EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA SANITARIO. UN ANÁLISIS TRAS EL NUEVO REGLAMENTO EUROPEO Y LOS ÚLTIMOS PRONUNCIAMIENTOS JURISPRUDENCIALES

Faustino Gudin Rodríguez-Magariños
Profesor Asociado UAH.
Doctor en Derecho/ Licenciado en Criminología.
Magistrado/ Letrado de la Administración de Justicia excedente

RESUMEN

Paso a paso, el Big Data se está metamorfoseando en el mítico Big Brother. Intuitivamente, se siente como la tecnología está progresando más rápido que la ley. En el ámbito sanitario, el alto riesgo de que la información médica sea compartida o publicada aumenta a la misma velocidad que el desarrollo tecnológico. Debemos construir un nuevo sistema legal para salvaguardar la privacidad de los pacientes. Del mismo modo, la irrupción del denominado internet de las cosas comporta nuevos retos que exceden de la mera anomización de datos pasando a la seudonimización. Las partes interesadas en hacer prevalecer un sistema jurídico pleno de garantías en la UE están tratando de implementar un espacio de libertades donde nadie pueda llegar a conocer su enfermedad o sus problemas de salud. La calidad de nuestro futuro depende de preservar estas barreras de salvaguarda del anonimato, porque la información médica no es un asunto público, y el Estado y las grandes empresas no deben controlar indiscriminadamente este tipo de información.

PALABRAS CLAVE

Big Data, información sensible, anomizacion, seudonimización e intimidad.

ABSTRACT

Step by step, Big Data is becoming Big Brother. Intuitively, it feels like technology is progressing faster than the law. The high risk that medical information is shared or published is increasing at the same speed as the technological development. We must build a new legal system in order to safeguard the privacy of the patients. Likewise, IoT involves a more difficult problem than processing of such anonymous information, furthermore the new goal would be application of pseudonymisation to personal data. The stakeholders in the legal system of UE are trying to implement a space of liberties where nobody could know their illness or their health problems. The quality of our future depends on preserving our anonymity, because the medical information is not a public business, and State and the big companies must not monitored indiscriminately this type of information in any case.

KEYWORDS

Big Data, sensitive information, IoT, sensitive information, pseudonymisation, anonymisation and privacy.

1. INTRODUCCIÓN

El arcaico concepto de intimidad decimonónico no sirve ya para hacer frente a los diferentes frentes tecnológicos que invaden nuestro derecho a hacer vida anónima en el seno de la sociedad de la información[1]. Ello ha dado lugar al nacimiento de un nuevo derecho fundamental denominado «derecho a la autodeterminación informativa» que encuentra su origen el término acuñado por el Tribunal Constitucional alemán en una célebre sentencia de 15 de diciembre de 1983 acerca de la Ley del Censo[2]. Mas a juicio de Denninger la "autodeterminación informativa no sólo depende de los datos sino también de su elaboración"[3].

Dentro de la autodeterminación informativa los datos sanitarios deben encuadrarse dentro de un núcleo duro que demanda una especial protección[4]. Adentrándonos en la cuestión, la protección de datos no es un ente aislado sino que procura impermeabilizar una esfera del individuo para que no se le ataque en otras esferas. Sin embargo, su protección cobra su auténtico sentido en la medida en que la protección de los datos personales se halla estrechamente unida a la privacidad y puede desempeñar un papel sustancial en el ejercicio de otros derechos como la libertad de expresión, o las libertades de religión y conciencia, (comprometiendo igualmente en ciertos casos la esfera patrimonial) el Consejo de Europa adoptó en 1981 el Convenio 108 del Consejo de Europa[5] para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

2. *BIG DATA* VERSUS *BIG BROTHER*

Junto a los innegables beneficios de la red, nunca los *arcana imperii de* los Estados y los grandes oligopolios han tenido más resortes y el ciudadano de a pie (*netcitizen*) ha estado expuesto a una situación más vulnerable que con la llegada de internet y la digitalización universal de la información.

En 1999, John Mashey publicó un emblemático artículo titulado "Big Data and the Next Wave of Infrastress"[6] (*Big Data* y la próxima ola de estresadas infraestructuras), donde hacía referencia al estrés que iban a sufrir las infraestructuras físicas y humanas de la informática debido al imparable tsunami de datos que ya se oteaba en el horizonte, inmanejable con los instrumentos de gestión al uso[7]. Tanto el *Big*

1 Vid. RUIZ MIGUEL, Carlos, "La nueva frontera del derecho intimidad", *Revista de Derecho y Genoma humano, Núm. 14,* 2001, pp.147-149,

2 El Tribunal alemán configuró con base al derecho general a la personalidad garantizado en la Constitución alemana (antigua Ley Fundamental de Bonn) un derecho concerniente a "la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de que límites procede revelar situaciones referentes a la vida privada".

3 Vid. DENNIGER, Erhard, "El derecho de autodeterminación informativa" en PÉREZ LUÑO, Antonio Enrique, *Problemas actuales de la Documentación y la Informática Jurídica*, Tecnos, Madrid, 1987, p.127.

4 Conforme al parágrafo 51 del Reglamento, 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. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose por la norma que el uso del término «origen racial» usado en el Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas.

5 El Convenio fue ampliado a través de un Protocolo en el año 2001 y está abierto a la adhesión de estados no miembro del Consejo de Europa.

6 Vid. MASHEY, John, "Big Data and the Next Wave of Infrastress: Problems, Solutions and opportunities", *Usenix Annual Technical Conference*, 6-11 Monterry California, junio de 1999.

7 Vid. ZIKOPOLOUS, Paul/ DEROOS, Dirk/ DEUTSCH, Tom/ LAPIS George, *Understanding Big Data:*

Data el fenómeno del internet de las cosas, el *cloud computing* son tecnologías disruptivas, que están revolucionando la forma en la que funciona nuestro mundo[8]. Actualmente hay más información a nuestro alrededor de lo que ha habido nunca en la historia[9]. El impacto del *Big Data* en la Sociedad de la información ha sido tras extraordinario que ha trastocado por completo el viejo concepto de privacidad convirtiéndolo en una especie de entelequia o un producto del pasado[10].

A mediados del siglo pasado, Orwell, conmovió al mundo con su novela 1984 que recogía, de un modo taimado, la arcaica idea la idea egipcia de Horus "el ojo que todo lo ve", que se pasó a ser el Gran Hermano que "todo lo ve" augurando la posibilidad de un sistema político totalitario donde cualquier mínimo gesto, movimiento o pensamiento del individuo pasase a estar controlado[11]. Por eso en la teología judeocristiana existe una tautología o pleonasmo: "dios es omnisciente porque es omnipotente"[12]. Poder y conocimiento son dos caras de la misma moneda, realmente Foucault[13] afirma que la relación entre conocimiento y poder es simplemente lingüística no existe una diferencia real.

Fue Jeremy Bentham el primero en percatarse que para controlar a los seres humanos la manera más inteligente era edificar un artilugio el Panopticon[14]. Dicho edificio permitía controlar los comportamientos humanos en base a la sencilla idea de que privando a las personas de tener un marco de intimidad, se les privaba la posibilidad de ser libres. Según Deleuze[15], la fórmula abstracta del Panoptismo no es tan sólo "ver sin ser visto" excede el "ojo que todo lo ve"[16], sino también comporta un "imponer una conducta cualquiera a una multiplicidad humana cualquiera". El Panoptismo hace que nos comportemos de forma "socialmente aceptable" por miedo, y no por una decisión individual derivada de una reflexión. Miedo a que alguien, en alguna parte, nos esté vigilando y nos castigue por torcernos del camino marcado.

La pirámide de Maslow, o jerarquía de las necesidades humanas[17] es una teoría propuesta por Abraham Maslow en un intento de explicar las motivaciones de a conducta humana. La salud las necesidades fisiológicas y evitar el dolor se encuentran en la primera línea de necesidad. Tras las necesidades fisiológicas del cuerpo se sitúa la necesidad de seguridad, al estar en la base de nuestras necesidades la inseguridad traducida en miedo se erige en uno de los elementos más asequibles para poder manipular a los individuos[18]. Como estrategia de poder, el panoptismo tiende a manipular la enfermedad y la sensación de inseguridad en orden a controlar sus conductas y

Analytics for Enterprise Class Hadoop and Streaming Data, McGraw-Hill, Nueva York, 2012, pp. 43 y ss.

8 Hoy, recién iniciado el siglo XXI, se generan, según la Unión Europea, 1.700 nuevos billones de bytes por minuto. Por ende, el *Big Data* implica recoger, almacenar y tratar grandes cantidades de datos y metadatos, en lugar de estudiar una muestra, como hace la estadística tradicional. El Boston Consulting Group ha estimado que se produce un crecimiento de 2,5 exabytes de información al día (sabiendo que un exabyte son 1.000.000.000.000.000.000 bytes). De hecho, son cantidades tan grandes que, para los no expertos, dejan de tener sentido y añadir más o menos ceros a la cifra ni siquiera nos permite ver la diferencia (Vid. CUKIER, Kenneth Neil / MAYER-SCHÖENBERGER.,Viktor, «The Rise of Big data. How It's Changing the Way We Think About the World», *Foreign Affairs, Vol. 92, Num. 3*, 2013, pp.20-32.

9 A nivel ilustrativo, podemos señalar que desde el inicio de la historia hasta 2003 los humanos habíamos creado 5 exabytes (es decir, 5 mil millones de gigabytes) de información. En 2011 ya creábamos esa misma cantidad de información cada dos días y en 2014 con los datos aportados por internet de las cosas, el volumen ingente de información crece de modo exponencial. [Vid. PUYOL, Javier, «Una aproximación al *Big Data*», *Revista de Derecho de la Universidad Nacional de Educación a Distancia*, (UNED), Núm. 14, 2014, pp. 471-505].

10 Vid. MONLEÓN-GETINO, Antonio, "El impacto del *Big-data* en la Sociedad de la Información. Significado y utilidad", *Historia y Comunicación Social. Vol 20, Núm. 2,* 2015, pp. 427-445.

11 Vid. WILSON, Hilary *Understanding Hieroglyphs: A Complete Introductory Guide,* Michael O'mara Books Ltd*, Londres,* 1965, p. 165.

12 "Los ojos de Jehová están en todo lugar, mirando a los malos y a los buenos" (Libro de los Proverbios 15: 3).

13 Vid. FOUCAULT, Michel, *Microfísica del poder*, Ediciones de La Piqueta, Madrid*,* 1979, pp. 177. El planteamiento de Foucault es tomado de Francis Bacon quien es el primero en defender la equiparación real entre ambos términos.

14 Vid, BENTHAM, Jeremy, *El Panóptico*, La Piqueta, Madrid, 1979.

15 Vid. DELEUZE, Gilles, *Différence et répétition*, PUF, Paris, 1997, pp. 1-2.

16 Vid. FOUCAULT, Michel, "El Ojo que todo lo ve", *Panoptico*, La Piqueta; Madrid, 1979, p. 9. También en FOUCAULT, Michel,· *Microfísica del poder* 1ª ed, e La Piqueta, Madrid, 1978.

17 Para MASLOW la naturaleza más elevada del hombre descansa en su naturaleza inferior: necesita dicha parte como base, pues sin ella no podría sostenerse. Esto significa que, para la masa humana, la naturaleza más alta del hombre es inconcebible sin una naturaleza inferior satisfecha que haga las veces de base. (Vid. MASLOW, Abraham, *Toward a psychology of being*, 2ª. Ed., Van Nostrand, Nueva York, 1968, p. 173).

18 La integración de la persona se verifica junto con la integración de su mundo. Cuando esa persona se siente bien, todo en el mundo parece estar bien. (Vid. MASLOW, Abraham, *The farther reaches of human nature*, Viking Press, Nueva York, 1971, p. 165).

hacer más controlable al alienado individuo frente al Poder omnisciente[19].

Al igual que su precedente el gran Hermano, el *Big Data* telemático se muestra como un ente omnisciente, los datos masivos acaparados a gran escala, que alcanzan a datos al mapa del genoma humano, datos penales, fiscales, tributarios, mercantiles, comunicaciones, etc. No es descartable que este poder acabe en manos o sea utilizado por un potencial tirano. Dado que toda información pude ser digitalizada y todo ciudadano puede ser supervisado hasta extremos intolerables.

El *Big Data* ha crecido exponencialmente derivado del crecimiento de los dispositivos electrónicos digitalizados que generan el denominado internet de las cosas (*IoT, Internet of Things*) que sinuosamente aporta una casi incalculable masa ingente de datos de los usuarios des tos dispositivos, supone un nuevo reto a la privacidad del individuo.

3. MARCO NORMATIVO

3.1 Derecho de la Unión Europea

En primer lugar el art.8.1 de la Carta Europea de los Derechos fundamentales[20] postula que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan que debe ser entendida en relación al precedente art.7 que vela por persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

En base a la misma, el parágrafo 35 del Reglamento Europeo de Protección de Datos[21] de 2016 da una definición de datos sanitarios englobando como tales los relativos a la salud y configurándolos como "datos sensibles" o de especial protección[22]. La norma explica que entre ellos se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro[23]. Dicho concepto se complementa a nivel interno con el art. 5.1.g del Real Decreto 1720/2007 de 21 de diciembre que los define como «datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética».

Anteriormente, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950, (en lo sucesivo CEDH) consagra el derecho al respeto de la vida privada y familiar: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia». Posteriormente, el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin «garantizar [...] a cualquier persona física [...] el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona».

Como consecuencia de la antigua estructura de pilares, actualmente están en vigor diferentes instrumentos legislativos, entre los que figuran

19 Los peligros del panoptismo, han sido convenientemente escenificados por la literatura distópica. En este sentido cabe citar múltiples y casi innumerables obras: la arquitectura de cristal de Zamiatin (en su novela Nosotros escrita en 1921), Aldous Huxley y mundo feliz (1932), George Orwel y su mundo bajo cámaras de televisión en 1984 (1948), Burhus Fiedrich Skinner en Walden 2 (1948), Ray Bradbury en 451º Farenheit (1953), etc.

20 Carta de los Derechos Fundamentales de la Unión Europea. DOUE núm. 326, de 26 de octubre de 2012, pp. 391 a 412.

21 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, DOCE de 4 de mayo de 2016, L119/1-88. [http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf]. (Último acceso 29/6/2017).

22 Se entienden como tales los datos sanitarios, biométricos, genéticos, raciales e ideológicos. Por lo tanto, sólo podrán ser recogidos, tratados y cedidos por razones de interés público, cuando lo establezca expresamente una ley o con el consentimiento previo y manifiesto del interesado.

23 La norma continua diciendo que "se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); 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".

instrumentos pertenecientes al antiguo primer pilar, como la Directiva 95/46/CE relativa a la protección de datos, la Directiva 2002/58/CE (modificada en 2009) sobre la privacidad y las comunicaciones electrónicas, la Directiva 2006/24/CE sobre la conservación de datos (declarada inválida por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 al constituir una injerencia de especial gravedad en la vida privada y la protección de datos) y el Reglamento (CE) nº 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios, así como instrumentos pertenecientes al antiguo tercer pilar, como la Decisión Marco del Consejo, de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Un intento de armonizar las legislaciones y de intentar forjar un ámbito sanitario europeo lo hallamos en Directiva 2011/24/UE del Parlamento europeo y del Consejo de 9 de marzo de 2011[24] relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza

Sin perjuicio de que su adecuado análisis posterior en el final de este artículo, cabe ya anticipar la importancia Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) que constituyó durante mucho el eje vertebrador de esta materia.

Correlativo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

3.2 Derecho interno español

En base al art.18.4 de la Constitución (en lo sucesivo CE) y el aludido Convenio 108, relativo a la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, el Tribunal Constitucional español (en lo sucesivo TC) llega a la afirmación, efectuada en las Sentencias de 292 y 290, ambas de 30 de noviembre de 2000, del derecho fundamental a la protección de datos personales en relación al art 43 CE que reconoce el derecho a la protección de la salud.

De otro lado, la protección de los datos sanitarios alcanzan una nueva dimensión cuando se conectan al respeto a la confidencialidad médico-paciente, la cual cuenta con una gran raigambre en el marco del orbe sanitario, del mismo puede decirse que la importancia de la confidencialidad se torna esencial cuando se piensa en el contexto de la relación 'profesional de la salud – paciente' puesto que es la confianza en el primero, como portador de un saber que puede ayudar a restaurar la salud o a devolver el bienestar, la que posibilita la apertura de la intimidad. La norma de confidencialidad en la relación aludida tiene una larga tradición, ya el Juramento Hipocrático enuncia la obligación del médico, de salvaguardar lo que el paciente le confía"[25].

Una norma troncal en esta materia es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (en lo sucesivo LOPD) en cuyo art.7.3 reputa los datos relativos a la salud como datos especialmente protegidos[26]. En su art.8 prescribe que las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Quizás la aportación más importante de esta última norma sea que introduce en su art.6 el consentimiento informado un concepto soberano en esta materia. Se trata de una técnica jurídica acuñada por el Juez de la Corte Suprema norteamericana Benjamin Cardozo en su celebérrima *Schloendorff v. Society*

24 Diario Oficial de la Unión Europea (en lo sucesivo DOCE) de 4 de abril de 2011.

25 En concreto, cabe citar el párrafo del Juramento hipocrático que dice: "Lo que en el tratamiento, o incluso fuera de él, viere u oyere en relación con la vida de los hombres, aquello que jamás deba divulgarse, lo callaré teniéndolo por secreto".

26 El Reglamente ejecutivo de desarollo en su artículo 5.1.g define los datos de carácter personal relacionados con la salud como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

of New York Hospital 1914[27] cuando trabajaba en la Corte de Apelación neoyorkina. En esta sentencia para justificar el consentimiento informado hace un razonamiento que con el paso del tiempo puede decirse que acabaría siendo acogido con carácter universal:

> "*Todo ser humano de edad adulta y sano juicio tiene el derecho de determinar lo que debe hacerse con su propio cuerpo, y un cirujano que realiza una intervención sin el consentimiento de su paciente comete una agresión por la que se le pueden reclamar legalmente daños. Esto es verdad, excepto en casos de emergencia, cuando el paciente está inconsciente y cuando es necesario operar antes de que sea obtenido su consentimiento*".

Paralelamente, el artículo 3.h) de la referida Ley Orgánica 15/1999 define el consentimiento como tal "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". Los datos relativos a la salud conforme al art.7.2 de la aludida norma demandan la necesidad de consentimiento expreso y escrito, con la excepción prevista en el art.11. f) de la propia norma, o sea, cuando sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. Finalmente, el tratamiento de datos sin consentimiento previo del afectado en aquellos supuestos no exceptuados legalmente, puede ser motivo de infracción grave de acuerdo con lo dispuesto en el artículo 44.3.b) de la Ley Orgánica 15/1999.

Seguidamente cabe destacar, la ley 41/2002, de 14 de noviembre de 2002, sobre la autonomía del paciente y los derechos y obligaciones relativos a la información y al expediente médico (artículo 16 § 3). El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de carácter personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso.

A su vez, el art.7.1 de la Ley 41/2002 prescribe que "toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley". A su vez, el art. 2.7 de esta norma indica que «la persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida». Finalmente, el art. 19 de la Ley de autonomía del paciente indica que éste «tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas[28]. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el art. 16 de la presente Ley».

Al igual que ya lo hiciera la LOPD, el consentimiento informado reconocido en el artículo 3 de la 41/2002 aborda la conformidad libre, voluntaria y consciente de un paciente, manifestada en el libre uso de sus facultades después de recibir la información adecuada para que tenga lugar una actuación que afecta a la salud y entre la misma se encuentra al divulgación de sus datos sanitarios.

Por su parte, la Ley General de Sanidad (Ley 14/1986, de 25 de abril)[29], en relación con los derechos de los pacientes, en el artículo 10.1 reconoce el "respeto a la personalidad, dignidad humana e intimidad" cuyo apartado 3º del mismo establece el derecho "a la confidencialidad de toda la información relacionada con el proceso y con su estancia en instituciones sanitarias públicas y privadas". De otro lado, el secreto profesional viene contemplado en el artículo 24.2, párrafo segundo, de la Constitución dispone: "la ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos"[30].

27 Sentencia de la Corte de Apelación de Nueva York *Schloendorff v. Society of New York Hospital*, de 14 de abril de 2014, 105 N.E. 92, 211 N.Y. 125. El caso versaba sobre una demanda que interpuso la señora Mary E. Schloendorff contra el Hospital de la Ciudad de Nueva York por haberle practicado una cirugía no autorizada por ella. El juez Cardozo falló a favor de la paciente, aduciendo que ella contaba con todas las facultades mentales para decidir qué procedimientos se podían hacer sobre su cuerpo.

28 La Historia Clínica se halla íntimamente unida a los datos sanitarios, la misma es definida por virtud del artículo 8.5 de la Carta de Derechos y Deberes de los pacientes del Defensor del Paciente de la Comunidad de Madrid reconoce el derecho a la información sobre la propia salud incluye el acceso a la información existente en la historia clínica,». (http://www.juansiso.es/Almacen/CARTA%20DE%20DERECHOS%20Y%20DEBERES%20DE%20LOS%20PACIENTES%20-%20DEFENSOR%20DEL%20PACIENTE%20DE%20MADRID.pdf, último acceso 31 de mayo de 2017).

29 Parcialmente derogada por la Ley 25/1999 del Medicamento.

30 Sobre la potestad de los Colegios Profesionales de ordenar la profesión y regular las normas sobre el secreto profesional, el artículo 5,i) de la Ley estatal de Colegios Profesionales, les otorga la siguiente función: "Ordenar en

El acceso a la historia clínica obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Por su parte, el art. 19. i) de la Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud configura el deber al respeto a la dignidad e intimidad personal de los usuarios de los servicios de salud, su libre disposición en las decisiones que le conciernen y el resto de los derechos que les reconocen las disposiciones aplicables, así como a no realizar discriminación alguna por motivos de nacimiento, raza, sexo, religión, opinión o cualquier otra circunstancia personal o social, incluyendo la condición en virtud de la cual los usuarios de los centros e instituciones sanitarias accedan a los mismos. Por su parte el apartado j) del mismo artículo enuncia el deber de mantener la debida reserva y confidencialidad de la información y documentación relativa a los centros sanitarios y a los usuarios obtenida, o a la que tenga acceso, en el ejercicio de sus funciones

Por su parte se reputa falta muy grave el art. 72 c) de la Ley 55/2003 la conducta consistente en el quebranto de la debida reserva respecto a datos relativos al centro o institución o a la intimidad personal de los usuarios y a la información relacionada con su proceso y estancia en las instituciones o centros sanitarios.

De otro lado, el art. de la Ley 62/2003, de 30 de diciembre, que es un norma accesoria a esta materia[31], de medidas fiscales, administrativas y del orden social reconoce el derecho del ciudadano a la confidencialidad de sus datos y el artículo 23 que reconoce la potestad de la Administración Sanitaria para crear registros y la adopción de los medios técnicos y organizativos que se establecen en el marco normativo.

El respeto a la intimidad en este contexto de vigilancia y protección de la salud del trabajador, el art. 22 de la ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales dispone que las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud. En este aspecto, se puede hablar más que de protección de la intimidad, de protección de la confidencialidad sobre unos datos personales compartidos, ya que hay un acceso de terceros a la intimidad del trabajador, pero siempre quedando obligados legalmente aquéllos a mantener la confidencialidad acerca de los mismos. La intimidad queda igualmente protegida por los principios de pertinencia y proporcionalidad, ya que sólo se podrán practicar las pruebas que sean idóneas para cumplir los objetivos de seguridad laborales y al mismo tiempo que las ventajas obtenidas con su realización sean mayores que los perjuicios que se pudieran ocasionar con ocasión de las mismas.

Por otro lado, una vez que el trabajador ha sido informado y ha prestado su consentimiento para la realización de exámenes médicos sobre su persona, no se podrán hacer más pruebas que las estrictamente imprescindibles, pues de otra forma se violaría su derecho a la intimidad, sin que en ningún caso puedan realizarse aquellas pruebas que no tengan relevancia para la actividad laboral.

4. LAS LÍNEAS ROJAS: EL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

Quizás para entender esta interesante materia sea preciso partir del examen de los conductas que implican desviaciones tan groseras que suponen una reacción del Derecho penal. Sabido que es, que dada la vigencia del principio fragmentario y de intervención mínima, el Derecho penal solo parece cuando nos topamos frente a conductas absolutamente intolerables. Supone descubrir los Secretos o vulnerar la Intimidad, entre otros, mediante el acceso a datos de carácter personal, (los datos de salud merecen esta consideración) registrados en ficheros informáticos u otros archivos o registros públicos o privado. El art. 197 del Código Penal constituye el precepto penal marco sobre el que se construye

el ámbito de su competencia, la actividad profesional de los colegiados, velando por la ética y dignidad profesional y por el respeto debido a los derechos de los particulares y ejercer la facultad disciplinaria en el orden profesional y colegial".

31 No se trata de una norma *ad hoc* reguladora de esta materia, es una mera ley de acompañamiento a los Presupuestos que introduce una relevante precisión.

la responsabilidad penal por la revelación de información íntima. Así, el núm.1 contempla las acciones delictivas de apoderamiento de datos secretos íntimos por parte de particulares. El núm. 2 se refiere a estas mismas conductas o de utilización o manipulación de datos secretos íntimos que están en ficheros informáticos. El núm. 3 se aplica a las personas que accedan a estos datos vulnerando las medidas de seguridad de los programas informáticos que protegen la información confidencial. El núm. 4 contempla las acciones de revelación de secretos íntimos o cesión a terceros. Los números siguientes contemplan agravaciones de responsabilidad para el caso de que los autores sean los responsables de la custodia de esta información, si la información personal tiene un carácter determinado. Es destacable que la difusión de información relativa a la salud de la persona es un supuesto de agravación. Además, se agrava la responsabilidad si se realizan tales conductas con fines lucrativos o por medio de una organización criminal[32].

Si el sujeto activo es un funcionario público nos adentramos en el delito de Violación de Secreto Profesional afecta al profesional (entendiendo por profesional toda actividad realizada con carácter público y jurídicamente reglamentada) que incumpliendo su obligación de sigilo y reserva, divulgue los Secretos de otra persona. Se encuentra previsto y penado en el art.199.2 del CP[33] supone revelar secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales.

5. JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

5.1 La STEDH C.C. contra España

No obstante parece necesario recordar que los datos relativos a la salud son especialmente sensibles. Al hilo de esta cuestión, cabe citar la STEDH asunto *C. C. v. España* de seis de octubre de 2010[34] que condenó a España a indemnizar a un ciudadano porque un Juez de primera instancia español acordó en resolución motivada que se le remitiera el expediente médico del solicitante de amparo, que revelaba que padecía un linfoma y de una infección por VIH[35].

La parte afectada se opuso a que estos datos aparecieran sin reservas en el expediente judicial y solicitó que el juicio se celebrase en audiencia cerrada siéndole denegado esta petición. El Tribunal europeo declara que existió violación del Convenio o de sus Protocolos y acuerda indemnizar a la parte en cinco mil euros por daños morales.

5.2 La desconcertante sentencia del Tribunal Europeo *Barbulescu.*

La controvertida STEDH *Barbulescu* que justifica la supervisión telemática realizada por una empresa rumana sobre el contenido de la cuenta de correo electrónico de un empleado. En dicha interceptación se captaron datos muy personales e íntimos derivado sus conversaciones particulares y como consecuencia, se le despidió sancionando así el envío de correos electrónicos personales durante horas de trabajo. En esta causa, el Alto Tribunal entendió que la empresa no había violado los derechos del empleado.

Se analiza en la analizada resolución una intromisión en la vida privada de sus trabajadores, si están efectivamente en el trabajo, incluso cuando se entrometa en conversaciones intimas y sobre el estado de la salud.

La controvertida sentencia, aun no firme, Barbulescu versus Rumania[36] (publicada el 12 de enero de 2016 por el Tribunal de Derechos Humanos de Estrasburgo) justifica y da legitimidad al hecho de que una empresa lea e inspeccione los correos electrónicos —privados o profesionales— de cualquier empleado si existe un previo soporte contractual donde se advierta al trabajador de dicha posibilidad. La sentencia se refiere a un caso "específico" ocurrido

32 La L01/2015 introduce los nuevos delitos de intrusión informativa, delitos relacionados con la protección intelectual acatando la directiva 2013/40 de 12 de agosto.

33 Literalmente: "el profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años".

34 STEDH CC Asunto *C.C. v. España*, de 6 de octubre de 2010, (Demanda Núm 1425/06), (Casadevall Pte).

35 Vid. LÓPEZ ORTEGA, Juan José, "CC C. España (STEDH de 6 de octubre de 2010)a propósito de la protección de la confidencialidad de las informaciones médicas en la doctrina del tribunal constitucional",
Conflicto y diálogo con Europa: las condenas a España del Tribunal Europeo de Derechos Humanos, [coord. por Rafael Alcácer Guirao, Margarita Beladíez Rojo, José Miguel Sánchez Tomás], Civitas, Cizur Menor, 2013, pp. 501-536.

36 STEDH (Sec. 4ª) caso *Bărbulescu v. Rumania*, Caso Núm. 61496/08. [Pte. András Sajó].

en Rumanía en un caso donde la empresa accedió al correo electrónico de un trabajador y se encontró con contenido personal, que leyó e incluso transcribió. El Tribunal de Estrasburgo opina que no hay vulneración de la privacidad porque los mensajes de contenido privado fueron enviados durante el horario laboral, a través de herramientas corporativas y, además, estaba prohibido expresamente por la normativa interna de la compañía.

6. LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL

La Sentencia 114/2006, de 5 de abril de 2006[37] postula "la necesidad de realizar esta ponderación y la identificación de los específicos intereses a tomar en consideración para justificar la excepción de la publicidad íntegra de la resolución viene siendo una práctica habitual de este Tribunal, en una labor que responde a criterios también seguidos por otros Altos Tribunales extranjeros, supranacionales e internacionales y, muy especialmente, por el Tribunal Europeo de Derechos Humanos (en lo sucesivo TEDH). Así, este Tribunal Constitucional, como ya se ha señalado en el ATC 516/2004, de 20 de diciembre, FJ 1, sin perjuicio del especial cuidado que muestra en no incluir en sus resoluciones ningún dato personal que no resulte estrictamente necesario para formular su razonamiento y el correspondiente fallo, (...) omitir la identificación de determinadas personas que aparecían mencionadas en sus resoluciones, bien atendiendo a la garantía del anonimato de las víctimas y perjudicados en casos especiales (...); atendiendo el específico deber de tutela de los menores (...).

Esta labor (...) responde también a la práctica seguida por el TEDH tanto en su Reglamento de procedimiento como en su jurisprudencia. Así, el Reglamento del Tribunal, en su versión consolidada que entró en vigor el 1 de diciembre de 2005, establece en su art. 47.3 que los demandantes que no deseen que su identidad sea revelada públicamente deberán solicitarlo y exponer las razones que justifiquen la excepción del principio general de publicidad del procedimiento y que el Presidente de la Sala sólo podrá autorizar el anonimato en casos excepcionales.

Como desarrollo de la normativa sobre prevención de riesgos laborales, su jurisprudencia el Tribunal Constitucional en su sentencia 37/1989 de 15 de febrero[38], sostiene que «el ámbito de intimidad corporal constitucionalmente protegido no es coextenso con el de la realidad física sino cultural, y determinada en consecuencia por el criterio dominante en nuestra cultura sobre el recato corporal, de tal modo que no pueden entenderse como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo sobre las que operan o por los instrumentos mediante los que se realizan, no constituyen, según un sano criterio, violación del pudor o del recato de la persona» .

Ahora bien, que se respete la intimidad corporal entendida ésta en el sentido anteriormente indicado, no significa que no se pueda invadir la intimidad personal considerada en un sentido más amplio; así ocurriría por ejemplo con unas analíticas realizadas únicamente con el objetivo de averiguar si se consumen drogas en el caso de que esta información resulte irrelevante para el desempeño de la actividad laboral. Un despido basado en ese tipo información que no guarda ningún interés para el desempeño de la prestación laboral sería declarado nulo por infracción del derecho fundamental del trabajador a su intimidad.

En este sentido, la STC 62/ 2008[39], en relación a un despido por enfermedad, afirma que no es esencialmente discriminatorio pues entiende que si la enfermedad hace demasiado oneroso para el empleador la contratación el despido se encuentra justificado.

7. JURISPRUDENCIA DEL TRIBUNAL SUPREMO

Analizando el art.22 el de la ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales,

37 STC 114/ 2016, (Sala 1ª), de 5 de abril, (Pérez Tremps).

38 STC 17/1989, (Sala 1ª), de 15 de febrero, (Rubio Llorente).

39 STC 62/ 2008, (Sala 1ª), de 26 de mayo (Casas Baamonde). En su FJº 3 dictamina "aun cuando el despido se produjera encontrándose el trabajador en situación de incapacidad temporal, no es dicho proceso de incapacidad temporal el causante del mismo, sino la enfermedad preexistente que dicho proceso puso de manifiesto y que la empresa afirma conocer únicamente a partir de ese momento, y no en el momento de la contratación. No puede hablarse, por tanto, de una discriminación por enfermedad temporal, al no existir indicio alguno de que fuera ésta la causa del despido, y ello al margen de que una enfermedad temporal, en cuanto situación que necesariamente afecta a la práctica totalidad de los seres humanos en muy diferentes momentos de su vida profesional, difícilmente puede configurarse en abstracto y con carácter general como un factor de discriminación prohibido por el art. 14 CE.

el Tribunal Supremo desestima el recurso de casación interpuesto por el sindicato CC.OO contra la sentencia del TSJ Valencia, sobre conflicto colectivo, y declara la conformidad a derecho de la exigencia empresarial de someter a reconocimientos médicos a los 700 trabajadores de las Brigadas Rurales de Emergencias. Se ampara dicha resolución en que dicho reconocimiento forzoso no es arbitrario pues se basa en una necesidad de proteger la vida de los trabajadores o terceros como justificación de la obligatoriedad del reconocimiento. Apreciación de circunstancias excepcionales en el caso concreto (tipo de actividad realizada por los brigadistas y necesidad de estar en buenas condiciones físicas y psíquicas), que amparan la obligatoriedad. El reconocimiento cuestionado cumple con las exigencias constitucionales y legales para que puedan imponerse a los que trabajan en las Brigadas Rurales de Emergencias adscritas a la empresa. La sentencia prefiere no entrar en el espinoso tema relativo a cuestiones ajenas al conflicto colectivo, como confidencialidad de los resultados o consecuencias a la negativa de someterse a las revisiones, etc.

Pese a que, como hemos visto, la revelación no autorizada del historial médico constituye un delito de revelación de secretos, la STS 778/2013[40], de 22 de octubre, considera que es posible la aplicación de un error invencible cuando la difusión de tales datos médicos se realiza para denunciar irregularidades en los implantes mamarios realizados en una clínica sobre múltiples pacientes. No obstante, el Tribunal Supremo también realizó una puntualización considerando que «el acusado debió limitarse a denunciar dejando a los institutos de persecución penal que actuaran en la finalidad que le es propia». Es decir, el acusado se excedió a la hora de acceder a la información confidencial, que podía haber sido recabada por los órganos públicos dedicados a la persecución de los delitos. Ahora bien, este exceso no es susceptible de generar responsabilidad penal por el descubrimiento de la intimidad de los pacientes, aunque si se genera responsabilidad civil.

En el orbe represivo penal, la Sentencia 532/2015[41], que añade que la conducta sería atípica vía art.197.2 del CP si no se acreditara el perjuicio para el titular de los datos o que éste fuera ínsito, por la naturaleza de los datos descubiertos, como es el de los datos relativos a la salud que son ontológicamente sensibles.

Paralelamente, merece destacarse la Sentencia 734/2015[42], sobre valoración manifestaciones del acusado en el marco de la entrevista con un facultativo**.** La Sala de lo Penal del Tribunal Supremo, ha precisado que las manifestaciones sobre los hechos que el acusado puede hacer en el marco de una entrevista con un facultativo (psiquiatra, psicólogo, forense) no pueden utilizarse como elemento probatorio nunca. Servirán al facultativo para su diagnóstico y para obtener sus conclusiones periciales, pero nunca puede convertir a este en un anómalo testigo de referencia de lo relatado por el acusado sin asistencia letrada ni advertencia de sus derechos. Esas entrevistas médicas no pueden servir en modo alguno para obtener información del imputado que, en ese escenario, es paciente y no investigado, y no puede ver arrebatada la confianza plena en el facultativo por el temor de que desvele lo que le narra sin ser advertido previamente de sus derechos. El facultativo debe informar en el acto del juicio sobre los aspectos periciales (conclusiones sobre padecimientos psíquicos). Pero ni se le pude preguntar si el paciente le relató algo sobre los hechos enjuiciados; ni mucho menos debe contestar a cuestiones de ese tenor.

40 STS 778/2013, (2ª), de 22 de octubre, (Martínez Arrieta). Para el Tribunal Supremo, el médico actuó de forma adecuada pese a que se hizo acopio de documentación personal de los pacientes a la que no estaba autorizado. La Sala considera que «el recurrente tiene un conocimiento de la situación de antijuridicidad en la que se sitúa la empresa para la que trabaja y ante el riesgo cierto de que esa situación repercuta en su contra, y con la finalidad de actuar por la salud de los pacientes de la clínica decide acopiar la información precisa para su denuncia ante los órganos que tienen la capacidad de corregir la situación de antijuricidad en lo que él no ha participado, pero le afecta». Por ende, la Sala 2ª consideró que el médico obró con un error invencible al apoderarse de la información médica de personas que no habían sido sus pacientes y difundirla mediante la presentación de una denuncia, pues el acusado «se asesoró, acudiendo a fuentes de su máxima solvencia para desvanecer el error, y actuó en defensa de su propio derecho al ejercicio de su profesión sin el temor de una responsabilidad exigible, y en la creencia, errónea, de que la denuncia que formulaba requería una previa indagación de los hechos».

41 STS 532/2015, (2ª) de 23 de septiembre, (Palomo el Arco). Se postula que el artículo 197.2 CP, conforme al ya postulado en las SSTS 123/2009, de 3 de febrero;1328/2009, de 30 de diciembre y990/2012, de 18 de octubre, sólo con relación al inciso primero (apoderamiento, utilización o modificación) y al último (alteración o utilización), menciona expresamente el legislador que la conducta se haga en perjuicio de tercero, mientras que no exigiría tal perjuicio en el caso de la conducta de acceso; si bien, resulta necesario realizar una interpretación integradora del precepto, pues no tendría sentido que en el mero acceso no se exija perjuicio alguno, y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles -y con la misma pena- en el inciso segundo.

42 STS 734/2015, (2ª) de 3 de noviembre, (Del Moral García).

8. JURISPRUDENCIA MENOR

Sobre este tema cabe destacar la sentencia de la Audiencia Provincial (en lo sucesivo) SAP de Valladolid de 14 de julio de 1998 relativa a un supuesto de vulneración de la intimidad de los miembros de una Asociación de parapléjicos y minusválidos físicos. La pena es la prevista en cada caso para la infracción cometida en su mitad superior (STS de 10 de diciembre de 2004 y 11 de julio de 2001). Por su parte, el Auto AP de Barcelona de 24 de enero de 2000 declara la atipicidad de la conducta de unos laboratorios los cuales comunican a su cliente, una compañía aérea, el resultado de análisis de sangre y orina encargados por ella con respecto a una trabajadora, contando con la autorización de ésta y sin que conste la difusión a terceros del dato íntimo conocido. El AAP de Madrid de 19 de octubre de 2004 ve indicios delictivos en la conducta de proceder a la digitalización y publicación en Internet de una historia clínica del personado como acusación particular, sin autorización ni consentimiento de éste.

En el ámbito penal destaca igualmente la SAP de Mallorca de 28 de enero de 2015[43], plenamente confirmada en todos sus puntos relativos al delito contra la intimidad por la STS 40/2016[44]. El supuesto factico parte de que el acusado, médico de un centro público de salud, había mantenido una relación sentimental con una enfermera también trabajadora del centro de salud. La relación terminó con varios desencuentros que determinaron la incoación de un expediente disciplinario al acusado en el que se tuvo conocimiento de que el médico había accedido a los historiales médicos de la perjudicada y su familia, lo que quedó reflejado en el sistema informático, para lo que ni estaba autorizado ni justificado. Las sentencia reprochan al acusado haber accedido sin consentimiento ni conocimiento de la perjudicada y amparado en su condición de funcionario médico de la Comunidad Autónoma de las Islas Baleares, que le permitía acceder a los sistemas de información del IB-salut y siendo consciente del compromiso de confidencialidad que había contraído".

9. EL RESPETO A LA INTIMIDAD MÉDICA: LA DOCTRINA *TARASOFF*

Es una de las doctrinas más importantes en relación al control externo de los flujos de información médico-paciente, con una dimensión universal que ha tenido un gran eco fuera de las fronteras de E.UU donde se engendró inicialmente. Esta doctrina analiza los límites de la confidencialidad médico-paciente relativizando un tanto los limites de dicha confidencialidad, no enmarcándose como un derecho absoluto sino que admite algunos condicionantes. Se parte de la idea de que aun siendo la confidencialidad médico-paciente una de los pilares de un moderno sistema sanitario, este axioma no es incondicional merece destacarse que como todos los derechos tiene sus propios límites el más claro de los cuales lo encontramos en la doctrina Tarasoff. El planteamiento de este pronunciamiento jurisprudencial del Tribunal de California parte del límite que dicha conducta de secretismo puede generar a terceros. La realidad nos ofrece situaciones en las cuales de no infringirse esta obligación, pudieran derivarse consecuencias perjudiciales para el paciente, el profesional u otras personas, podrían ser consideradas como razones válidas para fundamentar excepciones a la regla. Circunstancias tales como la revelación del paciente acerca de sus intenciones de matar, suicidarse o poner en peligro la vida o la seguridad de terceros, ilustran el dilema entre el deber de respetar la privacidad (autonomía) y el deber de no perjudicar (no-maleficencia) o de tener un trato equitativo para con todos (justicia). Éstos son casos en los que el profesional se cuestionará el cumplimiento de este deber".

Precisamente, en el ya referido caso *Tarasoff* el señor Poddar reveló al terapeuta que lo atendía la intención de matar a una compañera de la Universidad de Berkeley. Aunque no dio su nombre, el terapeuta se dio cuenta que se trataba de una antigua amiga de su paciente, Tatiana Tarasoff de la cual estaba obsesionado. Ordenó el internamiento del joven en un instituto psiquiátrico, pero los médicos forenses determinaron que el estado de Poddar no requería la reclusión y bajo la promesa (*parole*) de que no se acercaría a la muchacha, no lo retuvieron. Dos meses más tarde, Poddar mató a Tatiana.

Los padres de Tatiana demandaron civilmente a la Universidad de California por omisión del deber de cuidado y exponer a un palpable riesgo a su hija. En 1974, la Corte Suprema de California consideró que, a pesar del deber de confidencialidad, el facultativo que atiende al paciente tiene el deber de advertir a la potencial víctima para evitar un potencial daño grave causado por un problema psicológico de un enfermo.

43 Sentencia Audiencia Provincial de Baleares 5/2015, (Sec. 2ª, de lo Penal), de 28 de Enero de 2015, Rec 72/2014.

44 STS 40/2016 , (2ª), de 3 de febrero, (Martínez Arrieta).

Enfrentados con esta decisión, los profesionales de salud mental respondieron que esta norma violaba su relación profesional "especial" y que minaría la confianza de sus pacientes. Además advertían a la Corte que les parecía muy difícil predecir violencia y habría muchos falsos positivos (con los que se violentaría la tranquilidad de personas que en realidad no están en peligro), con lo cual a la larga sería aún peor.Ante ello, la Corte emitió una segunda opinión[45], mantuvieron el criterio de que los facultativos mentales tienen deberes con las víctimas potenciales, pero sólo deben aplicar un "cuidado razonable" para proteger a las personas. Es decir, el psicólogo puede tener que hospitalizar voluntariamente al paciente para evitar eventuales perjuicios a terceros, en lugar de advertir explícitamente a una víctima potencial.

Paralelamente, el alto tribunal estadounidense en la conocida sentencia *Washington v. Harper*[46] se posiciona sobre el rechazo de tratamientos psicotrópicos forzados con carácter generalizado. No obstante, el Tribunal Supremo de Estados Unidos dictaminó en la referida resolución que la Cláusula del Debido Proceso (Due process)[47] permite solo al Estado utilizar tal tipo de tratamiento sólo en que el interno penitenciario posea un trastorno mental grave con la medicación antipsicótica administrada en contra de su voluntad, cumpla el requisito o condición de que el estado mental del interno sea peligroso para ellos mismos o los demás y el medicamento recetado se aplique bajo los cánones de la *lex artis* o del puro interés médico.

Posteriormente en la sentencia *Riggins v. Nevada*, de 1992[48], el Tribunal Supremo de Estados Unidos se posicionó sobre si una persona con enfermedad mental puede ser obligada a tomar la medicación antipsicótica mientras que se encuentra en la vista del juicio, el Estado afirmaba que dicha medicación era necesaria para asegurarse de que el enjuiciado poseería capacidad durante el juicio.

Sin embargo, el Tribunal Supremo anuló la resolución del tribunal inferior afirmando que la administración forzada de medicamentos antipsicóticos durante el juicio *Riggins* violó sus derechos garantizados por la Sexta y Decimocuarta Enmiendas. La mayoría de siete miembros concluyó que el Estado no ha demostrado que la medicación antipsicótica fue apropiada bajo criterios clínicos y tampoco demostró que hubiera medios menos intrusivos en la obtención de su objetivo de tratar de *Riggins*. La Corte afirmó que la Octava Enmienda (que prohíbe que el gobierno federal imponga castigos inusuales o crueles) impide la administración forzosa de la medicación antipsicótica a un ciudadano lo que además le negó la oportunidad de mostrar al jurado su verdadero estado mental en el juicio.

Esta decisión puso de relieve dos factores que deben ser evaluados en los casos de la medicación involuntaria. En primer lugar, el tratamiento involuntario debe ser el tratamiento menos invasivo para la restauración de la capacidad mental. En segundo lugar, el tratamiento propuesto debe ser médicamente necesario en orden a garantizar la seguridad del individuo afectado por el mismo.

10. EL DERECHO A LA INTIMIDAD GENÉTICA Y EL MAPA DEL GENOMA HUMANO

Por más pequeños que puedan parecer los vestigios biológicos que se dejan al pasar, éstos pueden servir para la identificación de la huella genética que excluye a un individuo de todas las demás personas. La información genética, además, puede descifrar las relaciones de la familia biológica, el que se padezca una determinada enfermedad o que se tenga la posibilidad de padecerla. Los bancos de tejidos, como lo son, por ejemplo, los bancos de sangre, almacenan una información que, potencialmente, revela ilimitada datos sobre el individuo[49].

El art.5.a) de la Declaración Universal sobre el Genoma y los Derechos Humanos de 11 de noviembre de 1997, realizado en el ámbito de la UNESCO, establece que una investigación, un tratamiento o un diagnóstico en relación con el genoma de un individuo sólo podrán efectuarse previa evaluación

45 Sentencia del Tribunal Supremo de California *Tarasoff v. Regents of the University of California*, de 1 de julio de 1976, 17 Cal. 3d 425 (1976), 551 P.2d 334, 131 Cal. Rptr. 14.

46 Sentencia del Tribunal Supremo de los Estados Unidos, *Washington v. Harper* (494 US 210, 1990).

47 Contenida en la XIV Enmienda a la Constitución de los EE.UU, viene a singificar que todo juicio justo (*fair trial*) debe acomodarse a los garantías previstas en la propia Constitución.

48 Sentencia del Tribunal Supremo de los Estados Unidos, *Riggins v. Nevada*, 504 U.S. 127 (1992). No obstante, dado que procesalmente no se planteó en la solicitud de *certiorari*, en consecuencia, no fue abordado como a tema a debate por el tribunal.

49 Vid. MURRAY, Thomas H., "Genetic Exceptionalism and 'Future Diaries': Is Genetic Information Different from other Medical Informatics?", *Rothstein M, ed. Genetic Secrets: Protecting Privacy and Confidentiality in Genetic Era*, Yale University Press; New Haven, 1997, p. 63.

rigurosa de los riesgos y las ventajas que entraña y de conformidad con la legislación nacional. En todo caso -establece la declaración en su apartado b)- se recabará consentimiento previo, libre e informado de la persona interesada.

Por su parte el art.7 de la referida Declaración establece que se deberá proteger a las condiciones estipuladas por ley la confidencialidad de los datos genéticos asociados con una persona identificable, conservados o tratados con fines de investigación o cualquier otra finalidad.

Paralelamente cabe citar la Declaración Internacional sobre los Datos Genéticos Humanos, de 16 de octubre de 2003, también elaborada en el seno de la UNESCO. En dicha declaración tras reconocer en el art.7 el derecho a la protección especial de los referidos datos, se hace especial énfasis en el art.13 al derecho de acceso que toda persona directamente implicada e identificada en este tipo de estudio, debe tener respecto de sus propios datos genéticos o proteómicos, con la sola excepción hecha de las limitaciones que sean necesarias imponer por razones de salud, orden público o seguridad nacional. Asimismo el art.14 de la referida normativa, resalta la necesidad, recaba la necesidad el consentimiento del afectado para trasladar información respecto de los datos genéticos humanos pertenecientes a una persona identificable. No obstante el art.16 prevé que este consentimiento pueda ser suplido por una ley ad hoc, pero en ningún caso los datos genéticos humanos pueden ser empleados con un fin diferente para el que fueron obtenidos

Es necesario destacar que se trata de instrumentos jurídico que no pueden entenderse como estrictamente obligatorio (*soft law*), pero que orientan en la situación legislativa, sin perjuicio de que puedan considerarse principios generales del Derecho Internacional y de su alcance interpretativo.

La secuenciación del genoma humano revela nuestro futuro de un modo más o menos inmediato las enfermedades que nunca contraeremos, las que probablemente contraeremos e incluso ciertas patologías heredadas de nuestros parientes. La medicina del futuro se focaliza hacia el análisis de los datos del análisis genético que permite el diagnóstico y el grado de vulnerabilidad frente a determinadas enfermedades hereditarias, un manejo inadecuado de esa información dejaría inerme a un individuo que vería los grandes rasgos evolutivos de su futura salud, expuestos de un modo incontrolado de cara al público. El art.4.13 del nuevo Reglamento de 2016 que analizaremos después con más detalle, define los «datos genéticos»: 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.

También resulta destacable el Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997. En su desarrollo encontramos la Ley 14/2007, de 3 de julio, de Investigación Biomédica aborda entre sus cometidos el tratamiento de datos genéticos de carácter personal[50] y de las muestras biológicas de origen humano que se utilicen en investigación regulados como un objeto de la Ley en su art.1.2[51].

Dentro de esta última norma, es el art.5 el que garantizará la protección de la intimidad personal y el tratamiento confidencial de los datos personales. Así, el apartado 3º del referido artículo, prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento. De todas formas, las muestras biológicas no constituyen en sí mismas un dato personal, sino fuentes de las que se pueden obtener datos personales.

El artículo 59, apartado 1º de la ley de investigación biomédica establece que la información previa a la utilización de la muestra biológica que debe facilitarse por escrito al sujeto fuente debe incluir la "finalidad de la investigación o línea de investigación para la cual consiente". La referida norma, por consiguiente, tutela la voluntad del sujeto y la limita a la posibilidad de consentir que sus muestras sean utilizadas sólo en proyectos científicos determinados y en otros de la misma línea de investigación, sin contemplar la posibilidad de que el consentimiento permita la utilidad de las muestras en investigaciones futuras, aunque no estén relacionadas con aquella prevista inicialmente.

50 Definidos en el art.3.w) de la misma norma como aquellas operaciones y procedimientos que permiten la obtención, conservación, utilización y cesión de datos genéticos de carácter personal o muestras biológicas.

51 Por su parte, el art.2. c) postula que las investigaciones a partir de muestras biológicas humanas se realizarán en el marco del respeto a los derechos y libertades fundamentales, con garantías de confidencialidad en el tratamiento de los datos de carácter personal y de las muestras biológicas, en especial en la realización de análisis genéticos.

11. EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Con fecha de 4 de mayo de 2016 se publicó en el Diario oficial de la Unión Europea el nuevo Reglamento General de Protección de Datos (en lo sucesivo RGPD), que viene a derogar de facto la Ley Orgánica de Protección de Datos 15/1999 exigiendo del legislador una nueva norma de desarrollo. Se trata de una normativa largamente esperada y que posee un carácter revolucionario constituyendo todo un hito en esta materia. Esta norma será de aplicación directa en toda la Unión Europea a partir del 25 de mayo de 2018, sin necesidad de traslación a las legislaciones nacionales.

El objetivo del RGPD es conseguir una mejor protección de los datos personales de los europeos, dotándonos de mayor control sobre ellos a partir de una legislación uniforme para todos los países de la Unión. La norma contempla un nuevo régimen sancionador a este tipo de infracciones, con multas mucho más elevadas.

A partir del 25 de mayo de 2018, las administraciones públicas y las empresas deberán estar preparadas para esta nueva norma, que incluye obligaciones como la documentación y el registro obligatorio de tratamientos, la comunicación de las brechas de seguridad a las autoridades en 72 horas, la puesta en funcionamiento de análisis de riesgos, o la implementación de nuevos derechos de los ciudadanos como el de la portabilidad de los datos personales[52].

En la legislación actual (LOPD), los datos de salud tienen un nivel de protección elevado basado en su categorización como datos de nivel alto[53] además son de interpretación extensiva[54], y su tratamiento, de manera general, está sujeto al consentimiento expreso del ciudadano[55]. En el nuevo RGPD se establece una categoría de "datos de carácter personal relacionados con la salud", en general más restrictiva, que redefine aspectos como la prohibición general del tratamiento, los supuestos en los que se pueden tratar categorías especiales de datos y otras medidas que veremos a continuación.

El consentimiento inequívoco del ciudadano para que sus datos sean tratados permanece y, además, tendrá que ser recabado con anterioridad al tratamiento, cosa que no ocurría con la LO 15/1999 de Protección de Datos.

Aparte de los ya conocidos derechos ARCO: acceso, rectificación, cancelación y oposición de la LOPD, el nuevo RGPD establece el derecho de portabilidad, esto es, el ciudadano tendrá derecho a recibir sus datos personales almacenados en un formato adecuado para que pueda entregárselos a otro responsable del tratamiento. Por ejemplo, centrándonos en el entorno de la sanidad privada, el nuevo Reglamento reconoce el derecho a pedir a un prestador sanitario nuestra historia clínica electrónica para poder facilitársela a otro prestador.

Respecto a las obligaciones del responsable y del encargado del tratamiento, pasa a ser un elemento clave el principio de *accountability* (responsabilidad), introducido en la norma principalmente a instancias del Reino Unido por más que, finalmente, no vayan a disfrutarlo. Se trata sobre todo de establecer una "responsabilidad proactiva" basada en la existencia de procedimientos auditados, el establecimiento de políticas de protección de datos y la adhesión a códigos de conducta y certificaciones en materia de protección de datos. Respecto a este último punto, es previsible que el cumplimiento del RGPD pase en el futuro por mecanismos de certificación ante organismos que se creen a tal efecto. Un concepto

52 En este sentido el Considerando 68 establece que: "Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos".

53 Ello comporta conforme al art.9 del Reglamento de 2016, la prohibición del tratamiento de datos personales que revelen datos relativos a la salud. Aunque el apartado 2º i) del mismo artículo excepciona el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

54 Así el considerando 35 de la norma establece que "Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro". El art.4.15 del nuevo Reglamento define «datos relativos a la salud»: como 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.

55 Sin embargo, caben alguna flexibilizaciones como cuando se aborda la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud (considerando 52 del Reglamento)..

importante en el RGPD es el de "obligatoriedad de resultado". No es suficiente con haber cumplido la norma de protección de datos (o, en el futuro, estar certificado), sino que los datos deben efectivamente estar protegidos y no deben producirse brechas de seguridad de esta información si no los responsables pueden ser sancionados.

Una figura de corte alemán[56] que cobra aun mayor relevancia que en la norma anterior es la del Delegado de Protección de datos[57] (*Data Protection Officer, DPO*) que será obligatoria en la mayoría de las empresas. Será el responsable del cumplimiento de las obligaciones de protección de datos y sus funciones están descritas en el RGPD[58]. La importancia esta nueva figura es incalculable, el artículo 38 del nuevo RGPD, señala la obligación que tienen tanto el responsable, como el encargado del tratamiento de garantizar que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, pero esta obligación incluso va más allá, toda vez que los mismos tienen que respaldar, además, a dicho delegado de protección de datos en el desempeño de sus funciones, y a tal efecto le han de facilitar los recursos económicos, materiales y humanos necesarios para el desempeño adecuado de sus funciones, y al mismo tiempo, dicha obligación conlleva la posibilidad de permitirle con toda amplitud, el acceso a los datos personales y a las operaciones de tratamiento para el mantenimiento de sus conocimientos especializados. Dada la sensibilidad de los datos sanitarios dichos Delegados van a adquirir tanto un enorme poder como una enorme responsabilidad.

La Administración sanitaria y las empresas sanitarias, ya sean públicas o privadas, tienen en todo caso la obligación de contar con un Delgado de Protección de datos[59].

Respecto a las brechas de seguridad, éstas tendrán que ser obligatoriamente comunicadas al organismo nacional competente en un formato normalizado y en un máximo de 72 horas desde que se tuvo constancia. En determinados supuestos, también será obligatorio informar al interesado de que la brecha de seguridad se ha producido.

Otro mecanismo importante que impone el RGPD son los *Privacy Impact Assessments* (PIAs) o evaluaciones de impacto. Estas evaluaciones serán en muchas ocasiones obligatorias cuando estén en juego datos sensibles como los de salud, el artículo 40 del RGPD dedicado a los códigos de conducta recoge una referencia expresa a la seudonimización de los datos. Así, indica que las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento, podrán elaborar códigos de conducta o modificar/ampliar dichos códigos con el propósito de especificar la aplicación de disposiciones del Reglamento, por ejemplo, la seudonimización de datos personales. De otro lado, el artículo 40 del RGPD cuando aborda los códigos de conducta recoge una referencia expresa a la seudonimización de los datos. Así, indica que las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento, podrán elaborar códigos de conducta o modificar/ampliar dichos

56 Su origen se encuentra en el "Bundesbeauftragten für den Datenschutz" quefue incluida en la Ley Federal de Protección de Datos (Bundesdatenschutzgesetz, BDSG), de 27 de enero 1977.

57 Sobre este tema consultar mi artículo "El Data Protection Officer (Delegado de Protección de Datos) en el nuevo Reglamento de la Unión Europea", *Sepinnet, artículo monográfico*, SP/DOCT/20367mayo de 2016.

58 Extrañamente, pese a ser una figura troncal en la nueva normativa, no viene incluido en el catálogo de definiciones del art.4 RGPD. Sin embargo, es importante tener en consideración que la Comisión Europea, cuando presentó en 2012 su propuesta de RGPD (COM(2012) 11 final, de 25 de enero), no incluyó la definición en la misma, pero sí lo hizo en el Documento de Trabajo de los servicios de la Comisión relativo a la evaluación de impacto de su propuesta (SEC(2012) 72 final, de 25 de enero) se define al DPO de la siguiente manera: "una persona responsable dentro del responsable o del encargado del tratamiento para supervisar y monitorear de manera independiente la aplicación interna y el cumplimiento de las normas de protección de datos. El DPO puede ser tanto un empleado como un consultor externo". En cualquier caso el art.37.5 del RGPD precisa que "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".

59 El artículo 37 del Reglamento determina la obligatoriedad de la designación del Delegado de Protección de Datos: (1) cuando el tratamiento lo lleve a cabo una autoridad u organismo público; (2) cuando las actividades principales del responsable o encargado del tratamiento consistan en operaciones de tratamiento que requieran un seguimiento regular y sistemático de los interesados a gran escala; y (3) cuando las actividades principales del responsable o el encargado consistan en el tratamiento a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos. El sector público sanitario viene comprendido en el apartado 1º. Las empresas sanitarias privadas vienen comprendidas en el apartado 2º, entenderá que estamos ante una actividad principal cuando el tratamiento de datos sea el objetivo fundamental de la misma (una app que maneja perfiles, por ejemplo), o bien, cuando el tratamiento resulte parte intrínseca de la actuación de la empresa. Aquí encajar el caso de un hospital en el que, si bien finalidad principal es la prestación de servicios sanitarios, éstos no podrían prestarse sin operar con los datos de los pacientes

códigos con el propósito de especificar la aplicación de disposiciones del Reglamento, por ejemplo, la seudonimización de datos personales.

Por último, el régimen sancionador se endurece y las multas pueden alcanzar los veinte millones de euros o el cuatro por ciento de los ingresos globales de la compañía multada.

En definitiva, a partir de ahora seguramente se hace necesario un esfuerzo de adaptación de la normativa a los responsables o encargados de tratamientos de ficheros que incluyan datos de salud de los ciudadanos que va a deberán cambiar muchos de sus rutinas de trabajo en un plazo relativamente breve.

12. LA ANOMIMIZACIÓN Y SEUDONOMIZACIÓN DE DATOS EN EL NUEVO REGLAMENTO.

Hay que aclarar que los datos sanitarios no son *per se* maliciosos. Un conocimiento de los datos médicos es imprescindible para los profesionales y en la vital vital área de la investigación contra las enfermedades. Pero una vez más el uso no debe ser identificado con el abuso, por ello deben ser protegidos de tal forma que no se conviertan en una valiosa mercancía.

Dos nuevos conceptos troncales aparecen en esta materia con el RGPD son la anonimización y la seudonimización[60], enfocados como mecanismos de disociación o despersonalización de los datos en relación a su titular. La anonimización es aquel procedimiento que, aplicado a los datos de carácter personal, los convierte en datos que, de forma absoluta e irreversible, no permiten inferir la persona de la que proceden. Como en la LOPD, estos datos disociados quedan fuera del alcance del RGPD. Por el contrario, la seudonimización, según el art.4 del RGPD, es "el tratamiento de datos personales de tal manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, y dicha información adicional debe figurar por separado y estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

La seudonimización no deja los datos fuera del alcance y las medidas de seguridad del RGPD, pero ayuda a los responsables de los ficheros a cumplir con la normativa y, de hecho, el propio RGPD fomenta, junto con la encriptación, este tratamiento de los datos personales. Así, el artículo 32, referido a la seguridad de los datos, dispone que teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto, los fines del tratamiento, así como el resto de probabilidad y gravedad variables, para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Ello incluye la necesidad de la seudonimización y el cifrado de datos personales

En un principio, se podría entender que en la esfera sanitaria lo importante es anomizar los datos o desvincularlos de los pacientes para que no pudieran ser reconocidos. Como vimos el denominado internet de las cosas (*IoT*[61]) es una nueva amenaza pues un programa perfil[62] puede sonsacar conclusiones muy ajustadas de millones de datos aparentemente anodinos. Y es que una serie de datos asépticos sonsacados de la Administración sanitaria y derivados de los dispositivos mecánicos sanitarios también cabe inferir millones de datos, que los programas perfil pueden interpretar y vincular a pacientes concretos. La seudomización parte de datos asépticos, no personales, que convenientemente manipulados pueden ofrecer un perfil personal de su titular. Es un concepto inverso a la anomización que comporta una despersonalización de los datos obrantes en el *Big Data*. La principal diferencia que existe entre anonimización y seudonimización, parte de que sólo nos encontraremos ante un dato anonimizado cuando en ningún caso sea posible la vinculación del dato con la persona a la que hubiese identificado. Es decir, cuando sea imposible volver a identificar a la persona a través de ese dato. Por el contrario, la seudonimización se reduce a limitar la trazabilidad entre el conjunto de datos tratados y la persona física cuya identidad queda asociada a estos.

60 Sobre este tema consultar mi artículo "La seudonimización de datos derivados del Internet en las cosas: los peligros del caso Bates", *Sepinnet, artículo monográfico*, SP/DOCT/22786, mayo de 2017.

61 IoT es el acrónimo del internet de las cosas (Internet of Things), la abreviatura ha tenido tanto éxito n la red que ha desplazado internacionalmente al nombre original.

62 El art.4.4 del RGPD define los programas perfil como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

El Reglamento parte que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.

Sin embargo atendiendo al punto 26 de la Exposición del Reglamento establece que los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

La seudonimización de datos se encuentra definida en el art. 4.5) del Reglamento, reputándola como aquella información que, sin incluir los datos denominativos de un sujeto afectado –es decir aquéllos que lo pueden identificar de manera directa-, sí que potencialmente permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados.

Posteriormente, el Reglamento General de Protección de Datos, el art.25 incluye la seudonomización entre las estrategias a adoptar para lograr la protección de datos desde el diseño. Finalmente en su artículo 32 del Reglamento, introduce explícitamente relativo a la seguridad en el tratamiento de los datos personales, la seudonimización como una medida apropiada para garantizar un nivel de seguridad adecuado al riesgo. Los datos que desprenden la domótica cotidiana de cada individuo son datos seudonimizados aparente carecen de relevancia pero convenientemente instrumentalizados pueden revertir en un perfil muy preciso de la persona física de la que dimanan.

Hay que diferenciar entre anonimización y seudonimizacion, ya que tan sólo nos encontraremos ante un dato anonimizado cuando en ningún caso sea posible la vinculación del dato con la persona a la que hubiese identificado. Es decir, cuando sea imposible volver a identificar a la persona a través de ese dato. Por el contrario, la seudonimizacion se reduce a limitar la trazabilidad entre el conjunto de datos tratados y la persona física cuya identidad queda asociada a estos.

El proceso de seudonimización consiste en sustituir un atributo por otro en un registro, de tal forma que a pesar de que siga existiendo la posibilidad de vincular a la persona física de manera indirecta con el conjunto de datos origen, se ponen importantes barreras técnicas a dicha acción.

Por ello, se establece que la información adicional que permite dicha asociación debe encontrarse protegida por medidas técnicas y organizativas que impidan la determinación del sujeto afectado. Sin embargo, la información seudonimizada, siendo una información personal, goza de determinadas facilidades en su tratamiento.

Por ende, viene a representar una nueva herramienta que permite cumplir con mayor facilidad con ciertas exigencias del Reglamento y con uno de los mayores retos incluidos en el mismo, el del control del riesgo. Es decir, mediante técnicas de seudonimización podremos probar que hemos adoptado medidas tendentes al control de dicho factor. El gran peligro de los datos sonsacados mediante el internet de las cosas lo constituye el la elaboración de perfiles. El nuevo RGPD exige un consentimiento expreso del interesado que requiere una manifestación de voluntad libre, específica, informada e inequívoca, ya sea mediante una declaración o una clara acción afirmativa.

Es importante recordar que a efectos de la norma, los datos seudonimizados siguen siendo datos personales pues pese a que no permiten la identificación directa del interesado, no cabe dejar en el tintero en ningún momento, que nos encontramos ante datos de carácter personal, y como tal, objeto de protección de la normativa en materia de protección de datos. La seudonimización se concibe como una medida orientada a «reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos» e incluso se presenta como una medida preventiva de adopción rápida (lo antes posible).

Intentando explicar esta situación el considerando 78 del reglamento de 2016 apunta a que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales requieren la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del nuevo Reglamento.

A fin de poder demostrar la conformidad con el Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que

cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

13. CONCLUSIONES

La vieja noción de privacidad decimonónica ha quedado tan desfasada que privacidad y tratamiento de datos son conceptos muy distanciados. De un lado, tras los últimos avances en Genética y en Biomedicina sugieren posibilidades para la salud inconcebibles hasta hace apenas unas décadas. Mas, de otro lado, la revolución y las nuevas tecnologías facilitan las comunicaciones en un planeta cada vez más intercomunicado parecen convertir al ser humano en un conjunto de datos que revelan aspectos más frágiles de su salud, exponiéndoles al abuso.

Como afirmara Ulrich Beck[63] la sociedad de riesgos comportan notorios beneficios que deben ser debidamente sopesados con no menores o paralelos peligros (*checks and balances*). Los adelantos en Informática generan un nuevo escenario asimétrico que permite almacenar el máximo de datos en el mínimo espacio y que unos pocos puedan controlar la información sobre la mayoría. El mundo jurídico intenta hacer frente al nuevo desigual escenario aportando nuevas normativas que pretenden regular, entre otras materias, la reproducción asistida, la investigación biomédica, la extracción y trasplante de órganos, etc.

La irrupción avasalladora del mundo telemático en nuestras vidas tiende a alienar y anular a los individuos sino establecemos un sólido sistema de garantías que nos impermeabilice frente a un fenómeno que no solo nos supera sino que puede convertirse en una Caja de Pandora de incalculables consecuencias. La *vis atractiva* que la red ejerce sobre los datos masivos (*Big Data*) y el uso de sensores para la recogida de datos (Internet de las cosas, en inglés *IoT*), la protección de datos se hace cada vez más compleja. Por una parte, el riesgo de re-identificación de los ciudadanos tras la correlación de diferentes bases de datos, ya sean públicas o privadas, para el tratamiento de los datos masivos aumenta notablemente. Los datos que en un principio no podían identificar de forma aislada a un ciudadano, cuando se unen a otros pueden permitir su identificación mediante programas tipo perfil a pesar de que las bases de datos de origen estuvieran anonimizadas. El riesgo además dependerá de las técnicas de anonimización que se hayan aplicado a los mismos.

Con la aparición del mapa del genoma humano, detrás de los datos relativos al ADN, se desvelan potenciales enfermedades latentes o aletargadas que se pueden desencadenar en un período más o menos lejano en el tiempo. Estos datos afectan no solo al titular de los datos sino también a sus descendientes, ascendientes y demás allegados por lo que trascienden de la esfera estrictamente personal. Por lo tanto, ya no se trataría de un potencial en la esfera de lo individual sino que se ramifica hacia grupo familiar[64]. Por ejemplo, determinadas enfermedades venéreas dejan su trazo en los descendientes de los individuos y por lo tanto los hijos y demás descendientes acuñan un dato que debería permanecer a la esfera de lo estrictamente familiar.

El manejo de los datos incide en los sistemas expertos, en medicina los programas de ordenador tienden a trasladar la labor tradicional del diagnóstico médico hacia el mundo computacional tendiéndose a que el diagnóstico humano pueda aparecer como un elemento extraño en un futuro ya no muy lejano. Sin embargo, el objeto concreto de este artículo viene abordar cuál es el marco de garantías apropiado para el uso de los ficheros informáticos y el tratamiento de los datos de carácter personal o las plataformas digitales en relación al orbe sanitario.

Los datos son especialmente sensibles, en un futuro donde se prevé que la vida humana se puede

63 Vid. BECK, Ulrich, *La sociedad del riesgo: hacia una nueva modernidad*, Paidós Ibérica, Barcelona, 2006.

64 Así, por ejemplo, el artículo 5.3 de la tantas veces enunciada Ley 14/2007 exige que el consentimiento sea también prestado por los familiares del sujeto cuando los datos que pretendan cederse pudieran revelar información cuyo carácter personal sea extensible a ellos.

prolongar de modo imaginable hace solo unos años, la información sanitaria refleja nuestras expectativas de vida y atesora incluso problemas clínicos y enfermedades de nuestros desaparecidos ascendientes. Si esta información circulase sin cortapisas los individuos se hallarían alienados y condicionados frente a Estados y oligopolios, construiríamos un mundo sin privacidad. En un mundo aparentemente pleno de libertades, nuestra esfera más débil, nuestro talón de Aquiles individual, consistente en nuestras enfermedades quedaría expuesta para que cualquiera pudiera mofarse, controlarnos o aprovechársenos de nuestra debilidad. Para Rosen[65], "*la libertad es imposible en una sociedad que se niega a respetar el hecho de que actuamos distinto en privado que en público*". O en palabras de Kundera[66], cuando la sociedad de la vigilancia se instaura, la transformación de lo público en privado, nos conduce a una mutación de sujeto a objeto donde nuestros defectos se exponen a modo de vergüenza.

14. BIBLIOGRAFÍA

• BECK, Ulrich, *La sociedad del riesgo: hacia una nueva modernidad*, Paidós Ibérica, Barcelona, 2006.

• BENTHAM, Jeremy, *El Panóptico*, La Piqueta, Madrid, 1979.

• CUKIER, Kenneth Neil / MAYER-SCHÖENBERGER.,Viktor, «The Rise of Big data. How It's Changing the Way We Think About the World», *Foreign Affairs, Vol. 92, Num. 3*, 2013.

• DENNIGER, Erhard, "El derecho de autodeterminación informativa" en PÉREZ LUÑO, Antonio Enrique, *Problemas actuales de la Documentación y la Informática Jurídica*, Tecnos, Madrid, 1987.

• GUDIN RODRÍGUEZ-MAGARIÑOS, Faustino, "El Data Protection Officer (Delegado de Protección de Datos) en el nuevo Reglamento de la Unión Europea", *Sepinnet, artículo monográfico*, SP/DOCT/20367mayo de 2016.

- "La seudonimización de datos derivados del Internet en las cosas: los peligros del caso Bates", *Sepinnet, artículo monográfico*, SP/DOCT/22786, mayo de 2017.

• KUNDERA, Milan, *La insoportable levedad del ser,* Círculo de lectores, Barcelona, 1986.

• LÓPEZ ORTEGA, Juan José, "CC C. España (STEDH de 6 de octubre de 2010)a propósito de la protección de la confidencialidad de las informaciones médicas en la doctrina del tribunal constitucional", *Conflicto y diálogo con Europa: las condenas a España del Tribunal Europeo de Derechos Humanos,* [coord. por Rafael Alcácer Guirao, Margarita Beladíez Rojo, José Miguel Sánchez Tomás], Civitas, Cizur Menor, 2013.

• MASHEY, John, "Big Data and the Next Wave of Infrastress: Problems, Solutions and opportunities", *Usenix Annual Technical Conference*, 6-11, Monterry California, junio de 1999.

• MONLEÓN-GETINO, Antonio, "El impacto del *Big-data* en la Sociedad de la Información. Significado y utilidad", *Historia y Comunicación Social. Vol 20, Núm. 2,* 2015.

• MURRAY, Thomas H., "Genetic Exceptionalism and 'Future Diaries': Is Genetic Information Different from other Medical Informatics?", *Rothstein M, ed. Genetic Secrets: Protecting Privacy and Confidentiality in Genetic Era*, Yale University Press, New Haven, 1997.

• ROSEN, Jeffrey, *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, Nueva York, 2000.

• RUIZ MIGUEL, Carlos, "La nueva frontera del derecho intimidad", *Revista de Derecho y Genoma humano*, *Núm. 14*, 2001.

• WILSON, Hilary *Understanding Hieroglyphs: A Complete Introductory Guide, Michael O'mara Books Ltd, Londres,* 1965.

• ZIKOPOLOUS, Paul/ DEROOS, Dirk/ DEUTSCH, Tom/ LAPIS George, *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*, McGraw-Hill, Nueva York, 2012.

65 Vid. ROSEN, Jeffrey, *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, Nueva York, 2000.

66 Vid. KUNDERA, Milan, *La insoportable levedad del ser,* Círculo de lectores, Barcelona, 1986.