientes enlaces: "El TC estudiará la constitucionalidad de la norma que permite a los partidos recoger opiniones políticas en Internet", *La Vanguardia,* 12/03/2019, https://www.lavanguardia.com/vida/20190312/461005029521/el-tc-estudiara-la-constitucionalidad-de-la-norma-que-permite-a-los-partidos-recoger-opiniones-politicas-en-internet.html (último acceso: 21/10/2020). "Los partidos políticos no podrán recopilar datos de las opiniones políticas de los ciudadanos", *Iberley,* 23/05/2019, https://www.iberley.es/noticias/partidos-politicos-no-recopilar-datos-opiniones-politicas-ciudadanos-29599 (último acceso: 21/10/2020).

geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público[27].

Agrupando a modo de resumen final las categorías de datos considerados "sensibles", según lo contemplado en el articulado (artículos 9, 13, 14 y 15) y los Considerandos del RGPD (51 a 56), se consideran dentro de esta clasificación:

- Datos personales relacionados con el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas
- Datos relacionados con la vida sexual o la orientación sexual de la persona
- Datos sobre la filiación sindical
- Datos genéticos
- Datos biométricos
- Datos relacionados con la salud

En la LOPDyGDD, los datos sensibles son tratados como "categorías especiales de datos". Concretamente en el Título II, sobre *Principios de protección de datos,* y más específicamente en el artículo 9, se recogen, previa remisión expresa al artículo 9.2.a) del RGPD, los que se consideran entran dentro de esta tipología, datos sobre: ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Importante es igualmente prestar atención al *consentimiento del interesado,* al que hemos otorgado un lugar preferente, pues determina en muchos casos las decisiones que jueces y tribunales adoptan en sus pronunciamientos. Sin perjuicio del epígrafe que sigue, a efectos del tratamiento de los datos, por consentimiento se entiende toda manifestación de voluntad prestada de forma libre, específica, informada e inequívoca, por medio de la cual el interesado acepta que dicho tratamiento (de los datos que le conciernen) se lleve a cabo.

[27] Ambos tratados en los artículos 6 y 9 respectivamente de la citada Directiva.

3. El consentimiento y su importancia en la protección de datos

La *protección de datos* es un campo donde la prestación de consentimiento cobra especial importancia. La Directiva 95/46/CE, decía que este podía prestarse mediante cualquier medio apropiado que permitiese la manifestación libre, inequívoca y fundada de la voluntad del usuario, p. ej. mediante la selección de una casilla de un sitio web en Internet. Un ejemplo que ponemos a propósito de los quebraderos de cabeza que ocasiona a más de un usuario de forma frecuente: cabía entender que el consentimiento era prestado igualmente si no se desmarcaba una casilla premarcada. Es decir, el carácter inequívoco no era contrario a los consentimientos tácitos.

Según se desprende del Considerando 31 de la Directiva 2002/58/CE, el consentimiento que se ha de obtener para el tratamiento de datos personales a efectos de proporcionar un particular servicio con valor añadido debe ser el del abonado o el del usuario, en función de los datos a tratar y el tipo de servicio que se suministre y de que sea posible desde el punto de vista técnico, de procedimiento y del contrato distinguir la persona que utiliza un servicio de comunicaciones electrónicas de la persona física o jurídica que ha suscrito el mismo; el artículo 2, encargado de las definiciones, se remite de inicio a lo estipulado en la Directiva 95/46/CE y en la *Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas,* y por cuanto respecta a la definición de consentimiento hace remisión expresa a la primera de las citadas, entendiéndose equivalente el concepto de consentimiento de un usuario o abonado al dado para el consentimiento del interesado: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Según el artículo 3.2 de la *Carta de los Derechos Fundamentales de la Unión Europea* al hablar de derecho a la integridad de la persona y refiriéndose el legislador en este caso al ámbito de la medicina y la biología, contempla que debe ser particularmente respetado el consentimiento que en todo caso será libre e informado. Así mismo en el artículo 8.2 relativo a protección de datos dice que los datos se tratarán sobre la base del

consentimiento de la persona afectada (o en defecto, en virtud de otro fundamento legítimo previsto por la ley) siguiendo los principios de lealtad y concreción.

El tema del consentimiento supone una de las novedades, en el tratamiento, en el RGPD en el que primeramente encontramos su definición en el artículo 4 donde el undécimo apartado indica que por "consentimiento del interesado" debemos entender *toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa* (lo que viene a ser inequívoca), *el tratamiento de datos personales que le conciernen*. Esta declaración ha de reunir una serie de requisitos ente los que se encuentran el ser inteligible, de fácil acceso y que se utilice un lenguaje claro y sencillo.

El que se exija una acción positiva implica que por el contrario, en el tratamiento de datos de carácter personal, no se permite la vía del consentimiento tácito, lo que supone una novedad que se deduce claramente ya en el Considerando 32 donde se nos advierte que además de que se debe prestar mediante un *acto afirmativo* claro que refleje una manifestación de voluntad, como una declaración por escrito o por medios electrónicos o incluso verbal (siempre y cuando se cumplan los requisitos que acabamos de mencionar: que sea libre, específica, informada, e inequívoca). Por ejemplo: marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Teniendo en cuenta lo dicho, se entiende y así consta en dicho Considerando, que no deben constituir consentimiento el silencio, las casillas ya marcadas o la inacción del usuario[28].

En el Título II de la LOPDyGDD (además de recoger otros aspectos relativos al deber de confidencialidad, al tratamiento de datos, las categorías especiales de datos, el tratamiento de datos de naturaleza penal), se indican cuestiones importantes sobre el consentimiento, el cual ha de proceder de una declaración o de una clara acción afirmativa del afectado. Se

[28] El artículo 6 de la LOPDyGDD sobre tratamiento basado en el consentimiento del afectado, ya pone de manifiesto, de conformidad con lo dispuesto en el artículo 4 apartado 11 del RGPD que por consentimiento del afectado se entiende toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

excluye así el "consentimiento tácito", es decir, no cabe la posibilidad de que se pueda interpretar como afirmativo el silencio o la inacción del interesado, ha de ser por tanto explicito excluyendo cualquier forma implícita de la que quepa deducirse. Se indica, en la línea de lo argumentado anteriormente, que el consentimiento que ha de prestar el afectado debe ser preciso, es decir, que conste de manera específica e inequívoca, y con respecto a los menores, el legislador ha decidido mantener el límite de catorce años como edad a partir de la cual el menor puede prestar su consentimiento.

Con respecto a la prestación del consentimiento en menores, no es un tema que escape al debate, máxime si tenemos en cuenta que cada menor se desarrolla en un entorno que le condiciona, y esto en la práctica puede suponer un problema sobre el que únicamente el juez tiene facultad moderadora. Sin embargo, la ley se muestra tajante, al margen de consideraciones subjetivas o de índole social y estemos o no de acuerdo. Así las cosas, el RGPD determina que la edad mínima a partir de la cual los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (que es el mayormente utilizado, p. ej. con el uso de las redes sociales)[29], serán los 16 años. Lo que no significa que menores de 16 años no puedan tener perfiles sociales, sino que, por debajo de esta edad, sería imprescindible contar con el consentimiento de padres o tutores. Sin embargo, cabe hacer una puntualización a esta consideración: el propio legislador permite que en determinados

[29] A pesar de que la mayoría de los casos con los que a menudo nos topamos se relacionan con el uso de redes sociales, no escapa tampoco a esta problemática el tratamiento de datos relativos a historias clínicas, así p. ej. la SAN de 6 de abril de 2018 (rec. núm. 372 / 2016; Roj: SAN 1574/2018) en la que el recurrente, médico de cabecera y esposo de la demandante hasta aproximadamente finales de 2012, accedió en repetidas ocasiones a la historia clínica de la denunciante, cuando ya no era su médico y sin su consentimiento, desde enero de 2013 hasta abril de 2014. Los hechos que se enjuiciaban traían causa de una Resolución de la AEPD de 24 de febrero de 2016 (PS/01001/2015), que confirmaba en reposición la resolución de 3 de noviembre de 2015, que impuso una sanción de 2.500 euros por una infracción de los artículos 6.1 (en el que se enuncia que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa) y artículo 4.2 de la LOPD (sobre la finalidad de la recogida). La sanción se deriva del artículo 44.3.b) de la LOPD donde se establecía como grave el que se tratasen los datos personales sin haber recabado el consentimiento de la persona afectada (aludiendo igualmente al artículo 3 h) y al 6 de la citada Ley).
En esta misma línea sobre tratamiento de datos sin contar con el consentimiento de quien ha de prestarlo encontramos la SAN de 20 de septiembre de 2006 (rec. núm. 626/2004; Roj: SAN 3938/2006) y la SAN de 17 de noviembre de 2014 (rec. núm. 124/2013; Roj: SAN 4655/2014).

casos se rebaje esa edad y que cada Estado miembro pueda establecer la que considere oportuna siempre que no sea inferior al límite mínimo fijado en 13 años.

En nuestro caso, España, ese límite se sitúa en 14 años (artículo 7 de la LOPDyGDD)[30]. Un límite que ya había sido previsto, y que se mantiene, por a AEPD, que ya en el año 2000 (en su informe 2000-000)[31] llegó a la conclusión de que para poder recabar datos concernientes a menores, era necesario que estos recibieran, de forma expresa, toda la información sobre la totalidad de los extremos que contenía el artículo 5.1 de la LOPD sobre el derecho de información, exigiendo el consentimiento de los representantes legales en los casos de menores de 14 años cuyas condiciones de madurez no garantizasen la plena comprensión por sí mismos del alcance del consentimiento prestado[32].

Por último, cabe hacer una breve mención al hecho de que si el consentimiento es uno de los pilares fundamentales sobre los que se configura el derecho fundamental a la protección de datos personales, su retirada o la revocación del mismo debe ocupar un lugar igualmente destacado por cuanto interesa conocer de dicha posibilidad al interesado. En este sentido, queda reconocido a nivel legal que el interesado puede retirar el consentimiento previamente prestado en cualquier momento, independientemente que el tratamiento de datos que se esté realizando sea lícito. La novedad que presenta la

[30] Mantiene el criterio determinado por el RLOPD en cuyo artículo 13 se recogía la posibilidad de tratar los datos de mayores de 14 años, estableciendo como excepción los casos en los que se exija la asistencia de los titulares de la patria potestad o la tutela del menor. Especificaba también en el primer apartado que en caso de que fueran menores de 14 años se requeriría el consentimiento de padres o tutores. Y añadía en los siguientes apartados que ningún caso podría recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, características del mismo, datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos u otros, sin el consentimiento de los titulares de tales datos (con la salvedad de los datos de identidad y dirección del padre, madre o tutor con la finalidad de recabar la reseñada autorización). También se echa de menos en la redacción actual la referencia que se hacía en el apartado tercero respecto al lenguaje, este debía ser fácilmente comprensible para los menores a quienes iba dirigida la información. Por último destacaba que correspondería al responsable del fichero o tratamiento articular los procedimientos que garantizasen la comprobación de la edad del menor y la autenticidad del consentimiento prestado por los padres, tutores o representantes legales.

[31] Agencia Española de Protección de Datos (AEPD). "Informe 2000-000". https://www.aepd.es/es/informes-y-resoluciones/informes-juridicos?search_api_fulltext=2000%20consentimiento&f%5B0%5D=conceptos_resoluciones%3A2193&f%5B1%5D=informes_historicos%3A0(último acceso: 21/10/2020).

[32] En el uso de las redes sociales, cada una de ellas fija la edad de uso en la que estima conveniente, 13 años p. ej. en *Facebook*, *Twitter*, *Instagram* y *Snapchat* y 16 años en *WhatsApp*. Sobre menores y redes sociales vid. LAURA DAVARA FERNÁNDEZ DE MARCOS, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go* (Madrid: Agencia Española de Protección de Datos, 2017).

normativa más actual es que propugna que su retirada sea igual de fácil que su prestación[33]. Algo que *a priori* puede que parezca que es de sentido común, pero que sin embargo en la práctica acarrea algunos problemas. Basta ver la sanción de 50 millones de euros que la Comisión Nacional de la Informática y las Libertades (CNIL) ha impuesto a *Google* al contravenir los principios de transparencia, información y consentimiento (sobre el que ha dicho que el usuario no está suficientemente informado)[34] contemplados en el RGPD[35].

4. Bases legitimadoras del tratamiento de datos

Por último y como aventurábamos desde el principio, cabe hablar de las "bases legitimadoras" como criterios o requisitos que hacen lícito un tratamiento de datos, el cual, ha de hacerse conforme a unos principios. Esto, inevitablemente nos traslada como momento inicial al Convenio 108 en el que el Capítulo II se ocupa de los principios básicos para la protección de datos, recogiendo entre otros los de calidad, seguridad, derechos de acceso, rectificación y cancelación… También podríamos aludir al Considerando 40 del RGPD donde queda advertido que para *que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho [...]*, en este sentido el Reglamento sigue el camino previamente marcado por la ya derogada Directiva 95/46/CE, y mantiene las mismas bases jurídicas que se contenían en esta[36].

Las bases que legitiman el tratamiento son necesarias para que se considere lícito o legítimo el tratamiento, por ello es imprescindible que al menos se cumpla una de las siguientes condiciones:

---

[33] Artículo 7.3 del RGPD.

[34] La autoridad francesa también advierte que el consentimiento no es específico pues el método que se emplea para entender prestado el consentimiento se realiza en "bloque" es decir, el usuario acepta en una misma acción todos los fines que persigue *Google*, personalización de publicidad, ubicación, reconocimiento de voz, etc.

[35] "Francia multa con 50 millones a Google por infringir las normas de protección de datos," *La Vanguardia,* 22/01/2019, https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html (último acceso: 21/10/2020).

[36] Mientras que en la Directiva quedaban recogidas en el artículo 7, en el RGPD o hace en el artículo 6.

- Que el interesado haya prestado su consentimiento para uno o varios fines específicos: es una de las seis fórmulas propuestas por el RGPD que implica que para que se puedan procesar datos personales de cualquier individuo residente en la UE hay que recabar su consentimiento (un consentimiento, cuya importancia ya ha quedado puesta de manifiesto, que se ha de prestar conforme a las exigencias establecidas en el Reglamento -libre, específico, informado e inequívoco-, con especial atención a los datos de salud o menores en los que se hará imprescindible el contar con el consentimiento explícito).

- Que sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación a petición de este de medidas precontractuales. El tratamiento se justifica en el mantenimiento o cumplimiento de dicho contrato. Pensemos p. ej. en una Tarjeta de Identificación Profesional (TIP) para la que se necesitan determinados datos del trabajador, incluso en ocasiones una fotografía.

- Que sea necesario para el cumplimiento de una obligación legal aplicable al responsable, en este caso el interés legítimo lo tiene el responsable y se respetará en tanto no prevalezcan los derechos y libertades del interesado[37].

[37] A este respecto conviene destacar el tenor literal del Considerando 47 del RGPD en el que se dice que *el interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.*

Esto se traduce en que podrá tratar los datos que conciernan al interesado sin tener su consentimiento si demuestra tener un interés legítimo. Algo que en la práctica puede generar dudas y problemas en dos sentidos: el primero de ellos sobre la posición en la que queda el interesado en caso de que no esté de acuerdo, a cuyo respecto la respuesta es fácil: este tendrá a su disposición el ejercicio del derecho de oposición; el segundo se refiere a la posibilidad que tenemos de caer en un exceso de tratamientos que se justifiquen so pretexto de "interés legítimo", por eso se dice que es la base legitimadora con mayor indeterminación pues ante la falta de poder alegar otra, esta puede ser utilizada como cajón de sastre. Para evitar que se produzcan situaciones arbitrarias la ley pone algunos ejemplos que cabrían dentro de esta condición legitimadora del tratamiento:

- Cuando se trate de prevenir el fraude (Considerando 47).
- Transmisiones de datos personales dentro de un grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados (contemplado en el Considerando 48).
- Transmisiones de datos personales en la medida estrictamente necesaria y proporcionada, que tengan como fin garantizar la seguridad de la red y de la información (Considerando 49)[38].
- Que sea necesario para proteger intereses vitales del interesado o de otras personas. En este sentido los considerandos vuelven a tomar protagonismo y concretamente el 46, establece como ejemplos vitales y de interés público los relativos al tratamiento necesario para fines humanitarios, y precisamente pone como ejemplo el control de epidemias y su propagación y otras situaciones que se puedan considerar de emergencia humanitaria ya sean catástrofes naturales o de origen humano.

El título IV de la LOPDyGDD recoge disposiciones aplicables a tratamientos concretos donde se reúnen diferentes supuestos que constituyen claros ejemplos de tratamientos lícitos donde el "interés legítimo", y también en su caso el "interés público", están

[38] Otra excepción que legitima el tratamiento por parte del responsable es el uso de las *cámaras onboard* (normalmente las vemos instaladas en vehículos o en cascos de ciclistas y motoristas), su uso, cada vez más extendido, tiene por finalidad obtener imágenes en caso de accidente para servir de prueba en el arreglo de controversias.

presentes. Así p. ej., el legislador presume lícito el tratamiento de datos de contacto de empresarios individuales y profesionales liberales, siempre que los datos recabados sean los estrictamente necesarios para su localización profesional o con la finalidad de mantener el contacto entre el cliente y el profesional que preste el servicio (artículo 19); también considera lícito, en relación con los sistemas de información crediticia, el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando los datos hayan sido facilitados por el acreedor y lo sean en base a deudas ciertas, vencidas y exigibles, además el deudor deberá haber sido previamente informado (p. ej. en el contrato, si lo hay) sobre la posibilidad de ser incluido en dichos sistemas, en los que como máximo permanecerá durante 5 años desde que venciera la deuda y siempre que se mantenga el incumplimiento (artículo 20); otro ejemplo es el tratamiento que se realiza con fines de videovigilancia (artículo 22), debiendo tener presentes las condiciones y límites bajo los que se tiene que realizar (que el tratamiento se haga con el fin de preservar la seguridad de las personas, bienes e instalaciones; que sólo se capten imágenes de la vía pública cuando sea estrictamente imprescindible; que los datos sean suprimidos en el plazo máximo de un mes -salvo que se tengan que poner a disposición de la autoridad competente-; etc.); será igualmente lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas (artículo 23, relativo a los sistemas de exclusión publicitaria); resultarán también lícitos los tratamientos relacionados con la realización de determinadas operaciones mercantiles (artículo 21); los sistemas de información de denuncias internas (artículo 24; el tratamiento de datos en el ámbito de la función estadística pública (artículo 25); el tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas (artículo 26) y el tratamiento de datos relativos a infracciones y sanciones administrativas (artículo 27).

Un ejemplo muy actual, puede ser precisamente el relativo al tratamiento de datos en APP relacionados con el COVID. Cuando acceden a los datos de personas a través de sus terminales para identificar posibles focos de infección y tener así información para tratar de identificar y aislar y otras más enfocadas al autodiagnóstico en función de la sintomatología. En este sentido cada país actúa de una forma diferente conforme a la

normativa que le es de aplicación, así p. ej. encontramos diferencias entre oriente y occidente. En China el uso de estas aplicaciones es obligatorio para los ciudadanos, en Corea del Sur[39], han hecho un amplio uso de estas aplicaciones[40], mientras que los países europeos, donde la protección de datos está contemplada como un derecho fundamental, se han visto fuertemente condicionados por las restricciones establecidas en las normas que contemplan aspectos de la privacidad[41].

La AEPD, consciente de la proliferación de este tipo de aplicaciones y webs que ofrecen servicios relacionados con el COVID, ha advertido de los riesgos que implica facilitar datos como los que solicitan estas herramientas, considerados datos sensibles, al tratarse de información sobre la salud de los usuarios. En muchas ocasiones estos servicios adolecen de carencias en la información que facilitan al usuario y otros tratamientos ilícitos que se están llevando a cabo como p. ej. no recabar el consentimiento o incluir la geolocalización[42]. Por su parte el RGPD establece en su Considerando 46 que *el tratamiento de datos personales debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física* y a mayor abundamiento comenta que *ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como*

[39] *Self-quarantine safety protection* es la APP utilizada en Corea del Sur para paliar y prevenir los efectos de la pandemia. Recopila datos sobre el estado de salud del usuario, su ubicación y los lugares que ha visitado gracias a la información que facilita el GPS de su teléfono.

[40] A mayor abundamiento, vid. CLÁUDIO R. FLORES, "Sobre o uso de tecnologías e de IA em tempos de emergência, à luz dos direitos fundamentais e da ética: privacidade vs vida", en *COVID 19 e o Direito*, eds. Inês F. Godinho y Miguel O. de Castro (Lisboa: Edições Universitárias Lusófonas, 2020), 147-163, https://recil.grupolusofona.pt/bitstream/10437/10302/1/COVID%2019%20E%20DIREITO.pdf (último acceso: 22/11/2020).

[41] La Comunidad de Madrid ideó una APP (*CoronaMadrid*) precisamente persiguiendo estos fines y actuando en sí misma como responsable del tratamiento de los datos. En su política vemos reflejada, entre otros muchos aspectos, la finalidad del tratamiento identificada con fines estrictamente de interés público ante la situación de emergencia sanitaria decretada por las Autoridades Públicas como consecuencia de la pandemia del COVID-19 y la necesidad de controlarla lo antes posible, manteniendo siempre presente la protección y salvaguarda de la vida de las personas.

[42] El Gabinete Jurídico de la AEPD ha emitido un informe (N/REF: 0017/2020) en relación con los tratamientos de datos resultantes de la situación derivada de la extensión del virus COVID-19 donde advierte que el RGPD contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones como la presente, en que existe una emergencia sanitaria de alcance general. Documento accesible a través del siguiente enlace: https://www.aepd.es/es/documento/2020-0017.pdf (último acceso: 21/10/2020).

por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano. Y a efectos de reforzar la posición que defiende el uso de estas aplicaciones, tenemos la *Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública,* modificada recientemente mediante *Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública,* o la *Ley 33/2011, de 4 de octubre, General de Salud Pública.* Ya en la normativa de los años 80 el legislador tuvo a bien contemplar que con el fin de poder controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, puede adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible.

- Que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. En este sentido se permite que cada Estado introduzca las disposiciones que considere necesarias, así por ejemplo se pueden recoger determinados datos de los profesores que trabajan con menores, de los que se suele recabar la información necesaria para comprobar que no tienen antecedentes por delitos sexuales con menores.

- Que sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales, es decir, en base al cumplimiento de determinadas obligaciones legales no será necesario que se recabe el consentimiento del interesado si lo que se está haciendo es cumplir una obligación legal, por ejemplo, los periodos de conservación de los datos.

Siempre que el tratamiento esté justificado al menos en una de las seis bases legitimadoras anteriormente referidas, estará autorizado el tratamiento de datos, salvo que la autoridad competente determine lo contrario.

5. Conclusiones

Como apuntábamos inicialmente el legislador va legislando conforme las exigencias del momento, por eso, y a fin de tratar de dar la mejor solución a las controversias existentes busca adaptar las herramientas legales con las que contamos al contexto del COVID-19.

Debemos ser conscientes de la importancia que merece el derecho a la protección de datos, un derecho fundamental reconocido como individual y autónomo, a pesar de que no siempre fue así. Además, es a la luz de la situación presente, un derecho revalorizado, pero que al igual que sucede con otros como la intimidad, el honor o la imagen, cuando un supuesto exige una ponderación de los derechos puestos en liza, en algunos casos ha de ceder en pro de salvaguardar otros derechos más importantes como es la protección de la vida de las personas.

En conclusión, el interés general prevalece sobre la privacidad individual. En este sentido, como ya hemos tenido ocasión de apuntar, el propio RGPD (y más concretamente el Considerando 46) justifica como lícito el tratamiento de datos personales cuando sea necesario para proteger un interés esencial y responda a motivos de interés público poniendo como ejemplo el control de epidemias y su propagación, situaciones que trasladan a un segundo lugar la primacía del derecho a la protección de datos haciendo prevalecer la protección de la salud de las personas y el interés general.

Bibliografia

"Coronavirus y protección de datos cuando el interés publico se impone a la privacidad." *Heraldo.es,* 28/07/2020. https://www.heraldo.es/noticias/aragon/2020/07/28/coronavirus-y-proteccion-de-datos-cuando-el-interes-publico-se-impone-a-la-privacidad-1388168.html (último acceso: 21/10/2020).

"El derecho a la intimidad de los niños afectados por la covid-19 en los colegios".*El País,* 30/09/2020. https://elpais.com/mamas-papas/2020-09-30/el-derecho-a-la-intimidad-de-los-ninos-afectados-por-la-covid-19-en-los-colegios.html (último acceso: 21/10/2020).

"El gran debate de la privacidad en tiempos del coronavirus: qué está en juego realmente al dar nuestros datos para combatir la pandemia." *Xataka.com,* 02/04/2020. https://www.xataka.com/privacidad/gran-debate-privacidad-tiempos-coronavirus-que-esta-juego-realmente-al-dar-nuestros-datos-para-combatir-pandemia (último acceso: 21/10/2020).

"El TC estudiará la constitucionalidad de la norma que permite a los partidos recoger opiniones políticas en Internet". *La Vanguardia,* 12/03/2019. https://www.lavanguardia.com/vida/20190312/461005029521/el-tc-estudiara-la-constitucionalidad-de-la-norma-que-permite-a-los-partidos-recoger-opiniones-politicas-en-internet.html (21/10/2020).

"Francia multa con 50 millones a Google por infringir las normas de protección de datos." *La Vanguardia,* 22/01/2019. https://www.lavanguardia.com/tecnologia/20190121/454234917044/francia-multa-google-50-millones-infringir-proteccion-datos.html (último acceso: 21/10/2020).

"Los partidos políticos no podrán recopilar datos de las opiniones políticas de los ciudadanos". *Iberley,* 23/05/2019. https://www.iberley.es/noticias/partidos-politicos-no-recopilar-datos-opiniones-politicas-ciudadanos-29599 (último acceso: 21/10/2020).

"Radar Covid, la 'polémica' app que protege tus datos." *Big Data magazine,* 15/09/2020. https://bigdatamagazine.es/radar-covid-la-polemica-app-que-protege-tus-datos (último acceso: 21/10/2020).

Agencia Española de Protección de Datos (AEPD). "Informe 2000-000". https://www.aepd.es/es/informes-y-resoluciones/informes-juridicos?search_api_fulltext=2000%20consentimiento&f%5B0%5D=conceptos_resoluciones%3A2193&f%5B1%5D=informes_historicos%3A0(último acceso: 21/10/2020).

(AEPD). "Documento N/REF: 0017/2020". https://www.aepd.es/es/documento/2020-0017.pdf (último acceso: 21/10/2020).

(AEPD). http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/aepd_dpa_es.pdf (último acceso: 21/10/2020).

ARIAS POU, M. "Definiciones a efectos del Reglamento General de Protección de Datos" en *Reglamento General de Protección de Datos,* dirección de JOSÉ PIÑAR MAÑAS, 117 y ss. Madrid: Reus, 2016.

Comisión Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones,* COM (2010) 609 final. Bruselas: 4.11.2010. https://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52010DC0609&from=ES (último acceso: 21/10/2020).

DAVARA FERNÁNDEZ DE MARCOS, L. *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos Breve referencia al fenómeno Pokémon Go.* Madrid: Agencia Española de Protección de Datos, 2017.

FLORES, CLÁUDIO R. "Sobre o uso de tecnologías e de IA em tempos de emergência, à luz dos direitos fundamentais e da ética: privacidade vs vida". En *COVID 19 e o Direito,* editado por Inês F. Godinho y Miguel O. de Castro, 147-163. Lisboa: Edições Universitárias Lusófonas, 2020. https://recil.grupolusofona.pt/bitstream/10437/10302/1/COVID%2019%20E%20DIREITO.pdf

MAYER-SCHÖNBERGER, V. Y CUKIER, K. *Big Data, la Revolución de los datos masivos.* Madrid: Turner, 2013.

MESSÍA DE LA CERDA BALLESTEROS, J. A. *La cesión o comunicación de datos de carácter personal.* Madrid: Civitas, 2003.

MILLER, A.R. "Personal privacy in the computer age: The challenge of a new technology and information oriented society." *Michigan Law Review,* vol. 67, núm. 6 (1969): 1089 a 1246.

Organización para la Cooperación y el Desarrollo Económico. *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales,* 23 de septiembre de 1980. Disponible en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (último acceso: 21/10/2020).

TONIATTI, R. "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada." *RVAD Revista Vasca de Administración pública,* Núm. 29 (1991): 139.

WESTIN, A.F. Y BAKER M.A. *Data banks in a free society: computers, recordkeeping and privacy.* New York: Quadrangle, 1972.