Papeles el tiempo de los derechos

EL ACCESO A LOS DATOS RELATIVOS A LA SALUD: CRITERIOS APLICABLES DE ACUERDO CON LA LEY DE TRANSPARENCIA Y A LA LUZ DE LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Juan Manuel López Ulla
Profesor Titular de Derecho Constitucional
Universidad de Cádiz (España)
juanmanuel.ulla@uca.es

Palabras clave: Protección de datos de carácter personal. Datos relativos a la salud. Ley de transparencia. Ley de autonomía del paciente.

Número: 12 Año: 2018

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Manuel Calvo García (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

EL ACCESO A LOS DATOS RELATIVOS A LA SALUD: CRITERIOS APLICABLES DE ACUERDO CON LA LEY DE TRANSPARENCIA Y A LA LUZ DE LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Juan Manuel López Ulla
Profesor Titular de Derecho Constitucional
Universidad de Cádiz (España)
juanmanuel.ulla@uca.es

1. Contexto normativo de la Ley de Transparencia en relación con la protección de datos

El derecho de acceso a la información pública está reconocido en el artículo 105 letra b) de la Constitución española (en adelante, CE), donde se establece que "la ley regulará: (…) b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

El legislador ha dado cumplimiento a este mandato en varias disposiciones: principalmente y con carácter general en el artículo 13 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, y con carácter sectorial en la Ley 27/2006, de 18 de julio, que regula los derechos de

acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente; y en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, que regula el uso privado de documentos en poder de Administraciones y organismos públicos. En consecuencia, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante, LT) no parte "de la nada ni colma un vacío absoluto, sino que ahonda en lo ya conseguido, supliendo sus carencias, subsanando sus deficiencias y creando un marco jurídico acorde con los tiempos y los intereses ciudadanos", como reconoce su Exposición de Motivos.

La LT "tiene por objeto ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias derivadas de su incumplimiento" (artículo 1). Dado que el acceso a la información puede afectar de forma directa a la protección de datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios.

Como es sabido, la ley que desarrolla el artículo 18.4 CE en materia de protección de datos de carácter personal es la Ley Orgánica 15/1999, de 13 de diciembre (en adelante, LOPD), cuyo reglamento de desarrollo fue aprobado por Real Decreto 1720/2007, de 21 de diciembre[1]. El artículo 15 de la LT, que lleva por epígrafe "Protección de datos personales", contiene una serie de reglas que la autoridad competente habrá de observar cuando una persona solicite el acceso a información pública que contenga esta clase de datos. Esta ley no puede contravenir lo dispuesto en aquella normativa básica[2].

[1] Algunos Estatutos de Autonomía reconocen el derecho de acceso, corrección y cancelación de los datos de carácter personal gestionados por las Administraciones radicadas en sus respectivos territorios, a excepción de la Administración periférica del Estado, asumiendo la función de desarrollo legislativo y/o de ejecución de la legislación estatal. Son los de Andalucía (Ley Orgánica 2/2007, de 19 de marzo), Aragón (Ley Orgánica 5/2007, de 20 de abril), Islas Baleares (Ley Orgánica 1/2007, de 28 de febrero), Castilla y León (Ley Orgánica 14/2007, de 30 de noviembre) y Cataluña (Ley Orgánica 6/2006, de 19 de julio). Sobre la protección de datos personales como derecho y título competencial en Andalucía, véanse nuestros comentarios a los artículos 32 y 82 del Estatuto en Cruz Villalón, P. y Medina Guerrero, M.: *Comentarios al Estatuto de Autonomía de Andalucía*. Parlamento de Andalucía, 2012, Vol. I (pp. 516-526) y Vol. II (pp. 1349-1360), respectivamente.

[2] El artículo 13 de la LT entiende por información pública "los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de [esta la ley] y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones".

Además, el legislador español y la autoridad jurisdiccional habrán de observar los Convenios y Tratados internacionales suscritos por España en la materia (artículo 10.2 CE). Así, en el marco de la Unión Europea, su Carta de Derechos Fundamentales reconoce el derecho a la protección de datos en el artículo 8, elevando la protección del mismo al máximo grado. En ese ámbito también hay que tener presente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[3].

Por lo que al Consejo de Europa se refiere, el Tribunal Europeo de Derecho Humanos (TEDH) ha reconocido este derecho en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), que garantiza el derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia: "el mero almacenamiento de datos relativos a la vida privada de un individuo supone una injerencia en el derecho al respeto de la vida privada que garantiza el artículo 8 CEDH"[4]. El principio, pues, es que este precepto protege la información personal que los individuos pueden legítimamente esperar que no debería publicarse sin su consentimiento[5], como por ejemplo, el domicilio, el nombre completo, el nombre tan sólo, cuando del contexto se fácilmente identificable la persona, el correo electrónico, el teléfono, la propia imagen, una grabación de voz, fotografías, vídeos[6]. Al respecto, es interesante el caso *Verlagsgruppe News GmbH y Bobi c. Austria*, una Sentencia que declaró la lesión del artículo 8 por unas fotos tomadas en el apartamento del demandante durante un evento privado y que luego fueron publicadas sin su consentimiento[7].

También, en el ámbito del Consejo de Europa, habrá que observar lo dispuesto en el Convenio n. 108, de 28 de enero de 1981, para la protección de las personas con

[3] Véanse las Sentencias del Tribunal Europeo de Derechos Humanos en los casos *Leander c. Suecia*, n. 9248/71, de 26 de marzo de 1987, y *S. y Marper c. Reino Unido*, n. 30562/04 y 30566/04, de 4 de diciembre de 2008 (Gran Sala).
[4] Entre otras, *S. y Marper c. el Reino Unido*, cit., §§ 41 y; 67 *Flinkkilä y otros c. Finlandia*, n. 25576/04, de 6 de abril de 2010, § 75.
[5] *Flinkkilä y otros c. Finlandia*, cit., § 75; *Saaristo y otros c. Finlandia*, n. 184/06, de 12 de octubre de 2010, § 61,.
[6] Entre otras, *Alkaya c. Turquía*, n. 42811/06, de 9 de octubre de 2012; *Kurier Zeitungsverlag y Druckerei GmbH c. Austria (n. 2)*, n. 1593/06, de 19 de junio de 2012; *Bohlen c. Alemania*, n. 53495/09, de 19 de febrero de 2015, § 45.
[7] N. 59631/09, de 4 de diciembre de 2012, §§ 86, 89-90.

respecto al tratamiento automatizado de datos de carácter personal, firmado en Estrasburgo, y ratificado por España mediante Instrumento de 27 de enero de 1984.

2. Un derecho que no estaba reconocido en la Constitución

El derecho fundamental a la protección de datos de carácter personal no está reconocido expresamente en el artículo 18.4 CE. Lo que ordena este precepto es que el Parlamento apruebe una Ley que limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Fue la Sentencia 292/2000 la que extrajo de este precepto un auténtico derecho fundamental, distinto al derecho a la intimidad reconocido en el artículo 18.1 CE. Pero este reconocimiento fue progresivo. La citada Sentencia terminó de recorrer el camino que con anterioridad las SSTC 254/1993 y 290/2000 habían iniciado.

La Sentencia 254/1993 es la primera que advierte en el artículo 18.4 CE un derecho fundamental[8]. En ella, el Tribunal Constitucional (en adelante, TC) habló de *libertad informática* o *habeas data*, no de "protección de datos", pero sin concebirlo como un derecho autónomo o singular sino como una manifestación de la dimensión positiva que el derecho a la intimidad, reconocido en el párrafo primero de este precepto, tiene[9].

El siguiente paso en la configuración constitucional de este derecho se da con la STC 290/2000, que por primera vez utiliza la expresión "derecho a la protección de datos

[8] STC 254/1993, FJ. 6: "Dispone el art. 18.4 C.E. que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»".

[9] STC 254/1993, FJ. 7: "(…) El uso de la informática encuentra un límite en el respeto al honor y la intimidad de la personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) […]". Esta doctrina se reitera en las SSTC 143/1994 (FJ. 7); 11/1998 (FJ. 4); 94/1998 (FJ. 6) y 202/1999 (FJ. 2).

personales". El Tribunal lo definió como la facultad "de control sobre los datos relativos a la propia persona" que la STC 254/1993 había advertido en el artículo 18.4 CE (FFJJ. 6 y 7) empleando la locución "libertad informática". La STC 290/2000, sin embargo, se extiende un poco más que aquella primera en la configuración de su contenido[10]. También es interesante destacar que mientras la STC 254/1993 había reconocido en el artículo 18.4 CE el derecho a la libertad informática o *habeas data*, concibiéndolo como un derecho instrumental del derecho a la intimidad, reconocido en el párrafo primero del artículo 18, la STC 290/2000 alude por primera vez al carácter singular o "específico" de este derecho (FJ. 11). Cierto es que el TCl no aportó entonces ninguna consideración sobre lo que había querido decir al utilizar este adjetivo, pero sin duda este reconocimiento comenzó a deshacer el nudo que hasta entonces había unido los párrafos uno y cuarto del artículo 18 CE.

La STC 292/2000 representa el tercer y último paso en este proceso progresivo de configuración del derecho. Partiendo de la doctrina vertida en las SSTC 254/1993 y 290/2000, la novedad radica en que por vez primera se aclara la autonomía o singularidad de este derecho, especificando su contenido y subrayando especialmente las diferencias con el derecho a la intimidad, reconocido en el art. 18.1 CE. Concretamente, la STC 292/2000 insiste en que sean íntimos o no, "el derecho fundamental a la protección de datos persigue garantizar a [la] persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (FJ. 6). Esto es, "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o

[10] STC 290/2000, FJ. 7: "[Este derecho] confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos.// En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes".

uso" (FJ. 7)[11].

3. El derecho de acceso a la información pública: nomenclatura del artículo 15 de la Ley de Transparencia

El artículo 15 de la LT regula el acceso a la información pública que contenga datos de carácter personal. Antes de examinar su contenido en relación con los datos personales relativo a la salud de las personas, consideramos conveniente recordar el significado de algunos conceptos clave. Lo haremos brevemente recurriendo a las definiciones que encontramos en el artículo 3 de la LOPD:

En primer lugar, el artículo 15 de la LT se refiere a la información pública que contenga datos personales o de carácter personal. Por tales hemos de entender aquéllos que suministren "cualquier información concerniente a personas físicas identificadas o identificables" [letra a) del artículo 3 LOPD], esto es, personas cuya identidad quede manifiestamente clara o pueda establecerse sin realizar esfuerzos poco razonables[12].

El artículo 15 de la LT protege aquellos datos a los que hace referencia la LOPD, esto es, la información de carácter personal registrada en un suporte físico que la haga susceptible de tratamiento. Este soporte físico es lo que llamamos "fichero", concepto que la LOPD define como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" [letra b) del artículo 3]. Es curioso comprobar que la LT no se

[11] Continúa la STC 292/2000, FJ. 7: "(…). Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.// Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.// En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.// Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele».

[12] En el mismo sentido, el Convenio del Consejo de Europa de 1981 para la protección de las personas en lo que respecta al tratamiento automatizado de datos personales.

refiere expresamente en ningún momento a este concepto, aunque implícitamente está presente.

Cuando en materia de protección de datos personales nos referimos a un fichero, no es preciso que éste sea automatizado. Lo único necesario es que se trate de un soporte físico en el que la información se encuentre organizada de conformidad con algún criterio que permita que los datos en él incorporados puedan ser tratados. Por tanto, una carpeta cualquiera (en papel, por ejemplo) que cumpla con este requisito, también lo es a estos efectos.

Como acabamos de señalar, los datos incorporados al fichero han de poder ser "tratados, Esto significa que deben ser susceptibles de "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" [letra c) del artículo 3 LOPD].

Otro concepto clave, que en el artículo 15 de la LT aparece hasta en siete ocasiones, es el de "afectado". Por tal hemos de entender la "persona física titular de los datos que sean objeto [de] tratamiento (…)" [letra e) del artículo 3 LOPD]. Es él quien debe consentir para que sus datos puedan ser tratados. La LOPD define este "consentimiento" como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen" [letra h) del artículo 3 LOPD].

El consentimiento habrá de ser expreso cuando refiera al tratamiento de datos sensibles o especialmente protegidos (artículo 7 LOPD). En caso contrario, se admite el consentimiento tácito, pero siempre que tal conformidad resulte de manera inequívoca (artículo 6.1 LOPD), pudiendo ser revocado en cualquier momento. Por consentimiento expreso entendemos "aquel que se obtiene de una declaración inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos"13.

[13] Sentencia de la Audiencia Nacional de 24 de marzo de 2006 (rec. 121/2005).

Todas las reglas que el artículo 15 de la LT contiene no serían precisas cuando el acceso se efectúe previa disociación de los datos, señala finalmente su párrafo cuarto. Por "procedimiento de disociación" la LOPD entiende "todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable" [letra f) del artículo 3].

4. El artículo 15 de la Ley de transparencia en relación con los datos relativos a la salud.

4.1. Sobre el consentimiento expreso e informado.

El TC ha subrayado el carácter íntimo y confidencial de cualquier información relativa a la salud física o psíquica de la persona[14]. El tratamiento de estos datos exige bien la autorización del titular, bien que una ley lo permita.

El requisito que acabamos de señalar está previsto en el artículo 7.3 LOPD, que califica de "datos especialmente protegidos" aquellos relativos a la salud. Este precepto ordena que estos datos (además de aquellos que hagan referencia al origen racial y a la vida sexual) sólo puedan ser recabados, tratados y cedidos, cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente. En consecuencia, el apartado segundo del artículo 15.2 LT *in fine* no introduce nada nuevo cuando señala que "el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley".

El artículo 5.1, letra g) del Reglamento de desarrollo de la LOPD define los datos referidos a la salud de la siguiente manera: se trata de "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo[15]. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje

[14] En este sentido, la STC 159/2009, FJ. 3, que al efecto se apoya en la STC 70/2009, FJ 2.

[15] El artículo 8 LOPD lleva por epígrafe "datos relativos a la salud" pero en él no encontramos ninguna definición. Dice así: "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión [de datos], 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". Sobre los artículos 7.6 y 8 LOPD, véase nuestro trabajo, "El consentimiento del afectado en el tratamiento de datos relativos a la salud", en Troncoso Reigada, A.: *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, *cit.*., pgs. 671 a 684.

de discapacidad y a su información genética". La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica es otra norma a tomar en cuenta en la materia. Su artículo 3 contiene una serie de definiciones que a nuestro propósito son relevantes. Por "documentación clínica" entiende "el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial"; por "historia clínica", "el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial"; y por "Información clínica", "todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla".

El contenido de la historia clínica se describe con mayor detalle en el artículo 14 de la Ley 41/2002: "1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.// 2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información (…)". El artículo 15 de la Ley añade que: "1. La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada. 2. La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud (…)".

Otras normas que reconocen el carácter confidencial de los datos relativos a la salud son, el artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad[16] y especialmente el artículo 7.1 de la Ley 41/2002, reguladora de la autonomía del paciente, antes citada[17].

En aras de esa confidencialidad, si bien en principio el paciente puede acceder a la documentación de su historia clínica (art. 18.1 de la Ley 41/2002), no puede, sin embargo, ejercitar este derecho cuando ello suponga un perjuicio para terceras personas, cuyos datos figuren en ella y fueren recabados en razón del interés terapéutico para el paciente. Igualmente, este derecho podrá quedar limitado cuando fuera en perjuicio de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas (art. 18.3 de la Ley 41/2002).

Por lo que se refiere al acceso a la historia clínica de un paciente fallecido, el artículo 18.4 de la Ley 41/2002, lo permite "a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite". El precepto continúa señalando que en el caso de que el acceso a la historia clínica del fallecido fuera necesario para preservar la salud del tercero que así lo solicitara, dicho acceso se limitará a los datos que al efecto fueran pertinentes. En cualquier caso no se proporcionará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni a aquella que pueda perjudicar a terceros.

Cuando de acceso a datos relativos a la salud se trata, el consentimiento por parte del afectado debe ser eficaz o informado. No lo será así cuando la autorización se otorgue sin pleno conocimiento de lo que se está autorizando, sea por incapacidad física o

[16] El artículo 10.3 reconoce el derecho "a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público", siendo el mismo aplicable igualmente a los centros sanitarios privados, conforme a lo dispuesto en el artículo 10.15 de la propia Ley.

[17] Art. 7.1 de la Ley 41/2002: "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». Entre los principios básicos que inspiran a esta ley, el art. 2.1 señala que "la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica".

psíquica del titular, porque la información suministrada no haya sido exacta o completa, o porque se haya ofrecido de forma ininteligible.

Además, la autorización ha de ser específica, esto es, el afectado debe consentir respecto de una situación concreta y bien definida, por lo que una manifestación general de voluntad que, por ejemplo, permitiera acceder a determinados datos médicos del paciente en una historia médica electrónica, no legitimaría las posteriores transferencias de esos datos médicos del pasado y del futuro a otros profesionales médicos que puedan intervenir en el tratamiento. Cualesquiera que sean las dificultades, el responsable del tratamiento debe poder probar en todos los casos, en primer lugar que obtuvo el consentimiento explícito del interesado y, en segundo lugar, que ese consentimiento explícito se dio en base a una información suficientemente exacta.

Igualmente hay que recordar que consentir el acceso a estos datos relativos a la salud (artículo 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros. La cesión de los mismos a un tercero supone una nueva posesión y uso que requerirá el consentimiento del interesado. Así lo exige el artículo 11.3 de la LOPD: "será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se solicite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar". O en palabras del TC: "el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta"[18].

Obviamente, tampoco habrá consentimiento eficaz cuando el tercero al que se cedan los datos supere o exceda el ámbito de la autorización concedida, o como dice el TC, cuando se "subviertan los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" [STC 196/2004, FJ. 2, citada por la STC 159/2009,

[18] STC 292/2000, FJ. 13.

FJ. 3, apdo. c)].

4.2. El acceso sin necesidad del consentimiento expreso del afectado

En el epígrafe anterior hemos visto que el derecho de acceso a ficheros que contienen datos relativos a la salud sólo es posible previo consentimiento expreso del afectado o cuando una norma con rango de Ley así lo permita (artículo 15.1.2 de la LT). En este epígrafe nos centraremos en este segundo caso, y recordaremos alguna excepción más que establece en la LOPD.

La posibilidad de que una norma con rango de ley prevea el acceso sin necesidad de contar con el consentimiento expreso del afectado no es ninguna novedad pues ya se contemplaba en el artículo 7.3 LOPD. Como de un límite a un derecho fundamental se trata, este precepto exige que tal excepción esté justificada por razones de interés general, requisito que también habremos de tener presente cuando nos movamos en el ámbito de la LTLT. Al efecto, el TC ha recordado que "las posibles limitaciones del derecho fundamental a la intimidad personal deberán estar fundadas en una previsión legal que se justifique por tener un objetivo compatible con la Constitución, que sea proporcionada y que exprese con precisión todos y cada uno de los presupuestos materiales de la medida limitadora (STC 292/2000, de 30 de noviembre, FJ. 16; 70/2009, de 23 de marzo, FJ. 3), pues lo que impide el artículo 18.1 CE son las injerencias en la intimidad arbitrarias o ilegales»"[19]. Repasemos brevemente estos requisitos:

1.- Legitimidad constitucional del fin (juicio de idoneidad): la medida limitadora del derecho debe perseguir un objetivo congruente con la Constitución. No puede "ser calificada de ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos, siempre y cuando se respete el contenido esencial del derecho (STC 292/2000, de 30 de diciembre, FJ. 9, y ATC 212/2003, de 30 de junio) (…)" (STC 159/2009, FJ. 3).

[19] STC 159/2009, FJ. 3, apdo. c), que al efecto cita las SSTC 57/1994, FJ. 6; 143/1994, FJ. 6; 198/2004, FJ. 8; 25/2005, FJ. 6; y 70/2009, FFJJ. 3 y 5.

Es interesante al respecto el Informe Jurídico de la Agencia Española de Protección de Datos 0400/800 que permite a un facultativo acceder a la historia clínica de uno de sus pacientes con la finalidad de formular alegaciones en el expediente disciplinario que se le había incoado. A juicio de la Agencia, el derecho fundamental a la defensa del presunto infractor legitimaría ese acceso, limitado al ámbito del procedimiento administrativo abierto cuando el órgano instructor del mismo considere que efectivamente la información contenida en la historia clínica pueda resultar relevante para la resolución del expediente.

2.- La Ley deberá concretar de qué medidas restrictivas se trata: no se pueden establecer límites imprecisos o extensivos que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga (STC 292/2000, FJ. 11). La STC 49/1999, FJ. 4, ya señaló en relación justamente con la protección del derecho fundamental a la intimidad, que toda injerencia exige de modo "inexcusable" una previsión legal que "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención"; ha de poseer lo que en otras ocasiones el TC ha denominado cierta "calidad de Ley"[20].

3.- Principio de proporcionalidad: La legitimidad del fin perseguido no justifica la intromisión si la medida restrictiva del derecho resulta desproporcionada. No lo será cuando aquella persiga un fin legítimo de un modo idóneo, necesario y ventajoso desde la perspectiva constitucional. O lo que es lo mismo, sólo resulta proporcionada la medida restrictiva del derecho si no existen otras medidas menos gravosas que, sin imponer sacrificio alguno del derecho fundamental a la intimidad, o con un menor grado de sacrificio, puedan ser igualmente aptas para conseguir el fin constitucionalmente perseguido; o cuando la medida proporcione más beneficios que ventajas para el interés general que perjuicios para otros bienes o valores.

Por lo que a la historia clínica se refiere, es preciso señalar que si bien el artículo 16 de la Ley 41/2002 permite a los profesionales que asistan al paciente el acceso a los datos que en ella se contienen, dicho acceso estará modulado por el principio de proporcionalidad que consagra en el artículo 4.1 de la Ley Orgánica 15/1999, debiendo

[20] SSTC 49/1999, FJ. 5; 169/2001, FJ. 6; 184/2003, FJ. 2; 70/2009, FJ. 4.

en consecuencia quedar limitado al conocimiento de los datos que efectivamente resulten necesarios para el cumplimiento de la finalidad que justifique dicho acceso, sin que deba extenderse a otros que no reúnan tal vinculación. La recogida y manejo de los datos sobre la salud debe obedecer estrictamente al propósito legítimo para el que fueron recabados, sin que en ningún caso puedan ser tratados para una finalidad distinta ni cedidos sin el conocimiento del afectado[21].

Además de la autorización *ope legis* a la que hace referencia los artículos 15.1.2 de la LT, y 7.3 LOPD, tampoco será necesario el consentimiento expreso del afectado en los dos supuestos contemplados en el art. 7.6 LOPD:

1. Cuando la información "resulte necesari[a] para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto" (art. 7.6 LOPD, párrafo primero).

2. Cuando el acceso "sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento" (art. 7.6 LOPD, párrafo segundo).

En relación con el artículo 7.6.1 LOPD, recordaremos que requisito ético de confidencialidad de la profesión médica se estableció por primera vez en el "juramento hipocrático" *("Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no deba ser público, manteniendo estas cosas de manera que no se pueda hablar de ellas"),* y fue confirmado posteriormente por la Declaración de Ginebra de la Asociación Médica Mundial (1948). Protege la información obtenida por los profesionales sanitarios en el curso del tratamiento de un paciente. El uso de esta información se permite sólo dentro de los límites del contrato de tratamiento. Esta relación de confidencialidad excluye a cualquier tercero, incluso a otros profesionales sanitarios, a menos que el paciente haya autorizado la transmisión de sus datos o esto se prevea especialmente por ley. En caso de que surja la necesidad de

[21] En este sentido, los artículos 15.2 y 16 de la Ley 41/2002.

que personal no médico trate estos datos personales sensibles, este personal también deberá estar sujeto a normas vinculantes que garanticen al menos un nivel equivalente de confidencialidad y protección.

En el Ordenamiento español, el acceso a la historia clínica en el en el ámbito de un determinado centro sanitario está limitado al propio personal sanitario que preste asistencia al paciente, a fin de garantizar su adecuado diagnóstico y tratamiento (artículo 16.1 de la Ley 41/2002)[22]; y al personal de administración y gestión, exclusivamente en lo que resulte necesario para el ejercicio de sus propias funciones[23]. Unos y otros están sujetos al deber de secreto[24]. Al efecto, el artículo 10.5 del Reglamento de la LOPD señala que "no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".

El segundo párrafo del artículo 7.6 reproduce lo que señalaba el derogado artículo 8.2 c) de la Directiva 95/46/CE[25]. Al respecto, el Documento de Trabajo sobre Protección de Datos del artículo 29 (00323/07/ES WP 131) advierte que esta excepción sólo puede aplicarse a un pequeño número de casos de tratamiento y no puede utilizarse en absoluto para justificar el tratamiento de datos médicos personales con fines distintos del tratamiento del interesado, como por ejemplo realizar investigaciones médicas generales que sólo darán resultados en el futuro[26].

---

[22] Al respecto, el Informe 656/2008, de 7 de enero de 2009 de la Agencia Española de Protección de Datos señala que "en relación con el personal sanitario que esté prestando atención al paciente, no puede, sin más, establecerse una aplicación restrictiva de las normas reguladoras del acceso a la historia clínica que pudiera perjudicar la salud del paciente, dada la finalidad que para la propia historia clínica establece la Ley 41/2002. En consecuencia, el acceso a los datos por parte del personal sanitario que esté asistiendo al paciente (como por ejemplo el personal de enfermería, que tiene la condición de personal sanitario conforme a lo dispuesto en la Ley 44/2003, de 21 de noviembre, de Profesiones Sanitarias) siempre será posible cuando se lleve a cabo con la finalidad de "garantizar una asistencia adecuada al paciente" y en tanto los datos de la historia constituyan un "instrumento fundamental para su adecuada asistencia" en cada caso concreto (art. 16.1 de la Ley 41/2002)".

[23] Art. 16.4 de la Ley 41/2002: "El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones".

[24] Art. 16.6 de la Ley 41/2002.

[25] Señala el artículo 8.2 c) de la Directiva que lo dispuesto en el apartado 1 no se aplicará cuando "el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento".

[26] Supongamos que un interesado ha perdido la consciencia después de un accidente y no puede dar su consentimiento para la revelación necesaria de alergias conocidas. En el contexto de una historia médica

Por último, también habrá que tener presente lo dispuesto en el párrafo tercero del artículo 16 de la Ley 41/2002, que hay que leer de acuerdo con lo dispuesto en el artículo 11 de la LOPD respecto de la cesión de datos: "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[27], y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines 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[28]. 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".

El párrafo cuarto del artículo 15 de la LT señala que las reglas establecidas en sus tres primeros párrafos no serán aplicables cuando el acceso se efectúe previa disociación de los datos de carácter personal de modo que la identificación de las personas afectadas no sea posible. Como esta norma ya se contiene en el art. 11.6 LOPD, pensamos que nada hubiera pasado si no se hubiese incorporado al art. 15 de la LT: "Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores"[29].

---

electrónica, esta disposición permitiría el acceso a la información almacenada en ella a un profesional de la salud con el fin de extraer datos sobre alergias conocidas del interesado, que pueden resultar decisivos para el tratamiento elegido. Así lo señala el Documento 00323/07/ ES WP 131,

[27] Al respecto véanse los artículos 8, 7.6 y 11.2 apartados d), f) y e) de la LOPD.

[28] Salvo en los casos señalados en el artículo 11.2 de la LOPD, el consentimiento eficaz del interesado es necesario para que sus datos puedan ser comunicados a un tercero.

[29] Esos apartados anteriores a los que se refiere el art. 11.6 de la LOPD hacen referencia a la posibilidad de que los datos objeto de tratamiento puedan ser comunicados a un tercero.

5. Principios extraíbles de la jurisprudencia del Tribunal Europeo de Derechos Humanos

El TEDH ha subrayado en no pocas ocasiones que la protección de la información personal relativa al paciente forma parte del derecho al respeto de la vida privada y familiar reconocido en el artículo 8.1 CEDH, advirtiendo que la legislación interna de los Estados firmantes debe prever al efecto las garantías necesarias que impidan toda comunicación o divulgación de datos de carácter personal relativos a la salud que pudieran lesionar este derecho. Es un principio vital o esencial respetar no sólo la privacidad del paciente sino también preservar la confianza de éste con el médico y con el sistema de salud en general[30].

El artículo 8.2 del Convenio señala en qué casos el derecho reconocido en párrafo primero podrá quedar limitado. Dice así: "no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Por tanto, cuando la injerencia esté prevista en la ley, tenga un objetivo legítimo y se considere una medida necesaria en una sociedad, la demanda será desestimada o inadmitida a trámite por manifiestamente infundada[31].

[30] Véanse, entre otros, *I. c. Finlandia*, de 17 de julio de 2008, n. 20511/03, § 38; *caso*; *Z. c. Finlandia*, de 25 febrero 1997, §§ 95 y 96; *K.H. y otras c. Eslovaquia*, de 28 de abril de 2009, § 55.

[31] *Chave née Jullien c. Francia*, n. 14461/88, Decisión de inadmisión de la Comisión Europea de Derechos Humanos de 9 de julio de 1991: La parte demandante consideró que el registro de su internamiento en un psiquiátrico constituía una injerencia en su vida privada, solicitando que fuera eliminada. La Comisión declaró la demanda inadmisible por ser manifiestamente infundada. Al efecto, observó que el registro de la información relativa a los enfermos mentales no sólo servía para garantizar el buen funcionamiento del servicio público hospitalario sino también para proteger los derechos de los propios pacientes, especialmente en los casos de internamiento obligatorio. Advirtió que la información controvertida estaba protegida por normas de confidencialidad adecuadas, reconociendo que estos documentos en modo alguno eran accesibles al público sino exclusivamente a determinadas personas bien identificadas. Tampoco constató que la medida adoptada fuera desproporcionada con respecto al objetivo legítimo perseguido: la protección de la salud.

El primer requisito, como vemos, es que el límite esté previsto en una ley. Al respecto, el TEDH exige que ésta habrá de especificar con claridad en qué casos, por qué razón, y con qué medida o alcance los datos han de recopilarse[32].

El segundo requisito consiste en que, a la luz de las circunstancias del caso concreto, y respetando el margen de apreciación de los Estados parte, la injerencia denunciada se considere necesaria en una sociedad democrática, para lo cual, el TEDH habrá de comprobar si el límite se justificó en algunas de los motivos expresamente señalados en el artículo 8.2 del Convenio, si obedeció a una necesidad social imperiosas, si las razones ofrecidas por las autoridades nacionales fueron pertinentes y suficientes y si la restricción implementada fue proporcional al objetivo legítimo perseguido.

Internet han revolucionado el mundo de la medicina para bien, pero en cuanto al carácter reservado de dicha información, las amenazas son reales. Las historias clínicas en soporte informático o el acceso electrónico a las órdenes de prescripción de medicamentos son un ejemplo evidente. Hasta la fecha no se ha dictado ninguna resolución que concretamente haya abordado la necesidad de preservar los datos personales referentes a la salud en relación con los avances de la ciencia de la comunicación[33], pero de la jurisprudencia del Tribunal de Estrasburgo en relación con esta información se derivan algunos principios que, llegado el caso, serían igualmente aplicables. Veamos algunos de los casos más relevantes que terminaron con una Sentencia estimatoria, esto es, declarando la violación del artículo 8 del Convenio.

En primer lugar recordaremos cuatro casos en relación con datos relativos a la salud que fueron revelados al formar parte de la documentación incorporada a diversos expedientes judiciales:

[32] *L.H. c. Letonia*, n. 52019/07, de 29 de abril de 2014, §§ 56 a 60: el TEDH declaró la violación del artículo 8.2 del Convenio porque la ley aplicable no precisaba con claridad el alcance de los datos privados que podía recopilar un organismo estatal, ni la relevancia o importancia de los mismos, lo que permitió la recolección indiscriminada de los datos médicos del demandante. Esta Sentencia se apoya al respecto en las Sentencias dictadas en los casos *M.S. c. Suecia*, n. 34209/96, de 2 de julio de 2002, §§ 38, 42 y 43,y *L.L. c. Francia*, n. 7508/02, de 10 de octubre de 2006§ 46.

[33] El TEDH ha dictado alguna resolución en relación con las nuevas tecnologías y la libertad de expresión. Por todas, *Delfi AS c. Estonia*, n. 64569/09, de 16 de junio de 2015 (Gran Sala); *Pihl c. Suecia*, n. 74742/14, decisión de inadmisión de 7 de febrero de 2017.

Z. c. Finlandia, n. 22009/93, de 25 de febrero de 1997: la demandante acude al TEDH quejándose de que las autoridades jurisdiccionales habían ordenado que la información sobre su salud contenida en una Sentencia tan solo fuera confidencial durante diez años. Considerando que los datos médicos de la demandante habían pasado a formar parte de un proceso penal contra su ex marido sin su consentimiento, el TEDH declara que la decisión de revelar todo el expediente transcurridos diez años no se sustentaba en razones suficientes para anular el interés de la demandante en que permanecieran secretos por un período más largo. Entendiendo que la protección de los datos médicos es esencial para preservar el derecho al respeto a la vida privada y familiar, el Tribunal declara que la injerencia no era consideraba necesaria en una sociedad democrática (véanse en particular los §§ 94, 112 a 114).

Panteleyenko c. Ukrania, n.11901/02, de 29 de junio de 2006: el demandante denuncia que un procedimiento judicial revela información confidencial sobre su estado mental y el tratamiento psiquiátrico al que había estado sometido. El TEDH declara la violación del derecho del demandante al respeto de su vida privada personal y familiar, reconociendo que tal información no era imprescindible en relación con el objeto del procedimiento (§ 61).

L.L. c. Francia, n. 7508/02, de 10 de octubre de 2006: el demandante se quejó de no haber dado su consentimiento para que los Tribunales revelaran, en el marco de un procedimiento de divorcio, datos relativos a su salud, concretamente su adicción al alcohol. El TEDH advierte que esta información no resultó determinante en aquel procedimiento judicial, pues los órganos jurisdiccionales hubieran llegado a la misma conclusión sin necesidad de ellos. Por esta razón, el TEDH reconoce la violación del derecho a la vida privada y familiar, reconocido en el artículo 8 del Convenio, entendiendo que la injerencia en el derecho a la vida privada no estaba justificada. A mayor abundamiento, el TEDH señala que el Derecho interno no preveía garantías suficientes en lo que se refiere a la utilización de datos personales en este tipo de procedimientos (véanse en particular los §§ 40, 43, 44, 46).

Avilkina y otros c. Rusia, n. 1585/09, de 6 de junio de 2013: los demandantes son el Centro Administrativo de los Testigos de Jehová en Rusia, así como tres miembros de este grupo religioso. Denuncian la divulgación de sus expedientes médicos a las

autoridades judiciales rusas tras su negativa a ser transfundidos durante el tiempo que estuvieron en hospitales públicos. En el marco de una investigación sobre la legalidad de las actividades de esta organización, las autoridades del Ministerio Público habían ordenado a todos los hospitales de San Petersburgo que denunciaran las negativas de transfusiones de sangre de los testigos de Jehová. El TEDH declaró que los demandantes no eran sospechosos o acusados en ningún proceso penal y que el fiscal simplemente estaba realizando una investigación sobre las actividades de una organización religiosa a raíz de las quejas recibidas en su oficina. En consecuencia, el TEDH considera que no había ninguna necesidad social urgente de solicitar la divulgación de la información médica confidencial relativa a los demandantes. A mayor abundamiento, el TEDH toma en consideración que el fiscal disponía de otras opciones para dar seguimiento a las denuncias que había recibido sobre esta organización. Por todo ello estima la demanda y declara la violación del artículo 8 de la Convención (véanse en particular los §§ 53 y 54).

En relación con la necesidad de salvaguardar la confidencialidad de los datos incorporados a la historia clínica, es interesante el caso *I. c. Finlandia*, n. 20511/03, de 17 de julio de 2008: La demandante, una enfermera con VIH, sospechaba que personas no autorizadas habían accedido a su historia clínica. Si bien la estricta aplicación del Derecho interno hubiera garantizado la confidencialidad de esa información, la organización administrativa del hospital no permitió aclarar si la información contenida en el expediente de la demandante se había entregado a personas no autorizadas. Además, el TEDH advierte que en el momento de los hechos, la historia clínica podía ser consultada por personal no relacionado directamente con el tratamiento. El Tribunal declaró la violación del artículo 8 del Convenio entendiendo que el hospital no había garantizado de manera efectiva los datos médicos de la demandante[34].

Por último, sobre el derecho de las personas a acceder a los datos que pudieran ser relevantes para su salud, debiendo el Estado articular un procedimiento efectivo al efecto, podemos señalar las siguientes dos Sentencias:

[34] Otro caso en el que un periódico revela que determinadas personas estaban infectadas por el SIDA es *Biriuk c. Lituania*, n. 23373/03, de 25 de noviembre de 2008.

Roche c. el Reino Unido, n. 32555/96, de 19 de octubre de 2005 (Gran Sala): El demandante salió del ejército británico a finales de los años sesenta. En la década de 1980 su salud se deterioró hasta el punto de que fue declarado incapaz para trabajar. Sus afecciones fueron consecuencia de su participación en pruebas de gas mostaza llevadas a cabo por las Fuerzas Armadas británicas en la década de los sesenta. El demandante se queja de que no le hubiesen dejado acceder a la información pertinente que le hubiera permitido evaluar el riesgo al que había estado expuesto durante su participación en dichas pruebas. El TEDH declaró la violación del artículo 8 del Convenio, reconociendo que el Reino Unido debiera haber cumplido con su obligación positiva de proporcionar un procedimiento efectivo y accesible que hubiese permitido al demandante acceder a todos los documentos pertinentes y a la información adecuada que le hubiera permitido evaluar cualquier riesgo al que hubiese estado expuesto durante su participación en tales pruebas (§§ 162 y 167 y 169, citando al efecto, *McGinley y Egan*, § 101; y *Guerra y otros*, § 60).

K.H. y otros c. Eslovaquia, n. 32881/04, de 28 de abril de 2009: Las demandantes creen que han sido esterilizadas, pues ninguna puede concebir tras haber recibido un tratamiento ginecológico. Se quejan de que las autoridades sanitarias no les han permitido obtener copias de sus historias clínicas. Por este motivo (el no acceso a esta información), el TEDH declara la violación del artículo 8 del Convenio, pues tal negativa no fue justificada debidamente. Y añade que para evitar cualquier esta lesión, hubiera sido suficiente con que el legislador hubiese especificado con exactitud las personas y los casos con acceso a esa información. (§§ 55, 56 58).