Derecho y Realidad
Núm. 19 • I semestre de 2012
Facultad de Derecho y Ciencias Sociales, UPTC
ISSN: 1692-3936

VIH y derechos fundamentales: el derecho a la protección de datos personales y el registro obligatorio de los portadores del VIH en España*

HIV and fundamental rights: the right to protection of personal data and the compulsory registration of HIV carriers in Spain

Ana Garriga Domínguez**

Resumen

En este artículo estudiamos la regulación del registro obligatorio de los portadores del VIH en España, desde la perspectiva del derecho fundamental a la protección de datos personales del artículo 18.4 de la Constitución española. Además nos referimos a determinados problemas derivados del procesamiento de datos personales en la sociedad tecnológica, que pueden resultar relevantes para situar la problemática del registro de tan especial dato personal. Es relevante señalar que el derecho a la protección de datos personales, por incidir tan directamente en el núcleo de la personalidad, de la libertad y de la dignidad individual,

* Este trabajo enmarca dentro del Programa COSOLIDER-INGENIO 2010 HURI AGE «El tiempo de los derechos».
** Profesora titular de Filosofía del Derecho Universidad de Vigo.

se configura como un derecho cuya violación podría llevar aparejada en muchas ocasiones la violación de otros derechos fundamentales.

Palabras clave

SIDA, registro obligatorio de portadores de VIH, derecho a la protección de datos personales.

Abstract

In this paper we study the regulation of compulsory registration of HIV carriers in Spain, from the perspective of the fundamental right to the protection of personal data of article 18.4 of the Constitution. We also refer to certain problems of processing personal data in the technological society, wich may be relevant to situate the issue of so special personal data registration. It is relevant to point out that the right of protection of personal data, as directly affect the core of personality, freedom and individual dignity, is configured as a right whose violation could be accompany on many occasions with the violation of other fundamental rights.

Key words

AIDS, compulsory registration of HIV carriers, right to protection of personal data.

Antes de entrar en el análisis de la regulación del registro obligatorio de los portadores del VIH en España y su conflicto con determinados derechos fundamentales, he de advertir que este será abordado desde la perspectiva del derecho fundamental a la protección de datos personales del artículo 18.4 de la Constitución española. Este enfoque nos obligará a tener presente determinadas cuestiones relativas a la configuración constitucional del derecho a la protección de datos personales, así como a los derechos y a los bienes afectados por el tratamiento de la información personal, particularmente el dato personal que se refiere al padecimiento del SIDA o a la condición de portador del VIH. Por ello, resulta necesario referirse a determinados problemas derivados del procesamiento de datos personales en la sociedad tecnológica y que pueden resultar relevantes para situar la problemática del registro de tan especial dato personal. Igualmente resulta relevante señalar que, por incidir tan directamente en el núcleo de la personalidad, de la libertad y de la dignidad individual, «ya que el derecho a la protección de datos personales está en estrechísima conexión con la capacidad de desarrollo de la propia personalidad y de elección libre de los planes de vida», se configura como un derecho cuya violación podría llevar aparejada en muchas ocasiones la violación de otros derechos fundamentales. Ello es así porque este derecho protege la libertad de elección de las personas, su derecho a no ser discriminadas y se encuentra directamente engarzada con la propia idea de dignidad y autorrealización humanas.

La concepción del derecho a la protección de datos personales como un derecho instrumental para la garantía de otros derechos fundamentales, se encuentra expresamente recogida en el texto constitucional español. En el artículo 18.4 se establecen limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos de las personas. Se mencionan expresamente dos de los derechos que podrían verse amenazados por un uso abusivo e ilegítimo de las nuevas tecnologías de la información: los derechos al honor y a la intimidad personal y familiar; pero otros como la libertad ideológica o religiosa, la libertad sindical, el derecho a no ser discriminado, la presunción de inocencia o el derecho a acceder en condiciones de igualdad a la función pública, por ejemplo, podrían resultar igualmente amenazados.

Cuando se analiza la incidencia del tratamiento de datos personales en la dignidad, libertad, igualdad o en los derechos fundamentales de las personas se suele destacar, que a diferencia de otros procesos tradicionales, el uso de las nuevas tecnologías de la información y de la comunicación (TIC) ha supuesto mayores amenazas a la libertad y derechos de los ciudadanos que provienen, en primer lugar de la capacidad de acumular informaciones personales que tienen entidades privadas de toda índole, así como las distintas administraciones públicas. Se puede acumular sin límite la información y recabarla en cuestión de segundos con independencia de la distancia a la que se encuentre. De este modo nos

encontramos con que *«nuestra vida individual y social corren (…) el riesgo de hallarse sometidas a lo que Frosini ha calificado, con razón, de «juicio universal permanente»»* (citado por Pérez, 1992, p. 104). Desde el primer momento, una de las aplicaciones más importantes de la informática ha sido el tratamiento y la elaboración de la información, al propiciar inmensas posibilidades de acumulación y manipulación de toda clase de datos, incluidas las informaciones sobre personas. En el año 1884, Herman Hollerith, a quien se considera el precursor del tratamiento automatizado de la información sobre personas, creó la primera empresa[1] de procesamiento automático de información en el mundo, revolucionando de manera radical el análisis de la información del censo. Desarrolló un sistema de cómputo mediante tarjetas perforadas en las que los agujeros representaban el sexo, la edad o raza, entre otros. Gracias a la máquina tabuladora de Hollerith, el censo en Estados Unidos de 1890 se realizó en dos años y medio, cinco menos que el censo de 1880 (Ifrah, 2001, p. 180). La utilización de tarjetas perforadas en el procesamiento de datos permitía clasificarlas. De esta forma era posible saber cuántas tarjetas cumplían determinados requisitos, por ejemplo, el número de personas de un determinado sexo, raza, estado civil y edad que vivían en una localidad. Posteriormente, su invento se utilizó para elaborar y organizar estadísticas sanitarias en algunas ciudades y en el ejército (Black, 2001, p. 21)[2].

En el año 1978 y de manera muy expresiva, James Martin explicaba cómo, en la sociedad de las telecomunicaciones, los seres humanos nos podemos sentir como osos polares a los que se les haya conectado un radiotransmisor en miniatura que envíe continuas señales a un satélite, que puedan ser registradas y seguidas desde un ordenador. Pues, la informática puede hacer nuestras vidas tan visibles para quienes controlan los grandes bancos de información personal como lo son para nosotros los peces de colores que tenemos en una pecera (Martin, 1978, p. 250). Once años antes, Alan F. Westin daba cuenta de los millones de datos sobre personas que determinadas entidades y organismos en Estados Unidos tenían en su poder y como más y más información estaba siendo reunida y usada por corporaciones, asociaciones, universidades, colegios públicos y agencias gubernamentales (Westin, 1970, p. 159). Un lugar común para los estudiosos del impacto de las tecnologías de la información en las libertades es citar la antiutopía orwelliana del «Gran

---

1 H. Hollerith, fundó en 1896 la Tabulating Machine Company, empresa precursora de la que en 1924 se denominaría International Business Machines Corporation (IBM).

2 Las máquinas diseñadas por Hollerith fueron utilizadas por los nazis en Alemania para elaborar el censo de 1933. El uso de las tarjetas perforadas permitió elaborar una ficha informatizada de cada persona internada en los campos de exterminio. A cada categoría de personas, se le asignaron determinados códigos numéricos en las tarjetas perforadas. Había hasta 16 categorías diferentes que se clasificaban en función de los agujeros de las tarjetas: el agujero 3 significaba homosexual, el 9 antisocial, el 12 gitano y el número 8, judío. Sin duda, el uso de las tarjetas perforadas fue de suma utilidad para la localización y clasificación de los grupos de personas que posteriormente serían víctimas del genocidio nazi. (Black, 2001, p. 21). También, Barceló (2008, p. 91).

Hermano», descrita en su obra 1984, y es que las posibilidades de indagación, manipulación, control y persuasión de masas de las tecnologías de la información son de tal entidad, que esta sería plenamente realizable.

Por otra parte, el uso exclusivamente del perfil obtenido a través del tratamiento de datos personales en la toma de decisiones que afecten a un individuo podrá significar su discriminación en muchas de las actividades de la vida cotidiana. Destaca François Rigaux (1990, p. 597 y ss.), que las modernas técnicas de penetración en las aptitudes profesionales o de comportamiento individual se apoyan hoy, en los métodos informáticos que establecen correlaciones entre determinadas características y comportamientos concretos a los que se les confiere una apariencia de rigor científico. Tales previsiones serán, generalmente, discriminatorias y, sobre todo porque, «*en la creencia de descubrir en el sujeto ciertos signos anunciadores de su comportamiento futuro, el perfil instaura una forma de determinismo incompatible con el atributo más preciado de la libertad, la elección de un futuro autodeterminado*» (1990). Estos efectos perjudiciales son más evidentes en aquellos casos en los que el ciudadano aparece identificado en relación con unos hechos o una situación determinados, incorporándose su identidad y sus datos personales a las denominadas *listas negras*[3]. Se trata de un fenómeno muy extendido y de variada naturaleza y contenido (listas de morosos, de infracciones criminales o administrativas, de carácter laboral, de negligencias cometidas en el ámbito profesional, de carácter ideológico o sobre comportamientos políticos, sobre índices de peligrosidad de los individuos, ficheros sobre conductas consideradas inadecuadas por determinados sectores sociales, sobre datos adversos de los candidatos a un puesto de trabajo, sobre datos relativos a la salud, sobre informaciones genéticas, etc.), pero que tienen en común que la inclusión en alguna de estas listas va a implicar, generalmente, consecuencias adversas y perjudiciales para las personas incluidas en el fichero, consistentes en la mayoría de los casos en su discriminación al excluirlas de la posibilidad de acceso a un determinado bien o servicio o, también, en un daño directo a su reputación.

El uso desviado de la tecnología de tratamiento de datos personales supone claros peligros para la libertad, para el derecho a no ser discriminado y, asimismo, para la propia dignidad e identidad personal. El ser humano pasa a ser mero objeto de información, dejando de ser un ser dotado de dignidad y sujeto de derechos fundamentales[4]. Como ya se ha señalado, desde el principio, una de las características

---

[3] Vid. El Documento de Trabajo sobre listas negras, adoptado el 3 de octubre de 2002 por el Grupo de Trabajo sobre Protección de Datos de la Unión Europea (http://europa.eu.int/comm/privacy).

[4] La idea de dignidad significa asumir que *«la persona es un fin que ella misma decide (...), que no tiene precio y que no puede ser utilizada como medio»*. La vinculación de la dignidad con la idea de autonomía tiene dos momentos: *«autonomía que significa capacidad de elección, libertad psicológica, el poder de decidir libremente, pese a los condicionamientos y limitaciones de nuestra condición (...). En el segundo momento, autonomía significa libertad o independencia moral».* (Peces-Barba, 2002, p. 65-66).

básicas de los ordenadores fue la de incrementar exponencialmente las posibilidades del almacenamiento de información personal. El desarrollo de las tecnologías de la información, hizo posible recoger y conservar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizando sobre él un auténtico catálogo de su vida, a través de la interrelación de todos los datos existentes, con independencia de que se encuentren en archivos distintos, relativos a diferentes etapas de su vida, o que estos hubieran sido recogidos incluso en lugares lejanos. El progreso tecnológico propugna la abolición de toda privacidad de la vida individual, expuesta ahora a toda forma de inspección y violación (Frasoni, 1982, p. 168).

Además, cuando se registran las denominadas informaciones sensibles, los riesgos apuntados se incrementan exponencialmente. Las informaciones sensibles son aquellas que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana. Por ello, las posibles agresiones a la libertad, a la intimidad, las posibilidades de ser discriminado o cualquier otra contra el ejercicio de los derechos fundamentales de las personas, se van a ver agravadas cuando los datos tratados pertenezcan a la categoría de los denominados «sensibles». Los datos relativos a la salud se incluyen entre esta categoría. Sin embargo, debemos tener en cuenta, para valorar en su justa medida tanto la jurisprudencia como la regulación sobre el registro obligatorios de los portadores del VIH o de los enfermos de SIDA, que esta información, puede ser calificada como *«hipersensible»* habida cuenta de lo estigmatizante que puede resultar aún, en nuestras sociedades actuales. Es obvio para cualquiera, que no tiene la misma incidencia para los derechos fundamentales, especialmente para el derecho a no ser discriminado, el ser identificado como portador del VIH o portador de otro virus o padecer otra enfermedad, incluso de igual o superior gravedad, ya que no cuentan con esa carga extra peyorativa o incluso, en ocasiones, criminalizadora del VIH.

Señala Miguel Ángel Ramiro, que *«la primera diferencia que puede establecerse entre el estigma de las personas que viven con VIH/SIDA y el estigma de las personas diagnosticadas de cáncer es que en el primer caso se hace una asociación entre el VIH/SIDA y la homosexualidad o el uso de drogas inyectadas parenteralmente»* (Ramiro, 2008, p. 297). El VIH es percibido socialmente como peligroso para la comunidad y a su portador o al enfermo de sida se le considera culpable de su padecimiento, ya que este fue adquirido como consecuencia de un comportamiento irresponsable e inmoral de la persona seropositiva. Esta culpabilización hace que *«las personas que viven con VIH/SIDA experimenten una mayor estigmatización en forma de rechazo social, discriminación económica, vergüenza interiorizada y aislamiento social que las personas que viven con cáncer»* (2008).

También para el Tribunal Constitucional español está clara la relación que existe entre el padecimiento de SIDA y la estigmatización y rechazo social que sufre la

persona infectada. En su Sentencia de 20/1992, 14 de febrero, considera que la identificación periodística, indirecta pero inequívoca, de una determinada persona, como afectada por el Síndrome de Inmunodeficiencia Adquirida (SIDA) afecta directamente y sin ninguna duda a la reputación de las personas y depara, teniendo en cuenta actitudes sociales que son hechos notorios, un daño moral (y también económico) *«a quienes así se vieron señalados como afectados por una enfermedad cuyas causas y vías de propagación han generado y generan una alarma social con frecuencia acompañada de reacciones, tan reprobables como desgraciadamente reales, de marginación para muchas de sus víctimas»*[5].

Ante esta realidad, consciente de la situación de discriminación y estigmatización que acompaña este padecimiento, la novena de las Directrices internacionales sobre VIH/SIDA y los derechos humanos de ONUSIDA requiere de los Estados que fomenten *«la difusión amplia y constante de programas creativos de educación, capacitación y comunicación diseñados explícitamente para convertir las actitudes de discriminación y estigmatización contra el VIH en actitudes de comprensión y aceptación»*[6]. Pues, como también se señala en las directrices, el VIH *«provoca violaciones de derechos humanos tales como una mayor discriminación y violencia»*. Estigmatización y violaciones de derechos humanos que serán más intensas cuando la infección por VIH afecte a las personas y grupos más vulnerables, como son las mujeres, los niños y los grupos de personas pobres y marginadas.

ONUSIDA constata que *«el abuso de los derechos humanos y de las libertades fundamentales de las personas que viven con el VIH se ha generalizado en todo el mundo tras el paso de la epidemia»*. Ante esta constatación, los participantes en la Segunda Consulta Internacional sobre VIH/SIDA y Derechos Humanos llegaron a una serie de conclusiones relativa a la necesidad de fomentar, proteger y garantizar los derechos humanos en este contexto. Merece la pena recordar dos de ellas, especialmente pertinentes para nuestro análisis.

En primer lugar, debe destacarse que *«la protección de los derechos humanos es imprescindible para salvaguardar la dignidad humana en el contexto del VIH y para asegurar una respuesta eficaz, de carácter jurídico, a las cuestiones que plantea el VIH y el SIDA. Una respuesta efectiva requiere que se hagan efectivos todos los derechos humanos, tanto civiles y políticos como económicos, sociales y culturales, y las libertades fundamentales de todos, según la normativa internacional vigente de derechos humanos»*.

---

5 Fundamento jurídico tercero.

6 Versión consolidada de 2006.

En segundo lugar, los participantes en la Segunda Consulta Internacional sobre VIH/SIDA y Derechos Humanos concluyeron, que *«el interés de la salud pública no se opone a los derechos humanos. Al contrario, está demostrado que cuando se protegen los derechos humanos, menor es el número de personas infectadas y aquellas que viven con el VIH y sus familiares pueden hacer frente al VIH y el SIDA de una mejor manera»*.

Estas y otras consideraciones serán tenidas en cuenta a la hora de analizar la problemática que nos ocupa, pues el hilo conductor de este trabajo será el análisis de la legítima o ilegítima afectación del derecho fundamental a la protección de datos personales de las personas seropositivas.

1. El sistema español de información sobre nuevas infecciones (SINIVIH)

El Sistema de Información sobre nuevas Infecciones (SINIVIH) se instaura en España por una Orden de 18 de diciembre de 2000, por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH).

Las razones que justifican su necesidad, así como sus fines y usos, se encuentran recogidas en la propia orden, que establece que su finalidad es aportar información a la administración sanitaria sobre la incidencia y evolución de los nuevos diagnósticos de infección por VIH, para conocer los factores que la determinan y definir estrategias de prevención. También para la realización de estadísticas periódicas y para contribuir a la investigación científico médica.

En la orden se especifican también, de acuerdo con la legislación española de protección de datos personales, las personas afectadas y datos incluidos en el SINIVIH. Serán incluidas en el fichero todas las personas diagnosticadas de infección por VIH en los centros del Sistema Nacional de Salud, constando los siguientes datos personales: las iniciales del nombre y los apellidos, el centro sanitario de diagnóstico, la fecha de nacimiento, el sexo, la provincia de residencia, el país de residencia y, en su caso de origen, los mecanismos de transmisión de la infección y los datos clínicos y de laboratorio. Serán Comunidades Autónomas las que notificarán los nuevos casos y está prevista su cesión a la Organización Mundial de la Salud y al Centro Europeo para la Vigilancia Epidemiológica del VIH, aunque solo se cederán datos anónimos.

Igualmente se establece la necesidad de adoptar las medidas de seguridad reglamentariamente establecidas asegurando la confidencialidad, integridad y seguridad de los datos, así como el respeto a las demás exigencias de la legislación sobre protección de datos personales, en la actualidad, las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre (LOPD).

Para un correcto planteamiento de la situación han de tenerse presentes varias las normas de la LOPD en este momento. En primer lugar, que de acuerdo con lo dispuesto en el artículo 7.3 solo se podrán tratar los datos relativos a la salud con consentimiento del interesado o cuando, por razones de interés general, así lo disponga una ley. Además, en el apartado sexto de ese mismo artículo se permite el tratamiento de los datos relativos a la salud cuando *«resulte necesario 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».* Por otra parte, el artículo 11.2.f) de la ley de protección de datos personales establece que no será preciso el consentimiento para la comunicación de datos de carácter personal relativos a la salud 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.

Obviamente se trata de un registro obligatorio y no voluntario de datos personales relativos a la salud por lo que es necesario que exista una habilitación legal para la creación del fichero y el posterior tratamiento de los datos personales y que esté justificada por razones de interés general. Según ha establecido el Tribunal Constitucional español (sentencia 202, 1999), ambos requisitos han de cumplirse simultáneamente, ya que aunque esté contemplado en una norma con rango de ley, cualquier interés legítimo no es «un interés suficiente», sino que para que se pueda prescindir del consentimiento del interesado será necesario que estemos ante un interés general, por su propia naturaleza superior a un interés particular.

El fundamento para la limitación del derecho fundamental a la protección de datos personales en el caso particular del dato personal relativo al padecimiento de VIH lo encontramos en la propia Constitución española. Según dispone el artículo 43.2 CE, *«compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios».* Este precepto ha sido desarrollado legislativamente, en lo que ahora nos interesa por la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública y por la Ley 14/1986, de 25 de abril, General de Sanidad.

En el artículo 3 de la Ley Orgánica 3/1986, se autoriza a las autoridades sanitarias a realizar acciones preventivas generales, a adoptar las medidas oportunas para el control de los enfermos y de las personas que estén o hayan estado en contacto con los mismos, así como del medio ambiente inmediato y cualquiera otras «*que se consideren necesarias en caso de riesgo de carácter transmisible para controlar las enfermedades transmisibles».*

Asimismo, la realización de estudios epidemiológicos, para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, se considera como actividad fundamental del sistema sanitario, según se establece en el artículo 8 de la Ley General Sanitaria. Para ello, se deberá contar con un sistema organizado de información sanitaria, vigilancia y acción epidemiológica. Específicamente se establece en el artículo 23 de esta ley que las Administraciones sanitarias, de acuerdo con sus competencias, crearán los Registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria.

Para cumplir con las obligaciones de análisis y vigilancia epidemiológica y al amparo del artículo 3 de la Ley Orgánica 3/1986, se crea la Red Nacional Epidemiológica por Real Decreto 2210/1995, de 29 de diciembre, de Creación de la Red Nacional de Vigilancia Epidemiológica. El Real Decreto 2210/1995 constituye la Red Nacional de Vigilancia Epidemiológica para permitir «*la recogida y el análisis de la información epidemiológica con el fin de poder detectar problemas, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional y difundir la información a sus niveles operativos competentes*» (art. 1).

En el Capítulo IV del Real Decreto 2210/1995 sobre vigilancia epidemiológica del síndrome de inmunodeficiencia adquirida (SIDA) y de la infección por virus de inmunodeficiencia humana (VIH) se establece que, a nivel estatal, la vigilancia epidemiológica del SIDA corresponderá al Ministerio de Sanidad y Consumo, a través del Registro Nacional, y de la infección por VIH.

La información que habrá de recogerse en los registros de SIDA, tanto el nacional como los autonómicos, comprenderá la información sobre casos de infección por el VIH, con presencia clínica de una o más de las enfermedades indicativas de SIDA consideradas en la definición de caso de SIDA adoptada por el Ministerio de Sanidad y Consumo para la vigilancia epidemiológica.

Los médicos, tanto del sector público como privado, que diagnostiquen al enfermo, deberán, de forma inmediata al diagnóstico y obligatoriamente, notificarlo al Registro de SIDA de la Comunidad Autónoma, en el cuestionario que suministrará dicho Registro. Habrán de recogerse los datos individualizados de cada enfermo diagnosticado y, los registros autonómicos habrán de remitir la información recogida sobre nuevos casos al registro nacional con periodicidad trimestral.

2. El principio de seguridad y su incidencia en los derechos fundamentales de las personas

Previamente al análisis de la sentencia de la de la Audiencia Nacional de 24 de marzo de 2004 que anula la Orden del Ministerio de Sanidad y Consumo de 18 de diciembre de 2000, por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH), es preciso recordar que lo que está en juego es la limitación de, al menos, un derecho fundamental. Como he señalado en páginas anteriores, cuando se utilizan datos personales están en juego valores tan importantes en una sociedad democrática y de derecho como la dignidad, la libertad o la igualdad de las personas afectadas. Como ha venido señalando el Tribunal Constitucional español desde su pionera sentencia 254/1993, de 20 de julio, cuando el artículo 18.4 de la Constitución española dispone que la Ley debe limitar el uso de la informática para garantizar la intimidad, el honor y el pleno ejercicio de los derechos de los ciudadanos, está incorporando *«una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas (…) un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»»* (fundamento jurídico 6º)[7]. Así, en la medida en que se afecten datos personales, su tratamiento debe someterse *«a una serie de cautelas y de límites* (que conjuren los riesgos que se derivan de esta actividad, y que) *permitan reparar los daños que origine y evitar que se vuelvan a producir»* (Lucas, 1993, p. 39). Se trata de intentar «*conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información»*[8] y de impedir que las personas puedan sufrir más limitaciones o injerencias en sus derechos de las necesarias para garantizar otros valores o intereses legítimos en una sociedad democrática[9].

Con el fin de alcanzar el necesario equilibrio entre los derechos de las personas y la necesidad del tratamiento de informaciones personales, la legislación nacional e internacional sobre protección de datos personales concretan en unas exigencias específicas, las relativas a la recogida, registro y uso de los datos personales y que

---

7 En el mismo sentido, entre otras, STC 11/1998, de 13 de enero, 94/1998 y 202/1999, de 8 de noviembre.

8 Exposición de Motivos del Convenio 108 del Consejo de Europa.

9 En este sentido de manera reiterada se ha pronunciado el Tribunal Europeo de Derecho Humanos en relación con las limitaciones de los derechos garantizados en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Entre otras, la sentencia de 24 noviembre 1986 (caso Gillow contra el Reino Unido) y la sentencia de 2 de octubre de 2001 (Asunto Hatton contra el Reino Unido).

están encaminadas a garantizar tanto la veracidad y seguridad de la información contenida en los datos, como la congruencia y racionalidad de su utilización. En este sentido el Tribunal Constitucional español ha señalado que el artículo 18.4 de la Constitución «*impone a los poderes públicos la prohibición de que (los individuos) se conviertan en fuentes de información sin las debidas garantías; y también, el deber de prevenir los riesgos que puedan del acceso o divulgación indebidas de dicha información*» (sentencia 292, 2000). Es decir, los poderes públicos están obligados a establecer las medidas, garantías y límites necesarios para contrarrestar los peligros y riesgos que el tratamiento de datos personales entraña, garantizando la idoneidad de la información y su seguridad. A estos límites se les ha denominado, tradicionalmente, principios de calidad de los datos y entre ellos se encuentra el principio de seguridad. La LOPD establece que deberán adoptarse las medidas necesarias para garantizar la seguridad de los datos personales evitando su alteración, pérdida, tratamiento o acceso no autorizados. Por ello «*no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y las de los centros de tratamiento, locales, equipos, sistemas y programas*» (LOPD, art. 9.2). El concepto de seguridad debe abarcar tanto la confidencialidad de la información como la disponibilidad e integridad de la misma. La Ley, consecuentemente, exige que se adopten todas las medidas necesarias, de índole técnica y organizativa, que «*garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida o tratamiento o acceso no autorizado*» (LOPD, art. 9.1).

Por tanto, el principio de seguridad de los datos va a estar orientado en tres direcciones[10] debiéndose adoptar las medidas necesarias para garantizar, en primer lugar, que los destinatarios legítimos de los datos puedan recibirlos a tiempo y acceder a ellos; en segundo lugar, que no se altere o pierda la información y en tercero y último lugar, que solo las personas autorizadas tengan conocimiento de los datos de carácter personal registrados[11].

Actualmente, las medidas de seguridad de los ficheros que contengan datos de carácter personal se encuentran recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, regulándose tanto las aplicables a los ficheros y tratamientos automatizados como a los no automatizados en los Capítulo III y IV de este Título

---

[10] Sus objetivos deberán de abarcar: «*a las personas (y funciones que desempeñan, con la debida segregación), las propias instalaciones, los equipos y comunicaciones, los programas y, muy especialmente, los datos*». (Ramos, p. 133).

[11] Este último aspecto se garantiza a través de una doble vía: por un lado adoptando las medidas necesarias para impedir el acceso no autorizado a los datos y, por otro, a través del deber del responsable del fichero y las demás personas que intervengan en cualquier fase del tratamiento de guardar secreto profesional respecto de los mismos, obligación que subsistirá aún después de finalizar su relación con el titular del fichero (artículo 10 de la LOPD).

respectivamente. En los artículos 79 y siguientes del Reglamento se establece el marco vigente de referencia obligada para que los responsables del fichero adopten las medidas necesarias y adecuadas para garantizar su seguridad, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos. Las medidas de seguridad exigibles se califican en tres niveles distintos –básico, medio y alto–, en función del tipo de datos personales almacenados, tanto para los ficheros tradicionales como para los automatizados. El Reglamento de desarrollo de la LOPD deroga expresamente el anterior Reglamento de Medidas de seguridad de los ficheros de datos personales, aprobado por Real Decreto 994/1999, de 11 de junio y según el cual al fichero le correspondía adoptar las medidas de seguridad de nivel alto[12].

En su sentencia de 24 de marzo de 2004, la Audiencia Nacional anuló la Orden del Ministerio de Sanidad y Consumo de 18 de diciembre de 2000, que creó el fichero de datos de carácter personal SINIVIH. Resumidamente, pueden destacarse los siguientes aspectos de la resolución judicial:

1. La Orden cuenta con la correspondiente habilitación y cobertura legal: se dicta al amparo de los artículos 8.1 y 23 de la Ley 14/1986, de 25 de abril. A estos efectos, el Real Decreto 2210/1995, prevé expresamente la existencia de Registros de SIDA, nacional y autonómicos, con objeto de recoger información sobre casos de infección, fuentes de información, datos individualizados de cada uno de los enfermos, todo ello dentro de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos incorporados a los Registros.
2. la Orden debe entenderse necesaria en una sociedad democrática, pues no se dicta en función de simples criterios de oportunidad o conveniencia, está justificada en aras al interés general y las razones de su existencia son suficientes, convenientes y convincentes. No se viola por ello el derecho a la intimidad consagrado en el artículo 18.1 de la Constitución.
3. La estructura del fichero no garantiza la seguridad de los datos personales que contiene, o que debe contener, y no evita el acceso no autorizado, habida cuenta la naturaleza de los datos almacenados o a almacenar, según exige el artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

La Audiencia Nacional anula la Orden al considerar que no cumple con las medidas de garantía adecuadas para preservar la intimidad de los interesados, porque la estructura informática del fichero permite a terceros, mediante manipulación adecuada e interesada, obtener información de acceso reservado. La decisión judicial se apoya directamente un el informe pericial y en la aplicación de la doctrina del Tribunal

[12] Esta norma se completaba con lo dispuesto en el Real Decreto 195/2000, de 11 de febrero, por el que se establecía el plazo para implementar las medidas de seguridad.

Constitucional según la cual *«un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de esta»* (sentencias 143, 1994 y 197, 2003) .

Si bien, la Audiencia Nacional basó su fallo en el incumplimiento de lo dispuesto en el artículo 9 de la LOPD, al considerar que el fichero sobre portadores de VIH no cumplían las exigencias derivadas del principio de seguridad de acuerdo con la doctrina del Tribunal Constitucional, lo cierto es que, según el informe pericial *«las especificaciones de seguridad del SINIVIH cumplen con las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, salvo omisiones de escasa relevancia (falta de un sistema de actualización y revisión del fichero y no constancia del período mínimo -dos años- de conservación de los datos registrados)»*. Es decir, en lo sustancial, el fichero cumplía las exigencias técnicas derivadas del Real Decreto 994/1999.

Sin embargo, el informe pericial considera que *«el método o mecanismo empleado para el tratamiento de los datos personales introducidos en el fichero -nombre y apellidos, centro sanitario de diagnóstico, fecha de nacimiento, provincia de residencia, país de residencia, país de origen, datos clínicos y datos de laboratorio- posibilitan la identificación de una persona con alto nivel de evidencia, pues aunque aisladamente los datos en cuestión no permiten la identificación, la conjunción de varios de estos datos sí lo permiten, dado que pueden ser contrastados con los datos obtenidos en otra fuente -el Registro Civil automatizado, por ejemplo-»*. Además, se indica también por el perito, *«los indicadores personales pueden dar lugar a confusiones -repetición de datos por aproximación familiar, duplicidad de datos en el mismo afectado-, máxime en el caso de nombres y apellidos compuestos»*.

Tras el estudio pormenorizado del procedimiento de seguridad del fichero SINIVIH, el perito llega a una doble conclusión: *«la ficha dispone de los suficientes datos que permite asociarla a una persona concreta con alto grado de evidencia y, por otro lado, carece de los datos suficientes que permitan identificar con plena certeza a una persona para su posterior modificación o cancelación»*. Por ello considera que para garantizar la seguridad del fichero, hubiese sido más adecuado que en lugar de identificar al portador o enfermo de VIH a través de las iniciales del nombre y apellidos, debiera de haberse empleado un código numérico conocido solo por la Administración y el afectado.

Sin embargo, con posterioridad en sentencia de 9 de julio de 2007, el Tribunal Supremo casará la sentencia de la Audiencia Nacional haciendo suyos los argumentos

del Abogado del Estado y considerando que la Audiencia Nacional realiza una apreciación ilógica de la prueba al asumir un informe pericial contradictorio en sí mismo y trasladando esa incongruencia al resultado de la prueba. A juicio del Tribunal Supremo la Orden por la que se crea un fichero de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al sistema de información sobre nuevas infecciones no vulnera el art. 18,4 CE, pues de los datos personales incluidos en este sistema de información no se puede determinar la persona a la que los mismos se refieren. Señala Noelia de Miguel que *«el razonamiento elaborado por el Tribunal Supremo se aleja, sin duda, de los pronunciamientos de la Agencia Española de Protección de Datos sobre el concepto de disociación»* (De Miguel, 2008, p. 317).

Señala el Tribunal Supremo que el *«debate debía ceñirse a sí la Orden del Ministerio de Sanidad y Consumo de 18 de diciembre de 2000, sobre los procedimientos del SINIVIH están correctamente aplicados, se siguen las especificaciones previstas en el documento de seguridad y están en conformidad con el Real Decreto 992/1999, respecto a las medidas de seguridad de nivel alto, es decir un puro control de legalidad»*.

Según el informe pericial la Orden cumple las disposiciones reglamentarias en materia de seguridad de nivel alto exigidas. Incluso, señala el Tribunal Supremo, a instancias de la Agencia Española de Protección de Datos se modificaron determinados aspectos técnicos en la Orden, que finalmente la reputó conforme con lo exigido por la Ley Orgánica 15/1999, de 13 de diciembre. *«La Agencia había puesto de relieve en el informe inicial que los datos contenidos en el fichero habrán sido sometidos a un procedimiento de disociación, definido por el art. 3.f) de la citada Ley Orgánica como todo «tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable», lo que hará que los datos no permitan determinar la persona a la que los mismos se refieren»*.

Recuerda el Tribunal Supremo que del informe del perito se deduce que las medidas de seguridad son las correctas conforme al citado Real Decreto así como que el método es el correcto y garantiza la confidencialidad de la cesión. *«No se colige del Dictamen, ceñido a los concretos aspectos técnicos requeridos a un Ingeniero Superior de Telecomunicación, que el sistema de información establecido con respeto a las antedichas exigencias permita la identificación de las personas registradas en el fichero sino que al seguir aquellas cumple su fin de introducir un sistema de vigilancia epidemiológica conforme a las recomendaciones de los organismos internacionales acreditados en materia sanitaria»*. Pero, añade que informe que, aún cuando aisladamente los datos introducidos en el fichero no permiten la identificación de una persona, si sería factible cruzando los datos con los obtenidos de otro Registro, por ejemplo, el automatizado del Registro Civil. Por ello defiende en sistema alternativo de identificación, como se ha apuntado anteriormente, a través de un código numérico.

En opinión del Tribunal Supremo esta última objeción excede de los límites que corresponde apreciar a los Tribunales por lo que la valoración de la prueba resulta ilógica. Así, casa la sentencia del Audiencia Nacional, pues este órgano judicial debía haberse limitado al control de legalidad de la Orden centrándose en si cumplía o no las previsiones legales y reglamentarias en materia de seguridad, y no hacer un control de oportunidad «*acerca de cuál puede ser el método más adecuado para realizar una determinada actividad o establecer que la legalidad es perfectible mediante un método mejorable con la adopción de medidas no previstas en la norma*».

3. El sistema de información gallego sobre la infección por el virus de la inmunodeficiencia humana (SIGIVIH)

El sistema de información de la Comunidad Autónoma de Galicia sobre la infección por el virus de la inmunodeficiencia humana, se crea por el Decreto 33/2004, de 29 de enero para llevar a cabo la vigilancia epidemiológica de la infección por VIH en Galicia. Su finalidad es conocer la evolución temporal y geográfica de infección y su distribución en la población de riesgo

El SIGIVIH incluye los siguientes datos personales: nombre y apellidos de la persona declarante, teléfono de contacto, nombre del centro, unidad o servicio y fecha de declaración. Con el fin de controlar los datos duplicados, reincluirá la siguiente información: primera y segunda letra del nombre, primera y segunda letra del primer apellido, primera y segunda letra del segundo apellido, sexo, edad en el momento del diagnóstico, fecha de nacimiento, municipio de residencia, provincia de residencia, país de residencia, país de origen y año de llegada a España, en su caso. También se incluirá información clínica y epidemiológica y así se recogerá el test positivo confirmado, la fecha del primer resultado positivo confirmado, los posibles mecanismos de transmisión, el estadio clínico de la infección, el recuento de CD 4 y la carga viral.

En el año 2005, el Tribunal Superior de Justicia de Galicia suspende la ejecución del Decreto en un Auto de 18 de abril de 2005, pero en una sentencia de 14 de diciembre de 2007, el Tribunal Supremo casa y anula esta resolución judicial[13]. El Decreto 33/2004 por el que se crea el registro gallego de VIH, señala la necesidad conocimiento y seguimiento de las epidemias en materia de sanidad pública, así como la necesaria coordinación no solo entre las distintas administraciones sanitarias españolas, sino también a escala internacional. Destaca el Tribunal Supremo que el Decreto gallego impone el respeto a lo dispuesto en la LOPD y que expresamente se establece que «*la*

[13] De tenor muy semejante es la Sentencia del Tribunal Supremo de 26 de septiembre de 2007, que anula el auto del TSJ de Galicia de 6 de junio de 2005, que desestimó el recurso de súplica interpuesto por la Xunta de Galicia contra el auto de 18 de abril de 2005.

información recaudada se considerará estrictamente confidencial y solamente se utilizará para los fines expresamente previstos en el fichero denominado Sistema de Información y Vigilancia de Problemas de Salud Pública»[14].

Argumenta el Tribunal Supremo que, de acuerdo con su doctrina consolidada, cuando se trata de la suspensión de disposiciones generales se asume como prioritario el interés general o público implícito en las disposiciones generales, interés que solo cede o se pospone ante posibles perjuicios acreditados. *«Partiendo de la trascendencia del interés general que pretende conseguir la norma, y que no es otro que el de conocer los nuevos diagnósticos de infección por el VIH y las causas que lo originan para el seguimiento de la evolución de la epidemia y el control de la misma, así como el tratamiento de los afectados, es claro que ese interés prima sobre la intimidad personal de los afectados presuntamente comprometida».* Pues considera además el Tribunal Supremo que no se ha acreditado, como correspondía hacer a quien instó la suspensión, la realidad o la inminencia del peligro de que la intimidad personal pueda verse afectada. Al contrario, señala, *«lejos de ello, la resolución recurrida habla de que con la suspensión se pretende evitar un «peligro evidente», aún cuando este sea «hipotético». En consecuencia, y, desde este punto de vista, la suspensión no debió acordarse al no estar acreditado el perjuicio que se decía querer evitar, y ante el que no podía ceder el interés general perseguido por la Administración con la creación de ese sistema de vigilancia».*

Finalmente, por lo que respecta al SIGIVIH es imprescindible hacer referencia a la sentencia del TSJ Galicia de 21 de mayo de 2008. Me centraré en aquellos aspectos que pudieran resultar novedosos respecto de otras resoluciones judiciales ya tratadas. En concreto, las asociaciones recurrentes alegaron la violación de varios preceptos de la LOPD: el artículo 5, que garantiza el derecho de información y el artículo 4 que establece los principios de calidad de los datos.

El TSJ de Galicia desestima ambos motivos. El primero de ellos porque *«desde el momento en que es el personal médico el que está obligado a declarar los casos de nuevos diagnósticos de infección por el VIH a través del formulario de notificación contenido en el anexo I del Decreto, no tiene sentido que haya de recogerse en dicho formulario la información mencionada en el artículo 5 de la L.O. 15/1999».* Pero, además, añade esta sentencia de acuerdo con lo establecido en la propia ley de protección de datos personales, no es necesario el consentimiento del interesado, según se deduce de los artículos 8, 7 y 11. *«Y ese régimen peculiar se ahonda en el ámbito de la vigilancia epidemiológica, precisamente por la naturaleza de las*

[14] Artículo 5 del Decreto de la Comunidad Autónoma de Galicia 33/2004, de 29 de enero por el que se crea el Sistema de Información Gallego sobre la Infección por el Virus de la Inmunodeficiencia Humana (SIGIVIH).

enfermedades de que se trata, en cuyo sentido el artículo 33 del Real Decreto 2210/ 1995, de 28 de diciembre , por el que se crea la Red Nacional de Vigilancia Epidemiológica, establece la declaración obligatoria de esta patología, una vez detectada por el profesional correspondiente; así, ese precepto establece que los médicos, tras el diagnóstico, procederán a la comunicación inmediata y obligatoria al Registro del SIDA de la Comunidad Autónoma, añadiendo el artículo 34 del mismo Real Decreto, que «Se recogerán los datos individualizados de cada uno de los enfermos diagnosticados mediante protocolo específico»».

Añade el TSJ de Galicia que también la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, refuerza esta obligación en su artículo 23 al exigir a los profesionales sanitarios *«el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica».*

Igualmente considera que no se ha infringido el artículo 4 de la LOPD al considerar que no son excesivos datos como sexo, edad al diagnóstico, fecha de nacimiento, municipio de residencia, fecha del primer resultado positivo confirmado, posibles mecanismos de transmisión, estadio clínico de la infección, en un registro que tiene por finalidad el control epidemiológico y la recogida de datos para la elaboración de actividades preventivas y profilácticas en materia de SIDA, habida cuenta la finalidad que justifica su obtención.

Finalmente, considera que se cumplen los requisitos para la limitación de los derechos a la intimidad y a la protección de datos personales establecidos por el Tribunal Europeo de Derechos Humanos, ya que esta injerencia en los derechos a la vida privada de los afectados tienen una base legal adecuada, persigue un fin legítimo (la prevención, gestión y prestación de servicios sanitarios a enfermos de infección por VIH y SIDA) y, por último, *«el Decreto debe entenderse necesario en una sociedad democrática, pues no se dicta en función de simples criterios de oportunidad o conveniencia, está justificado en aras al interés general y las razones de su existencia son suficientes, convenientes y convincentes».*

4. La sentencia del Tribunal Superior de Justicia de Asturias de 12 de septiembre de 2005

Esta resolución judicial, es en mi opinión, la más interesante de todas las analizadas y no solo porque en ella se haga un estudio pormenorizado y exhaustivo del derecho fundamental a la protección de datos personales, sino porque centra el problema de

la legitimidad en una sociedad democrática de la existencia de un registro, autonómico o nacional, de personas portadoras del VIH o enfermas de SIDA en el que a mi juicio es el tema clave de toda esta problemática: el si se trata o no de una medida necesaria y proporcionada. Como hemos visto el Tribunal Superior de Justicia de Galicia, pasó de puntillas sobre esta cuestión considerando adecuados y no excesivos los datos personales que se recaban y por lo tanto necesaria y proporcionada la recogida de los mismos, habida cuenta la finalidad perseguida. ¿Pero es necesario, proporcionado y adecuado en una sociedad democrática un registro nominal de personas con este padecimiento? De la lectura de la sentencia del TSJ de Asturias se desprende que la sala de lo Contencioso-Administrativo tenía sus dudas.

Coincide el TSJ asturiano con las otras resoluciones vistas en que los ficheros cuenta con la habilitación legal adecuada, *«pues se trata de una epidemia y los dos ficheros se instituyen para fines legítimos, pues era necesario el conocimiento de la distribución o localización de los infectados por el VIH para conocer los grupos de población más susceptibles de transmisión y adquisición, para orientar políticas y programas de prevención de nuevas infecciones y para poder redirigir las actuaciones sanitarias actuales cara al tratamiento de los ya infectados, y la resolución que regula los ficheros ha de considerarse necesaria en una «sociedad democrática», en defensa de la protección de la salud como bien individual y también de carácter general, dado que se trata de una epidemia de ámbito no solo regional sino mundial y de duración «sine die», no coyuntural»*.

Respecto de la necesidad de la identificación afirma la sentencia que «*podría admitirse excepcionalmente que dicha identificación lo sea mediante el nombre y apellidos, siempre que no existan o no se den históricamente las condiciones de desarrollo tecnológico adecuadas para la creación de códigos anónimos o sistemas que permitan salvaguardar al máximo la confidencialidad o anonimato del afectado, sin alterar los fines legítimos de los ficheros y que se adopten unas medidas de seguridad igualmente adecuadas. A ese «debe ser» se refiere el Comité recurrente y ese reto es asumido por la Administración cuando refiriéndose al asunto concreto de la identificación mediante códigos anónimos señala que «… ni es posible, en el momento actual implantar otro tipo de medidas que puedan sustituir a corto plazo los datos que se solicitan en el Registro». Con ello la propia Administración está admitiendo que en cuanto se den las condiciones necesarias que eviten confusiones y duplicación, hará cuanto proceda al respecto para llevar a la práctica ese deseado anonimato. Sin embargo en aquellos momentos (1999) la Administración reconoce que no era posible el establecimiento de códigos anónimos y así se asume también por parte del Comité recurrente, lo que, evidentemente, no puede vedar ni veda, desde entonces, en el futuro, la exigencia de obtener tal vez ya hoy, en las actuales circunstancias y con los nuevos adelantos tecnológicos, el tan deseado anonimato, y no solo para esos dos ficheros concretamente»*

Es decir, si la tecnología hiciese posible el anonimato, podría afirmarse que el registro nominal y obligatorio de los portadores de VIH dejaría de ser una medida proporcionada en una sociedad democrática.

5. La calidad de los datos y el principio de proporcionalidad en la recogida y tratamiento del dato relativo a la condición de seropositivo o enfermo de sida

Uno de los elementos esenciales que configuran el derecho fundamental a la protección de datos personales es el denominado como principio de calidad de los datos. Son estos, en realidad varios principios o requisitos recogidos, tanto en la legislación española (en La Ley Orgánica 15/1999) como en la Directiva de la Unión Europea sobre Protección de Datos personales[15] y el Convenio número 108, del Consejo de Europa[16]. Al igual que la ley española, estas normas internacionales intentan conjurar los riesgos que, para los derechos de las personas, suponen el tratamiento de sus datos personales y al mismo tiempo garantizar los intereses legítimos, públicos o privados que justifiquen ese tratamiento. Las disposiciones sobre protección de datos, a fin de conseguir ese doble objetivo, establecen una serie de cautelas, límites y pautas de comportamiento que deberán de ser respetadas, tanto en el momento de la obtención de los datos personales como en cualquier otra fase del tratamiento, incluida su cesión. Tanto en el Convenio de 28 de enero de 1981, como en la Directiva 95/46/CE, se expresa la necesidad de conciliar el respeto de los derechos de las personas con la libre circulación de información entre los pueblos y a este fin deberán establecerse unas garantías suficientes *«para que las innegables ventajas que pueden obtenerse del tratamiento automatizado de datos no den lugar a la vez a un debilitamiento de la posición de las personas a las cuales hacen referencia los datos registrados»*[17]. Este objetivo se logra, principal aunque no exclusivamente, a través del establecimiento de una serie de garantías en forma de límites y modos en los que las informaciones personales pueden y deben obtenerse, registrarse y ser tratadas y en forma de derechos subjetivos que dotan de contenido efectivo a las anteriores cautelas y con lo que se conseguirá un sistema eficaz de protección de los derechos fundamentales de los ciudadanos.

El artículo cuarto de la LOPD regula la *calidad de los datos* estableciendo los principios básicos que deberán respetarse en la recogida, tratamiento, uso y almacenamiento de los datos personales, de manera que solo tendrán una calidad adecuada aquellos

---

15 Directiva 95/46/CE, del Parlamento Europeo y del Consejo de la Unión Europea, de 24 de octubre de 1995, sobre Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

16 Convenio 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.

17 Memoria explicativa del Convenio 108 del Consejo de Europa, punto segundo.

datos respecto de los cuales se cumplan estos principios. Son normas que regulan la recogida, registro y uso de los datos personales y están encaminados a garantizar tanto la veracidad de la información contenida en los datos, como la congruencia y racionalidad de su utilización. En este momento nos interesa detenernos en dos de ellos: el principio de pertinencia y el de finalidad.

El principio de pertinencia exige que los datos personales estén relacionados con el fin perseguido, por lo que habrán de ser *«adecuados y no excederán de las finalidades para las que se hayan registrado»* (Pérez, 1992). Es decir, los datos deben servir para la finalidad para la que se obtienen de forma que exista una *«clara conexión entre la información que se recaba (…) y el objetivo para el que se solicitó»* (Lucas, 1993, p. 65). Por tanto, no van a poder solicitarse ni registrarse más datos personales que los estrictamente necesarios para llevar a cabo la investigación de que se trate o cumplir la finalidad legítimamente encomendada al organismo público o empresa privada solicitante. Además, no podrán recabarse más datos que aquellos que sean estrictamente necesarios en ese momento, aunque fuesen susceptibles de serlo para cumplir objetivos futuros.

Por su parte, el principio de finalidad establece que solo se podrán recoger y tratar los datos personales que *«sean adecuados (…) en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido»* (LOPD, art. 4). Asimismo, los datos personales objeto de tratamiento *«no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos»* (LOPD, art. 4, apartados 1 y 2). Esto es, los datos solo podrán recogerse y tratarse de acuerdo con una finalidad legítima y determinada y, por lo tanto, no podrán recogerse datos para finalidades contrarias a las leyes o al orden público, debiendo ser respetuosas con los valores constitucionales y los derechos fundamentales. Tampoco se recabarán datos personales para el cumplimiento de objetivos imprecisos o inconcretos y, en último término, los datos personales no podrán ser utilizados de forma incompatible con las finalidades para las que fueron recabados.

El principio de finalidad se encuentra íntimamente conectado con el principio de pertinencia, hasta el punto de que el cumplimiento del segundo implica necesariamente el respeto al primero, ya que los datos han de ser adecuados para una finalidad concreta. No obstante, el principio de finalidad es más amplio en su contenido que el de pertinencia al aportar el requisito de que los datos deberán ser usados exclusivamente para la finalidad para la que fueron recabados y esta deberá ser respetuosa con el Ordenamiento jurídico. El cumplimiento de este requisito impide asimismo que, una vez que los datos personales hayan sido utilizados para la finalidad legal para la que hubiesen sido recabados, puedan ser reutilizados para el cumplimiento de objetivos distintos a aquellos que motivó su solicitud y registro.el ámbito sanitario, de acuerdo con las disposiciones legales vigentes.

Debe insistirse en la necesidad de que en un ámbito tan sensible para las libertades individuales, tanto la recogida como el tratamiento de los datos, han de hacerse respetando escrupulosamente los principios de pertinencia y finalidad, pues, el acceso a esta información, aún habilitado por lo previsto en su normativa específica reguladora, debe limitarse a los datos que efectivamente resulten necesarios para el cumplimiento de la finalidad que justifique dicho acceso, sin que pueda extenderse a datos no vinculados a dicha finalidad. Obviamente, ambos principios son plenamente aplicables al caso que nos ocupa.

Conviene recordar que la finalidad que justifica la existencia de un registro obligatorio de portadores de VIH, según las normas que le dan cobertura legal es aportar información a la administración sanitaria sobre la incidencia y evolución de los nuevos diagnósticos de infección por VIH, para conocer los factores que la determinan y definir estrategias de prevención. También para la realización de estadísticas periódicas y para contribuir a la investigación científico médica. Asimismo, para la realización de estudios epidemiológicos, para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria. La información epidemiológica debe servir para detectar problemas, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional, así como para difundir la información a sus niveles operativos competentes.

Por otra parte en la actualidad nos encontramos inmersos en el proceso de informatización de las historias clínicas. Este proceso *«ha traído consigo la integración de la información dispersa en bases de datos de los centros sanitarios, así como las de los laboratorios clínicos y los programas de admisión»* (Carnicero, 2003, p. 257). La historia clínica electrónica ha supuesto la integración de la información clínica, correspondiente a una persona, que se encontraba ubicada en los distintos los centros sanitarios en que hubiera sido atendida. Además, permite *«el acceso a la información clínica desde cualquier momento y lugar en el que pueda ser necesario para la debida atención del paciente, con independencia de en qué centro sanitario haya sido generada esa información»* (2003).

Pero, asimismo, la historia clínica informatizada o electrónica tiene como consecuencia un importante cambio en el concepto de la historia clínica, ya que esta *«deja de ser un registro con la información generada en la relación entre un paciente y un profesional, o en el mejor de los casos un centro sanitario, a formar parte de un sistema integrado de información clínica»* (Carnicero, 2003, p. 107). De esta manera, la historia clínica electrónica forma parte de un sistema que incluye las aplicaciones clínico administrativas, las de planificación y gestión, los sistemas departamentales y todos aquellos que contienen información sobre la salud de una persona, con independencia del centro sanitario en el que se haya originado. En ella se encuentra no solo a la

información relativa a un paciente en un centro sanitario, sino a toda la información de salud de una persona, con independencia de dónde y cuándo haya sido generada. Pues, la historia *«forma parte de un sistema de información clínica que integra la procedente de todos los sistemas clínicos o clínico administrativos. Este sistema permite el acceso a toda la información clínica de una persona en cualquier momento y lugar que sea necesario»* (2003, p. 108). Además ese sistema clínico formará parte necesariamente del sistema de información del servicio de salud correspondiente.

La *Estrategia 11, «Sanidad en línea»,* del Plan Nacional de Calidad para el Sistema Nacional de Salud (SNS) pretende garantizar la identificación inequívoca de los ciudadanos en todo el Sistema Nacional de Salud mediante la tarjeta sanitaria y la base de datos de población protegida del SNS[18]. Así, se garantizará la accesibilidad desde cualquier punto del sistema, la interoperabilidad y la explotación adecuada de la información (pág. Web, SNS).

Destacan Javier Carnicero y José Manuel Vázquez, que, para el sistema sanitario, el problema más acuciante es la clave primaria de la entidad paciente, pues al paciente hay que identificarlo de forma inequívoca. En su opinión *«la clave no puede depender de los valores de los atributos del elemento que identifica. En otras palabras, debe ser un código aséptico, de forma que defina, en el caso de un individuo, una persona, con independencia de los valores de sus atributos como el nombre, apellidos o la fecha de nacimiento»* (Carnicero, 2003, p. 113). Pues, *«la identificación por nombre y apellidos y fecha de nacimiento facilita los errores y la probabilidad de coincidencias múltiples, por ello la identificación con estos datos es impracticable»* (2003, p. 109) y para evitar estos problemas en cada centro sanitario se utilizan los números que se asignan para identificar las historias clínicas.

A la vista de estos argumentos, debemos plantearnos si en la actualidad la identificación nominal del paciente seropositivo sigue siendo necesaria, es decir, si los datos personales identificativos son ya pertinentes. En mi opinión, con la implantación de la historia clínica electrónica en todo el territorio español, resulta muy dudosa esta necesidad, pues el acceso a la información necesaria dentro del sistema nacional de salud está garantizado a través de la identificación del paciente mediante la tarjeta sanitaria. Se evitarían además de este modo las deficiencias de seguridad recogidas en la sentencia de la Audiencia Nacional de 24 de marzo de 2004[19]. Se darían, por

[18] Consagrados por el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

[19] Que también fueron detectados por la Agencia Española de Protección de Datos, según consta en las Recomendaciones de 9 de marzo de 2000, como consecuencia del Plan de inspección de oficio al registro nacional del SIDA. En concreto se señalaba que *«la detección de duplicados es frecuente ya que un mismo enfermo puede ser notificado desde diferentes hospitales e incluso desde diferentes provincias»*.

tanto, las circunstancias para que el registro fuese anónimo mediante un código que permitiese identificar inequívocamente a la persona con VIH, para cumplir con las finalidades que la normativa reguladora encomienda al SINIVIH.

Finalmente, es necesario tener en cuenta una última razón que nos permite cuestionar la constitucionalidad del registro nominal y obligatorio del VIH: el principio de proporcionalidad. Este principio ha de ser tenido en cuenta necesariamente en la utilización de informaciones que hagan referencia a la salud de una persona. Pues, incluso en aquellos supuestos en los que exista una habilitación legal que permita recabar y tratar esta clase de informaciones personales, ha de realizarse la ponderación que exige el principio de proporcionalidad.

El Tribunal Europeo de Derechos Humanos ha venido estableciendo que la limitación de los derechos amparados por el artículo 8 del Convenio ha de ceñirse a lo estrictamente imprescindible para realizar el fin legítimo justificador de tal limitación, debiendo optarse por la medida, de entre las posibles, menos gravosa para el derecho fundamental a la vida privada.

Las condiciones que exige el Tribunal de Estrasburgo para considerar que la injerencia de la autoridad pública en los derechos del artículo 8, constituya una medida justificada en una sociedad democrática son las siguientes:

1. La medida limitativa de los derechos a la vida privada debe estar «prevista por la ley». Este requisito exige no solo que la medida tenga una base legal en el derecho interno, sino que sea «*accesible al justiciable y previsible*»[20], es decir, que exista una base legal en derecho interno accesible y previsible. Una norma es previsible cuando está redactada con la suficiente precisión para permitir a toda persona –si es necesario, con el consejo apropiado– regular su conducta.

2. La injerencia en la vida privada debe «perseguir un fin legítimo», en concreto, los mencionados en el apartado segundo del artículo 8.

3. La intromisión en los derechos del artículo 8 debe ser «necesaria en una sociedad democrática» para alcanzar tal fin. La noción de necesidad implica una exigencia o necesidad social imperiosa para la intromisión. El concepto de necesidad no equivale al de «indispensable», pero *«tampoco tiene la flexibilidad de términos como «admisible», «normal», «útil», «razonable» u «oportuno»»* (Ruiz, s.f.). Este último requisito exigirá normalmente la ponderación de los intereses en conflicto, el derecho o derechos afectados y la finalidad de la injerencia, o un juicio de

[20] SSTEDH de 16 de febrero de 2000 (caso Amann contra Suiza), o de 4 de junio de 2002 (caso Landvreugd contra Holanda), entre otras.

proporcionalidad para determinar si no existe algún medio menos lesivo para el derecho afectado que la medida adoptada y que constituye una injerencia. Así lo ha establecido el TEDH, entre otras, en la sentencia de 24 noviembre 1986 (caso Gillow) en la que establece que *«la noción de necesidad implica una injerencia basada en una necesidad social imperiosa y sobre todo proporcionada al fin legítimo perseguido»*[21].

4. Finalmente, para el TEDH, el respeto al carácter confidencial de la información sobre la salud constituye un principio esencial del sistema jurídico de todos los Estados parte en la Convención y, por ello, la legislación interna debe prever las garantías apropiadas para impedir toda comunicación o divulgación de datos de carácter personal relativos a la salud contraria a las garantías previstas en el art. 8 del Convenio europeo de derechos humanos (SSTEDH caso Z. c. Finlandia de 25 de febrero de 1997, y caso L·L. c. Francia, de 10 de octubre de 2006)[22].

Respecto de esta cuestión se ha manifestado también el Tribunal Constitucional español[23]. El TC considera que la información relativa a la salud física o psíquica de una persona es, no solo una información íntima[24], sino además especialmente sensible

---

[21] El mencionado juicio de proporcionalidad ha sido analizado por la Agencia Española de Protección de Datos en resolución de 22 de agosto de 2007. Esta resolución señala que de los apartados 3 y 5 del artículo 16 de la Ley 41/2002 y siempre previa ponderación de la proporcionalidad, «se deduce la existencia de tres supuestos en los que será posible el uso de la historia clínica con fines distintos de los médico-asistenciales, estableciendo la Ley especialidades distintas en cada uno de los supuestos». Para estos usos, deberán someterse a una previa disociación los datos contenidos en la historia clínica «de manera que como regla general quede asegurado el anonimato», a menos que el interesado haya prestado su consentimiento para ello, en los términos que impone el artículo 7.3 de la Ley Orgánica 15/1999.

[22] SSTEDH caso X. e Y., de 26 de marzo de 1985; caso Leander, de 26 de marzo de 1987; caso Gaskin, de 7 de julio de 1989 EDJ1989/12019 ; mutatis mutandis, caso Funke, de 25 de febrero de 1993; caso Z., de 25 de febrero de 1997). También el Tribunal de Justicia de las Unión Europea, en la Sentencia de 5 de octubre de 1994 (asunto X. contra Comisión, C-404/92 P), referida a la protección de la intimidad y al tratamiento de datos relativos a la salud, afirma que «los derechos fundamentales pueden ser sometidos a restricciones, siempre y cuando estas respondan efectivamente a objetivos de interés general y no constituyan, en lo que respecta al fin perseguido, una intervención desmesurada e intolerable que afecte a la propia esencia de los derechos garantizados».

[23] Igualmente, para el Tribunal de Justicia de la Unión Europea, el derecho al respeto a la vida privada, consagrado en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, que tiene su origen en las tradiciones constitucionales comunes de los Estados miembros y que está amparado por el derecho comunitario, comprende particularmente el derecho a mantener secreto el estado de salud. No obstante según la jurisprudencia del TJCE, los derechos fundamentales pueden ser sometidos a restricciones, siempre y cuando estas respondan efectivamente a objetivos de interés general y no constituyan, en lo que respecta al fin perseguido, una intervención desmesurada e intolerable que afecte a la propia esencia de los derechos garantizados. Vid. Punto 23 de la STJCE de 8 de abril de 1992, Comisión / Alemania, C-62/90. En el mismo sentido STJCE de 5 de octubre de 1994, Caso X contra la Comisión, C-404/92 P.

[24] Entre otras, en la STC 196/2004, de 15 de noviembre, se afirma que la cobertura constitucional del artículo 18.1 CE «implica que las intervenciones corporales pueden también conllevar, no ya por el hecho en sí de la intervención, sino por razón de su finalidad, es decir, por lo que a través de ellas

y por tanto digna de especial protección desde la garantía del derecho a la intimidad y de la protección de los datos de carácter personal. Ambos derechos quedan relevantemente afectados cuando, sin consentimiento de la persona, se accede a datos relativos a su salud o a informes relativos a la misma.

Si bien estos derechos no son absolutos, pues pueden ceder ante otros derechos y bienes constitucionalmente relevantes. Así ocurrirá cuando la limitación que haya de experimentar esté fundada en una previsión legal que tenga justificación constitucional, se revele necesaria para lograr el fin legítimo previsto y sea proporcionada para alcanzarlo, y sea además respetuosa con el contenido esencial del derecho[25]. El juicio de proporcionalidad cuando se afecta el derecho a la intimidad y a la protección de los datos personales relativos a la salud exige que se presente una justificación objetiva y razonable, debiendo ser la medida limitadora de los derechos fundamentales idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo[26]. La limitación de ambos derechos resultará legítima si es proporcionada y será proporcionada si, entre otros requisitos, no existen otras medidas menos gravosas que, sin imponer sacrificio alguno estos derechos fundamentales, *«o con un menor grado de sacrificio, puedan ser igualmente aptas para conseguir dicho fin»*[27].

Resumiendo, el juicio de proporcionalidad exige que la medida limitadora de los derechos fundamentales a la intimidad y a la protección de datos personales persiga un fin legítimo, sea necesaria en una sociedad democrática, no vaya más allá de lo estrictamente necesario, atienda a razones relevantes y convincentes que la justifiquen y, además, deberá valorarse la gravedad de la intromisión y si la medida es imprescindible e idónea para asegurar el interés público que la justifica.

Son dos las cuestiones, pues, que hemos de valorar: si existe una medida menos gravosa y que permita igualmente cumplir con la finalidad prevista en la norma limitativa de los derechos fundamentales a la intimidad y a la protección de datos personales y si esta medida restrictiva es idónea para conseguir esta finalidad. Pues, ha quedado sobradamente argumentado que la medida limitadora de ambos derechos cuenta con la cobertura legal necesaria y persigue un fin legítimo en una sociedad democrática: la protección de la salud pública.

---

se pretenda averiguar, una intromisión en el ámbito constitucionalmente protegido del derecho a la intimidad personal. Esto es lo que ocurre cuando, como en el presente caso, a consecuencia de un análisis de orina se llega a la conclusión de que el trabajador había consumido drogas. Una prueba médica realizada en términos objetivos semejantes supone una afectación en la esfera de la vida privada de la persona, a la que pertenece, sin duda, el hecho de haber consumido algún género de drogas». En este sentido también STC 207/1996, de 16 de diciembre.

25 Entre otras, SSTC 57/1994, de 28 de febrero, 143/1994, de 9 de mayo y 25/2005, de 14 de febrero.

26 SSTC 25/2005, de 14 de febrero y 207/1996, de 16 de diciembre.

27 STC 70/2009, de 27 de abril.

De acuerdo con la Recomendación R(87) 25 sobre política sanitaria común europea en la lucha sobre el SIDA[28], en el diseño de una política de salud pública en la lucha contra el SIDA son esenciales el principio de voluntariedad, la confidencialidad de la información y el anonimato en la elaboración de estudios epidemiológicos y análisis de grupos de riesgo[29].

En la misma línea, las Directrices internacionales VIH/SIDA y los Derechos Humanos (versión consolidada, 2006) de ONUSIDA establecen la importancia primordial del respeto a la confidencialidad de la información y a la intimidad de la persona infectada con el virus del VIH. En el texto se contienen más de 25 referencias a ambos principios. Ya en el Informe de Naciones Unidas sobre SIDA y Derechos Humanos (Ginebra 1989), resultado de la Primera Consulta Internacional sobre el SIDA y los Derechos Humanos, ya se destacaba que la recogida y almacenamiento de estos datos por parte de las autoridades públicas constituiría una violación del derecho a la vida privada, salvo que esta información estuviese protegida por el más estricto secreto médico y por una anonimato total en el momento de la recogida de los datos, de modo que fuera imposible identificar a la persona a la que se refirieran.

En este Informe se considera que, la notificación obligatoria de esta enfermedad de forma que se permita la identificación de los pacientes, disuadiría a muchos de realizarla las pruebas médicas para la detección del VIH. Por ello, habrá que justificar específicamente esta clara violación del derecho a la confidencialidad *«teniendo en cuenta que pruebas acumuladas que esta forma de proceder disuadiría a alguno –quizás a muchos- posibles portadores del VIH de someterse a las pruebas, sabiendo que su afección, si se comprueba que están afectados por el VIH, sería notificada a la autoridad pública con pormenores que permitirían identificar a la persona afectada»*. Pero, si el sistema respetase las normas más estrictas del secreto médico o, especialmente, *«si la notificación fuese anónima desde el primer momento, es evidente que no habría nada que objetar»* (De Miguel, 2008, p. 306).

En la versión consolidada de las Directrices de ONUSIDA se exige a los Estados que justifiquen específicamente esta violación de la regla de la confidencialidad. En la Tercera Directriz sobre legislación sanitaria, se requiere a los Estados que analicen y reformen su legislación sanitaria *«para que se preste suûciente atención a las cuestiones de salud pública planteadas por el VIH, a ûn de que las disposiciones sobre las enfermedades de transmisión casual no se apliquen indebidamente al VIH y que*

---

[28] Recomendación R(87)25 a los Estados miembros para una política sanitaria europea común para combatir el SIDA del Comité de Ministros del Consejo de Europa de 1987. Ver punto. 2.2.4.

[29] En el mismo sentido, la Recomendación R(89) 14 sobre los aspectos éticos de la infección por el VIH en la atención sanitaria y los entornos sociales del Comité de Ministros del Consejo de Europa, de octubre de 1989. Sobre esta cuestión Vid. De Miguel (2004, p. 124 y ss.).

dichas disposiciones concuerden con las obligaciones internacionales en materia de derechos humanos». Concretamente se solicita de los Estados que su legislación sanitaria debería asegurarse de que la prueba del VIH se realice únicamente *con el consentimiento informado específico del interesado*[30]. Para que se admitiesen excepciones a la voluntariedad de la prueba, *«debería ser necesaria una autorización judicial especial, que se otorgaría únicamente tras evaluar debidamente las consideraciones de libertad e intimidad»*.

Resulta interesante recoger, asimismo, las recomendaciones específicas para la aplicación del derecho a la intimidad en el contexto de la epidemia de VIH. En este ámbito, el derecho a la intimidad comprende obligaciones relativas a la intimidad física, en particular la obligación de pedir el consentimiento informado para las pruebas del VIH y la intimidad de la información, incluida la necesidad de respetar la confidencialidad de todo lo relativo a su situación respecto del VIH.

La protección de su intimidad es especialmente imperiosa por el estigma y la discriminación que acarrearía la falta de confidencialidad si se conoce el estado serológico de una persona. Además si la intimidad no se asegura lo suficiente, las personas no se sentirían seguras para utilizar los servicios y las medidas de salud pública. El interés de la salud pública no justificaría las pruebas o la inscripción del VIH con carácter obligatorio, salvo en casos muy concretos: donaciones de sangre, órganos o tejidos en los que no se analiza a la persona sino al producto humano antes de utilizarlo en otra persona. *«El deber de los Estados de proteger el derecho a la intimidad incluye la obligación de garantizar que se apliquen salvaguardias adecuadas para que no se realicen pruebas sin consentimiento informado, que se proteja la confidencialidad, especialmente en el ámbito de la salud y el bienestar sociales, y que la información sobre el estado serológico con respecto al VIH no se revele a terceros sin el consentimiento de la persona. En este contexto, los Estados deben garantizar también que, al recoger y comunicar datos epidemiológicos, se protegen la información personal relacionada con el VIH así como la intimidad de las personas frente a la injerencia arbitraria de la investigación e información de los medios de comunicación*.

Las recomendaciones internacionales, tanto de ONUSIDA como del Consejo de Europa, van en la misma dirección: garantizar la confidencialidad, intimidad y el anonimato de las personas seropositivas. Por una parte, para impedir su discriminación y estigmatización y, por otra y no menos importante, para que el conocimiento de

[30] En España y según datos del Informe FIPSE Discriminación y SIDA, elaborado por el Instituto de Derechos Humanos Bartolomé de las Casas de la Universidad Carlos III de Madrid, en 2005, al menos en el 11% de los casos, la prueba de detección del VIH se realizó sin el conocimiento y sin el consentimiento de las personas concernidas (página 58).

que tal información puede quedar registrada de una forma no anónima, no disuada a muchas personas de la realización de la prueba, lo que dificultaría enormemente la lucha contra la enfermedad. Pues, debe recordarse que el derecho a la intimidad y a la protección de datos personales exige que la falta de consentimiento para la realización de pruebas médicas que permitan conocer el estado serológico de un paciente debe ser respetada en toda su extensión. Esto es, si una persona se niega expresamente a someterse a una prueba de detección del SIDA, estos derechos se oponen a que la Administración realice *«cualquier tipo de prueba que permitiera sospechar o comprobar la existencia de dicha enfermedad, cuya revelación»* hubiera reusado el interesado[31].

Recordemos que las finalidades del Registro obligatorio de portadores del VIH —según se desprende de sus normas reguladoras, especialmente el Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica y la Orden de 18 de diciembre de 2000, por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH)— son poder detectar problemas de salud pública, valorar los cambios en el tiempo y en el espacio, contribuir a la aplicación de medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud de incidencia e interés nacional o internacional y difundir la información a sus niveles operativos competentes. También y más específicamente, la prevención, gestión y prestación de servicios sanitarios a enfermos con infección por VIH y SIDA.

En mi opinión, como he señalado anteriormente, con la implantación de la historia clínica electrónica resulta muy dudoso que esta medida siga siendo necesaria en una sociedad democrática, de acuerdo con la jurisprudencia del TEDH. Pero, además, según se desprende de las recomendaciones internacionales sobre la materia, tanto del Consejo de Europa como de ONUSIDA, el registro nominal y obligatorio de las personas infectadas con VIH no sería la medida más idónea para asegurar las finalidades relativas a la protección de la salud pública, ya que si los posibles portadores decidieran no realizarse las pruebas médicas por miedo a quedar nominalmente registrados, se produciría probablemente una mayor expansión de la enfermedad.

Por último, de acuerdo con la doctrina del Tribunal Europeo de Derechos Humanos y del Tribunal Constitucional español, la medida restrictiva del derecho a la intimidad y a la protección de datos personales, violaría el principio de proporcionalidad si existen medios menos gravosos para los derechos fundamentales afectados para conseguir las finalidades que justifican la creación del fichero de portadores de VIH, y esa medida sería más idónea porque preservaría el anonimato de las personas

[31] STJCE de 5 de octubre de 1994, Caso X contra la Comisión, C-404/92 P, apartado 23.

que viven con VIH/SIDA, y menos gravosa sería la adopción de un código que permitiese su identificación indubitada y preservase la confidencialidad de la información médica.

Lista de Referencias

Barceló, M. 2008. *Una historia de la informática*. Barcelona: UOC.

Black, E. (2001). *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. S.l.: Crown Publishers.

Carnicero, J. (Coord.). (2003). V informe SEIS «De la historia clínica a la historia de salud electrónica». Pamplona: Sociedad Española de Informática de la Salud (SEIS).

De Miguel, N. (2004). *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público*. Valencia: Tirant lo Blanch.

De Miguel, N. (2008). Análisis de la Sentencia del Tribunal Supremo de 9 de julio de 2007, relativa al fichero sistema de información sobre nuevas infecciones (SINIVIH): una obligada reflexión en torno al principio de seguridad. *Revista jurídica de Castilla y León, (16),* 317.

España. Artículo 1 del Real Decreto 2210/1995, de 29 de diciembre, de Creación de la Red Nacional de Vigilancia Epidemiológica.

España. Tribunal Constitucional español. 254/1993, de 20 de julio. Fundamento jurídico 6º.

España. Tribunal Constitucional español. STC 292/2000, de 30 de noviembre.

España. Tribunal Constitucional español. STC 202/1999, de 8 de noviembre.

España. Tribunal Constitucional español. STC 143/1994, de 9 de mayo.

España. Tribunal Constitucional español. ATC 197/2003, de 16 de junio.

España. *Sistema Nacional de Salud SNS*. Recuperado de http://www.msps.es/organizacion/sns/planCalidadSNS/tic_pnc01.htm#o1

Frosini, V. (1982). *Cibernética, derecho y sociedad*. Madrid: Tecnos.

Ifrah, G. (2001).*The Universal History of Computing. From the abacus to the quantum computer*. New York: John Wiley.

Lucas, P. (1993). *Informática y protección de datos personales*. Madrid: Centro de Estudios Constitucionales.

Martin, J. (1978). *The Wired Society*. Englewood Cliffs, N.J.: Prentice-Hall.

Peces-Barba, G. (2002). La dignidad de la persona desde la filosofía del derecho. En Cuadernos «Bartolomé de las Casas», 26. Madrid: Dykinson.

Pérez, A. E. (1992).Vittorio Frosini y los nuevos derechos de la sociedad tecnológica. (p. 104). En *Informatica e Diritto*, 1-2. Edizioni Scientifiche Italiane.

Ramiro, M. A. (2008). *El VIH/SIDA y el principio de igualdad. Asamblea: revista parlamentaria de la Asamblea de Madrid, (18),* 297.

Ramos, M. A. (s.f.). *La seguridad y la Confidencialidad de la información y la LORTAD. Informática y Derecho, (6-7)*, 133.

Rigaux, F. (1990). *La protection de la vie privée et des autres biens de la personnalité*., Bruxelles : Bruylant.

Ruiz, C. (s.f.). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. s.l.: s.n.

Westin, A.F. (1970). *Privacy and Freedom*., New York: Atheneum.