Centro de Estudios de Consumo

PUBLICACIONES JURÍDICAS
http://centrodeestudiosdeconsumo.com

SISTEMA DE INFORMACIÓN SOBRE NUEVAS INFECCIONES POR VIH (SINIVIH)

PERSPECTIVA DESDE EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Cristina Gil Membrado
cristina.gil@uib.es
Profesora Titular de Derecho Civil
Universidad de las Islas Baleares (UIB)

Fecha de publicación: 6 de septiembre de 2018

Resumen: El equilibrio entre el interés público inherente a la salud pública y el derecho a la intimidad materializado en la protección de datos de carácter personal siempre es complejo. La técnica de la seudonimización de la información, conforme el nuevo régimen de protección de datos de carácter personal, se erige como un ejemplo de conciliación entre la intimidad y la satisfacción del interés público, en cuanto que garantiza el principio de minimización en el tratamiento y la salvaguarda de los derechos fundamentales del interesado. A propósito del ilógico pronunciamiento del Tribunal Supremo en relación al fichero SINIVIH justificado por las necesidades en materia de prevención, de gestión y de prestación de servicios sanitarios a enfermos con infección por VIH y SIDA, se abordarán las bondades de la utilización de procedimientos de seudonimización de la información en materia de salud pública y la frontera con la anonimización de la información.

Palabras clave: Salud pública, vigilancia epidemiológica, protección de datos personales, intimidad, seudonimización

SUMARIO

1. La vigilancia epidemiológica y el derecho a la intimidad 4
2. El sistema de Información sobre nuevas infecciones: el caso del SIDA/VIH 5
   2.1. Los registros de SIDA y la protección de los datos personales 6
   2.2. La Orden de creación del fichero SINIVIH 8
   2.3. El criterio de la Audiencia Nacional: la falta de garantías adecuadas 9
   2.4. La postura del Tribunal Supremo: la valoración ilógica de la prueba ..10
3. La cuestión a la luz del nuevo escenario en protección de datos.....11
4. La seudonimización y la información epidemiológica 13
   4.1. Las bondades de la seudonimización para el fichero SINIVH.....13
   4.2. ¿Cuándo está la información seudonimizada? 14
   4.3. La frontera entre la seudonimización y la anonimización 14
5. Reflexión personal 16
6. Bibliografía.....18

1. La vigilancia epidemiológica y el derecho a la intimidad

La Ley General de Sanidad[1] en su artículo 8 considera la realización de estudios epidemiológicos que sean necesarios para la prevención de los riesgos de la salud como una actividad principal del sistema sanitario, y la creación de registros, como se deriva del artículo 23 con el objeto de mantener un sistema organizado de información sanitaria, vigilancia y acción epidemiológica.

Para recabar esta información, el artículo 41 de la Ley General de Salud Pública[2] (en adelante, LGSP) establece que las autoridades sanitarias para tutelar la salud de la población pueden requerir a los servicios y profesionales sanitarios los informes, protocolos y otros documentos con fines de investigación sanitaria. Por su parte, las personas públicas o privadas están obligadas a ceder los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública.

Es este uno de los supuestos en los que se ha venido limitando la intimidad del paciente en beneficio de la comunidad, de modo que se han venido tratando datos de carácter personal con fundamento en la "concepción comunitaria del derecho a la salud" conforme reza la Exposición de Motivos de la Ley 41/2002[3] (en adelante, LAP). En este sentido, el artículo 16.3 de la LAP si bien establece que el acceso a la historia clínica con fines epidemiológicos asegure el anonimato, en los términos previstos por la LGSP y cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población las administraciones sanitarias podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública[4].

Hay que considerar que si bien el artículo 18.1 CE garantiza el derecho a la intimidad, ello no significa que garantice una intimidad determinada, sino el derecho a poseerla y por ello determinar una esfera personal y familiar a la que terceros no puedan acceder. No obstante, este derecho fundamental, como el resto, no es ilimitado, puesto que en determinadas circunstancias los poderes públicos pueden establecer determinadas medidas para proteger la salud pública que puedan colisionar con el derecho fundamental. Ello reviste la necesidad de ponderar, por un lado, la gravedad de la intromisión en la intimidad, y por otro, valorar si la medida resulta imprescindible para defender el interés público que se trata de proteger. En atención a la doctrina constitucional[5] sobre los límites

[1] Ley 14/1986, de 25 de abril, General de Sanidad (BOE núm. 102, de 29.4.1986).
[2] Ley 33/2011, de 4 de octubre, General de Salud Pública. (BOE núm. 240, de 5.10.2011).
[3] 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 (BOE núm. 274, de 15.11.2002).
[4] Sobre el acceso a la historia clínica con fines epidemiológicos GIL MEMBRADO, C., *La historia clínica. Deberes del responsable del tratamiento y derechos del paciente*, Comares, Granada, 2010, págs. 282ss.
[5] SSTC 2.12.1998 (RTC\1998\231); 17.10.1991 (RTC\1991\197).

y en aplicación del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950[6], la injerencia deberá tener una base legal, perseguir un fin legítimo ser una medida necesaria en una sociedad democrática.

Por el Real Decreto 2210/1995, de 28 de diciembre[7] (en adelante, RD 2210/1995), se crea la Red Nacional de Vigilancia Epidemiológica, con el objeto de recoger y de analizar la información epidemiológica con el fin de detectar problemas y de valorar los cambios en el tiempo y en el espacio, contribuir a establecer medidas de control individual y colectivo de los problemas que supongan un riesgo para la salud a nivel nacional e internacional y de difundir información.

Uno de los instrumentos epidemiológicos reside en la comunicación a las autoridades sanitarias de los casos de enfermedad y de fallecimiento en relación a determinadas enfermedades infecciosas, entre las que se encuentra el SIDA –entre la lista de enfermedades de declaración obligatoria que figuran en el Anexo I del RD 2210/1995-.

Es este un claro límite al derecho fundamental a la intimidad que deriva de la dignidad personal prevista en el artículo 10.1 CE, que si bien garantiza un ámbito de reserva de la vida de la persona exento a la intromisión y vedado al conocimiento de terceros, inclusive poderes públicos, está no obstante limitado en otros derechos.

2. El sistema de Información sobre nuevas infecciones: el caso del SIDA/VIH

En el Capítulo IV del RD 2210/1995 se regula la vigilancia epidemiológica del síndrome de inmunodeficiencia adquirida (SIDA) y de la infección por virus de la inmunodeficiencia humana (VIH).

La infección por el virus de inmunodeficiencia humana (VIH) puede estar presente hasta que se desarrolla la enfermedad durante largos periodos de tiempo. Si bien con la aparición de los tratamientos antirretrovirales se consiguió la disminución significativa de los casos de SIDA, no ha implicado un descenso en las infecciones de VIH, por lo que es una cuestión de salud pública la prevención de infecciones por VIH así como el conocimiento de las prácticas de riesgos a través de las que la enfermedad se transmite. Así la creación de sistemas de información sobre VIH es una necesidad a nivel internacional para el control adecuado de la infección. Desde 1999, la creación y la

[6] Convenio de Protección de los Derechos Humanos y Libertades Fundamentales, de 4 de noviembre 1950 , ratificado por Instrumento de 26 de septiembre 1979 (BOE núm. 243, de 10.10.1979).
[7] Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica (BOE núm. 21, de 24.1.1996).

extensión de sistemas de información sobre VIH se encuentra entre las recomendaciones de los organismos nacionales e internacionales acreditados en cuestiones sanitarias: la Organización Mundial de la Salud; el Programa Conjunto de Naciones Unidas sobre VIH/SIDA (ONUSIDA) y el Centro para el Control de Enfermedades de Atlanta (CDC)[8].

2.1. Los registros de SIDA y la protección de los datos personales

El artículo 8.2 del RD 2210/1995 establece que en todos los niveles de la Red nacional de vigilancia epidemiológica se adoptarán las medidas necesarias para garantizar la seguridad de los datos, incluyendo la confidencialidad como obligación de todos aquellos que en virtud de sus competencias puedan tener acceso a la información.

Los registros de SIDA, tanto a nivel nacional como autonómicos, recogen información sobre los casos de infección de VIH con presencia clínica de una o más de las enfermedades indicativas de SIDA. Son los médicos del sector público y privado la fuente de información y quienes tras diagnosticar al paciente trasladan la comunicación al Registro de SIDA de la Comunidad Autónoma mediante un cuestionario unitario y homogéneo.

El propio artículo 23 de la LAP establece como una obligación a cargo del profesional sanitario cumplimentar los "protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarde relación con los procesos clínicos en los que intervienen, y los que requieran los centros y servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la […] información epidemiológica".

El Registro recoge y trata los datos relativos al nombre, apellidos y fecha de nacimiento de los afectados. En relación a ello, la Agencia de Protección de Datos en el Plan de Inspección de Oficio al Registro Nacional de Sida aclara que estos datos se recogen exclusivamente "para evitar duplicados y poder incorporar información de interés epidemiológico que se genere a posteriori, especialmente los datos del fallecimiento"[9]. Además se recogen datos de sexo, edad, provincia de residencia y país de origen que se utilizan para estudios epidemiológicos.

En la práctica, los datos son recabados por el centro sanitario que atiende al paciente que ha desarrollado SIDA recogiendo los datos en formularios predeterminados.

[8] Decreto 33/2004, de 29 de enero por el que se crea el Sistema de Información Galego sobre la Infección por el Virus de la Inmunodeficiencia Humana (SIGIVIH) (DOG núm. 29, de 11.2.2004).
[9]Plan de Inspección de oficio al Registro Nacional del SIDA.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/REGISTRO_NACIONAL_DEL_SIDA-_2000.pdf

Posteriormente estos formularios se remiten a las Consejerías de Salud de las Comunidades Autónomas, y estas trimestralmente envían la información al Centro Nacional de Epidemiología, en concreto, los nuevos casos y las modificaciones en los ya registrados. Una vez la información ha sido descargada en el Registro Nacional del SIDA, el Centro Nacional de Epidemiología devuelve a la Comunidad Autónoma el fichero de datos por ella generado con el número de caso cumplimentado, además de un fichero con los duplicados.

De lo dispuesto en el artículo 16.3 de la LAP se desprende que el tratamiento de datos con fines epidemiológicos obliga a preservar los datos de identificación personal del paciente separados de los clínico asistenciales, para que quede garantizado, con carácter general, el anonimato.

No obstante, en el ámbito en el que nos movemos, si no se tratara la información personal junto a los datos clínicos se ocasionarían duplicidades, ya que desde distintos centros se podría comunicar el mismo caso. Documentos como el DNI no son suficientes para evitarlo, ya que imaginemos el caso del extranjero con tarjeta de residencia que obtiene posteriormente el DNI: podría ser comunicado como un nuevo caso. Cierto es que si fuera factible utilizar otros medios como la identificación biométrica podría evitarse el tratamiento de datos personales en una de las patologías socialmente más estigmatizantes para el individuo.

La necesaria identificación se pone de manifiesto por el Tribunal Superior de Justicia de Asturias[10] en relación al artículo 34 del RD 2210/1995 donde se establece que "se recogerán los datos individualizados de cada uno de los enfermos diagnosticados". Justifica la identificación de los afectados de SIDA y VIH en que en este momento –y para ello acoge las alegaciones de la Administración- no es posible mediante códigos anónimos evitar el riesgo de confusión y duplicación, si bien el Tribunal insta a la Administración a que desde ese momento haga realidad, mediante los nuevos adelantos tecnológicos, la posibilidad de garantizar el anonimato.

No plantea cuestión alguna el tratamiento posterior de información disociada acerca de sexo, edad, provincia de residencia, país de residencia y de origen para estudios epidemiológicos, así como para su cesión al Centro Europeo de la Organización Mundial de la Salud, donde se centraliza a nivel europeo la información sobre SIDA y al Instituto Nacional de Estadística, ya que los datos se remiten anonimizados, de

[10] STSJ Asturias, 12.9.2005 (RJ\2007\330).

modo que el interesado deja de ser identificable[11].

2.2. La Orden de creación del fichero SINIVIH

Mediante Orden de 18 de diciembre de 2000 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)[12] que se justifica por las necesidades en materia de prevención, de gestión y de prestación de servicios sanitarios a enfermos con infección por VIH y SIDA, al amparo del RD 2210/1995.

La finalidad del fichero es "aportar información específica 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. Para la realización de estadísticas periódicas y para contribuir a la investigación científico-médica".

Como personas afectadas lo son los diagnosticados de infección por VIH en los centros del Sistema Nacional de Salud.

El procedimiento de recogida es mediante formulario de notificación de casos en soporte magnético por parte de las Comunidades Autónomas.

Los datos de carácter personal a incluir en el fichero son: "Identificador personal: Iniciales del nombre y apellidos. Centro sanitario de diagnóstico. Fecha de nacimiento. Sexo. Provincia de residencia. País de residencia. País de origen. Mecanismos de transmisión de la infección. Datos clínicos. Datos de laboratorio".

Las cesiones previstas de datos procedentes del fichero tienen como destinatarios: "Organización Mundial de la Salud/Centro Europeo para la Vigilancia Epidemiológica del VIH (datos anónimos). Comunidades Autónomas. Organismos de investigación".

[11] "[…] los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". Considerando 26 del 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 (DOUE, de 4.5.2016).

[12] 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) (BOE núm. 11, de 12.1.2001).

2.3. El criterio de la Audiencia Nacional: la falta de garantías adecuadas

Esta Orden Ministerial fue recurrida por una serie de colectivos afectados ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional, que por Sentencia de 24 de marzo de 2004[13], la declara nula por no ser conforme a Derecho a consecuencia del incumplimiento de las medidas de garantía adecuadas para salvaguardar la intimidad de los afectados, ya que la estructura informática del fichero permitía a terceros, mediante manipulación, obtener información personal sin estar legitimados para ello.

De la prueba pericial se deriva que en relación a las medidas de seguridad del fichero, salvo omisiones de escasa relevancia, el grado de cumplimiento es satisfactorio[14], sin embargo el perito ingeniero no considera que se actúe correctamente en relación al tratamiento de la información personal. Estima el perito que el método utilizado para el tratamiento de los datos 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", ya que aunque de modo aislado los datos no permitan la identificación, la conjunción de varios sí la permiten, al ser contrastados con otras fuentes de información (por ejemplo el Registro Civil). A su vez, considera que los indicadores personales pueden dar lugar a confusión y a repeticiones de datos por aproximación familiar, y duplicidad, sobre todo en casos de nombres y apellidos compuestos. En definitiva, la conclusión es que la ficha que deriva de este tratamiento de datos dispone de la suficiente información como para asociarla a una persona concreta con un alto grado de evidencia y, a su vez, carece de los datos suficientes como para identificar con plena certeza a una persona para la posterior rectificación o cancelación de la información. El perito considera que en lugar de la identificación por las iniciales del nombre y apellidos, la seguridad se garantizaría empleando un código numérico solo conocido por la Administración y el afectado.

Este informe pericial es el motivo por el que la Sala anula la Orden impugnada y añade que conforme a doctrina constitucional "un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro,

[13] SAN, 24.3.2004 (RJCA\2004\409).

[14] En aquel momento según disposiciones establecidas en el RD 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (BOE núm. 151, de 25.6.1999). Disposición derogada por Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17, de 19.1.2008).

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 ésta" [15].

2.4. La postura del Tribunal Supremo: la valoración ilógica de la prueba

El Abogado del Estado sostiene en vía de recurso que si bien la valoración de la prueba no es revisable en casación, ello no obsta para proceda en los casos en los que el resultado es absurdo o contradictorio, como considera que acaece en este caso a colación de la resolución dictada por la Audiencia Nacional.

Alega que teniendo en cuenta que del informe pericial se desprende con claridad que el fichero SINIVIH cumple con todos los requisitos y medidas de seguridad y que la única tacha que se plantea es que la asignación de un código alfanumérico podría permitir, a través de una serie de operaciones, que terceros extraños identifiquen a una persona, el ingeniero, en este particular, está especulando sobre cuestiones fantasiosas propias de "inteligencia" y espionaje, que aunque puedan resultar sugerentes o sugestivas, nada tienen que ver con el ajuste o no a disposiciones legales y reglamentarias. Así el Abogado del Estado considera que "las diferentes cuestiones planteadas deben abordarse con seriedad y equilibrio, sin buscar patologías de laboratorio".

La Sala acoge el motivo de casación en tanto en cuanto considera el dictamen pericial contradictorio en sí mismo derivando, así, en un resultado ilógico de la prueba.

El debate, para la Sala, tendría que haberse ceñido a un mero control de legalidad respecto a si las medidas establecidas en el fichero son acordes a las de nivel alto previstas reglamentariamente. No corresponde, para la Sala, a los órganos jurisdiccionales un control de oportunidad acerca de cuál puede ser el método más adecuado o si hay un método mejorable no previsto en la norma.

El dictamen pericial controvertido se aporta posteriormente también a los autos de una serie de recursos ante el Tribunal Superior de Justicia de Galicia contra el Decreto 33/2004, de 29 de enero, por el que se crea el sistema de información gallego sobre la infección por el virus de inmunodeficiencia humana de la Xunta de Galicia[16] (en adelante, Decreto 33/2004).

[15] SAN, 24.3.2004 (RJCA\2004\409).
[16] Decreto 33/2004, de 29 de enero por el que se crea el Sistema de Información Galego sobre la Infección por el Virus de la Inmunodeficiencia Humana (SIGIVIH) (DOG núm. 29, de 11.2.2004).

En todos los casos se hace extensible el razonamiento realizado en la Sentencia del Tribunal Supremo de 9 de julio de 2007 en relación a SINIVIH por lo que no se aprecia en el Decreto 33/2004 vulneración del derecho a la intimidad ni infracción de la legalidad vigente, ya que el control jurisdiccional debe ceñirse a la actuación de la Administración, conforme determina el artículo 106.1 CE, de modo que no cabe acoger el recurso por cuestiones de conveniencia o de oportunidad, por lo que siendo el fichero acorde a la normativa no cabe estimar la pretensión de nulidad de dicho Decreto[17].

Con posterioridad, es el propio Tribunal Supremo el que se reafirma[18] en la postura sostenida en su resolución de 9 de julio de 2007 en relación a pronunciamientos del Tribunal Superior de Justicia de Galicia declarando la suspensión cautelar del Decreto 33/2004. Dicha suspensión se acordó a consecuencia del "evidente peligro, aun hipotético de que pueda resultar comprometida la intimidad y la vida privada de los ciudadanos, a través de un registro de datos personales y médicos en relación a una enfermedad que, por su específica naturaleza, alcance y trascendencia social, exige mayores garantías de sigilo". Para el Tribunal Supremo, el Decreto 33/2004 cumple con la consecución del interés general, que no es otro que el conocimiento de los nuevos diagnósticos de infección por VIH y las causas que lo originan para seguir la evolución de la epidemia y su control, así como el tratamiento de los afectados, primando este interés general sobre el derecho a la intimidad particularmente considerado. Considera la Sala que "la suspensión no debió acordarse al no estar acreditado el perjuicios 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".

Tampoco fue apreciada la alegación de la doctrina de la apariencia de buen derecho a consecuencia del paralelismo entre el Decreto 33/2004 y la Orden Ministerial que todavía no había sido anulada por la Audiencia Nacional.

3. La cuestión a la luz del nuevo escenario en protección de datos

Considerar que el perito estaba rozando la ciencia ficción cuando lo que únicamente proponía es el tratamiento más acorde con la salvaguarda de la intimidad de conformidad

[17] STSJ Galicia, 1.10.2008 (RJCA\2009\309); STSJ Galicia, 23.4.2008 (RJCA\2008\559); STSJ Galicia, 16.1.2008 (RJCA\2008\700); RJCA Galicia 21.5.2008 (RJCA\2008\285).
[18] SSTS 26.9.2007 (RJ\2007\7611); 14.12.2007 (RJ\2007\9361).

a las medidas establecidas por el Reglamento de seguridad[19] y derivadas de la Ley Orgánica de Protección de Datos[20] mediante el tratamiento de datos adecuados, pertinentes y no excesivos –en este caso la utilización de un código numérico con preferencia al nombre y apellidos- supone por parte del Tribunal Supremo ignorar la conveniencia de utilizar los procedimientos de seudonimización de la información, realidad que ha venido siendo habitual especialmente en el ámbito sanitario –basta pensar en el número de historia clínica que hace identificable al paciente para quien tenga acceso al fichero maestro que vincula dicho número con un paciente concreto-[21].

De hecho, el RGPD introduce en su artículo 4.5 la definición de seudonimización refiriéndose a este procedimiento que es una constante como baluarte del nuevo régimen en cuanto que garantiza "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Como antecedentes a la nueva normativa en materia de protección de datos, podemos hacer alusión a los procedimientos que la Ley de Investigación Biomédica[22] viene proponiendo para el tratamiento de las muestras biológicas, situando la seudonimización entre el tratamiento de datos de persona claramente identificada y el tratamiento de datos anonimizados o disociados. En este mismo sentido, la Agencia de Protección de Datos (en adelante, APD) viene, desde hace mucho tiempo, ensalzando las bondades de la seudonimización como un método mediante el que sin producir la desidentificación irreversible se puede conciliar el tratamiento de datos y la protección de la intimidad[23]. Precisamente el método propuesto por el ingeniero para el fichero SINIVIH fue la seudonimización por medio de códigos alfanuméricos en sustitución de las iniciales del nombre y de los apellidos.

Nos interesa el futuro de esta cuestión a la luz del Reglamento General de Protección de

[19] RD 994/1999.
[20] Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 298, de 14.12.1999).
[21] Sobre la historia clínica y la protección de su información personal véase GIL MEMBRADO, C., *La historia clínica. Deberes del responsable del tratamiento y derechos del paciente*, Comares, Granada, 2010.
[22] Ley 14/2007, de 3 de julio, de Investigación biomédica (BOE núm. 159, de 4.7.2002).
[23] A modo de ejemplo, véase el Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la Farmacovigilancia.
http://www.farmaindustria.es/web/documento/codigo-tipo-de-farmaindustria-de-proteccion-de-datos-personales-en-el-ambito-de-la-investigacion-clinica-y-de-la-farmacovigilancia-2/

Datos[24] (en adelante RGPD) y de la proyectada LOPD[25] (en adelante, PLOPD).

4. La seudonimización y la información epidemiológica

El ingeniero que elaboró el informe sobre el tratamiento de información en el fichero de SINIVIH no incurre en contradicción alguna al señalar que si bien las medidas de seguridad estaban implantadas correctamente procedía utilizar otro sistema distinto a las iniciales del nombre y apellidos como podría ser un código numérico. Quizá fue demasiado tajante al afirmar categóricamente que no había nada que objetar a la observancia de las medidas de seguridad, ya que sin duda la seudonimización cuando sea posible manteniendo la posibilidad de llevar a cabo el uso o la finalidad pretendida es parte de esas medidas de seguridad para el manejo de la información personal con garantías adecuadas.

Con todo, si bien en la práctica, y especialmente en el ámbito sanitario y de investigación biomédica la utilización de información y de muestras biológicas seudonimizadas ha sido constante y además promovido y aceptado por la APD, como ya hemos avanzado, actualmente es la nueva normativa de protección de datos la que viene a fijar expresa y claramente esta modalidad como una manera de tratar los datos protegiendo la intimidad del afectado.

Así, la utilización de un código numérico en el fichero de información sobre nuevas infecciones implicará el uso de datos personales de modo que no puedan atribuirse al interesado sin utilizar información adicional, que se encuentre almacenada por separado y sometida a medidas técnicas y organizativas adecuadas[26].

4.1. Las bondades de la seudonimización para el fichero SINIVH

Las enfermedades infecto-contagiosas tienen un carácter estigmatizante *per se*, y el SIDA es quizá el paradigma de ello, por lo que hay que extremar las cautelas en la salvaguarda de la información personal que a esta enfermedad transmisible haga referencia[27].

El RGPD considera la seudonimización como un método óptimo para el cumplimiento del principio de protección de datos desde el diseño y por defecto, lo

[24] 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 (DOUE, de 4.5.2016).
[25] Proyecto de Ley Orgánica de Protección de Datos (BOCG, núm. 13.1 de 24.11.2017).
[26] Art. 4.5 RGPD.
[27] SÁNCHEZ CARAZO, C., *La intimidad y el secreto médico*, Díaz de Santos, Madrid, 2000, págs. 216ss.

que implica adoptar las medidas técnicas y organizativas necesarias para garantizar que la información tratada sea la mínima posible conforme al principio de minimización en el tratamiento de datos personales.

Conforme a lo dispuesto en el artículo 25 del RGPD, el responsable del tratamiento tiene que valorar el estado de la técnica, el coste de la aplicación, la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos que entraña el tratamiento para los derechos y libertades de la persona, medidas técnicas y organizativas adecuadas como la seudonimización[28]. En realidad, esta modalidad de tratamiento es coincidente con la propuesta por el perito ingeniero, es decir, consiste en la sustitución de la identificación directa de los afectados por VIH/SIDA por un código numérico que solo la Administración y el afectado pudiera conocer, en beneficio de los principios de protección de datos, como el de minimización –que no es otro que el tratamiento de datos adecuados, pertinentes y no excesivos, y por lo tanto ya previsto en la normativa anterior-.

4.2. ¿Cuándo está la información seudonimizada?

El Considerando 26 del RGPD deja claro que la información seudonimizada es información personal, puesto que hace referencia a persona identificable. Es decir, quien tenga posibilidad de acceder al fichero que vincula el código numérico al que se refería el perito informático, estará tratando información de carácter personal cuando trate datos albergados en el fichero SINIVIH.

Para determinar si el proceso aplicado a la información hace que la persona sea identificable y por lo tanto estamos ante información seudonimizada hay que tener en cuenta todos los medios que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar bien sea directa o indirectamente a la persona física.

El responsable del tratamiento del fichero SINIVIH es el Centro Nacional de Epidemiología del Instituto de Salud Carlos III. Por lo tanto, para determinar si los datos están seudonimizados es necesario precisar si existe una probabilidad razonable de identificar a la persona a la que se refieren. Para ello deben utilizarse factores como los costes y el tiempo necesario para la reidentificación teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

4.3. La frontera entre la seudonimización y la anonimización

La normativa de protección de datos no es aplicable, sin embargo, cuando se trata

[28] Véase en relación a la seudonimización como garantía el Considerando 78 del RGPD.

información anónima, que es la que no tiene ninguna relación –ni de modo remoto- con persona física identificada o identificable. Tampoco se aplica a los datos anonimizados o disociados irreversiblemente, de modo que el individuo deje de ser identificable, por lo menos acudiendo a métodos razonables.

Cabe precisar que la disociación entendida como irreversible no es más que una utopía ya que siempre existen riesgos inherentes al proceso que suponen una potencial posibilidad de reidentificación[29], por ello el límite es fijado en la razonabilidad de vincular determinada información a la persona –o a la familia- a la que hace referencia.

Así, conforme apuntó la APD en el informe jurídico 0283/2008[30] para ser considerada disociada una información sería necesario que no resulte posible la asociación a la persona o que exija un esfuerzo tan desproporcionado que sea suficiente para disuadir a quien tenga la posibilidad.

En este caso concreto, es posible identificar a la persona de modo razonable desde el momento en que la Administración tiene la posibilidad de acceder al fichero maestro para vincular el código numérico con el afectado, por lo que nos encontramos ante datos seudonimizados. Este sería el método óptimo de tratamiento de información en el fichero SINIVIH teniendo en cuenta que es preciso el seguimiento de los casos y la plena identificación de estos para evitar errores y duplicidades, por lo que no es factible incorporar datos irreversiblemente disociados, sino que el límite conforme a la finalidad establecida estaría en la información seudonimizada. De hecho, el propio perito ingeniero dejaba constancia en su informe de la debilidad de tratar la información mediante la constancia de las iniciales de nombre y apellidos, que daban lugar a confusiones y repeticiones especialmente en los casos de nombres y de apellidos compuestos[31]. En este sentido se pronuncia también la APD en el Plan de inspección de oficio al Registro Nacional del Sida[32]. Por lo tanto el método utilizado,

[29] Dictamen 5/2014 del Grupo de Trabajo sobre Protección de Datos de Carácter Personal del artículo 29, de 10 de abril de 2014.
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
APD. Orientaciones y garantías en los procedimientos de anonimización de datos personales.
https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf
[30] Informe Jurídico 0283/2008 APD.
https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2008-0283_El-n-uu-mero-de-historia-cl-ii-nica-que-pueda-asociarse-con-la-identidad-del-paciente-es-un-dato-de-car-aa-cter-personal.pdf
[31] SAN, 24.3.2004 (RJCA\2004\409).
[32] Extracto de las Recomendaciones de 9 de marzo de 2000 dictadas por el Director de la Agencia de Protección de Datos, Juan Manuel Fernández López.

conforme expresaba el ingeniero en su informe, ni garantiza la intimidad ni evita duplicidades y errores.

5. Reflexión personal

El nuevo escenario de protección de datos de carácter personal requiere que mediante normativa interna se concreten determinados aspectos sobre el tratamiento de datos de salud en el ámbito de la salud pública, donde la proyectada Ley Orgánica de Protección de Datos deberá precisar la gran cantidad de conceptos jurídicos indeterminados que utiliza la norma europea además de colmar las remisiones que el legislador europeo realiza a la normativa interna.

El artículo 9.2.i del RGPD establece el interés público en el ámbito de la salud pública como base legitimadora del tratamiento de datos personales, si bien supedita su régimen al Derecho de la Unión y de los Estados miembros, que deberán establecer medidas adecuadas y específicas para proteger los derechos y libertades del interesado.

Sin perjuicio de la indeterminación de concepto salud pública, que puede generar dudas respecto a la subsunción o no de aquellos estudios epidemiológicos cuya finalidad sea mejorar la salud de la población (como la investigación sobre causas del cáncer) los que tendrían mejor encaje en el régimen previsto para la investigación científica en general[33], no cabe duda que la información sobre nuevas infecciones de declaración obligatoria tiene cabida dentro de la noción de interés público en el ámbito de la salud pública y por lo tanto es legítima la comunicación de información a la Administración sin consentimiento del interesado.

En este sentido, la Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS)[34] propone una definición de salud pública a incluir en el PLOPD que abarca

---

http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/REGISTRO_NACIONAL_DEL_SIDA-_2000.pdf

Sobre investigación en general y la interpretación de la Agencia de Protección de Datos del nuevo escenario de tratamiento de datos personales con fines de investigación véase el Informe Jurídico APD 073667/2018 sobre la incidencia que en el ámbito de la investigación biomédica va a producir la aplicación de la nueva normativa de protección de datos.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2018-0046_Investigaci-oo-n-biom-ee-dica.pdf

[33] En este sentido, BELTRÁN AGUIRRE, J.L., GARCÍA LÓPEZ, F.J., NAVARRO SÁNCHEZ, C., *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, SESPAS, Barcelona, 2017, pg. 10.
http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/

[34] http://sespas.es/

claramente "los estudios epidemiológicos necesarios para la prevención de un riesgo grave e inminente para la salud de la población" y "la vigilancia epidemiológica de las enfermedades de declaración obligatoria"[35]. En este sentido "La autoridad sanitaria y los órganos competentes de las Administraciones sanitarias a los que se refiere la Ley 33/2011, General de Salud Pública, podrán recabar la comunicación de datos personales en poder de cualquier Administración o de entidades privadas cuando el conocimiento de tales datos resulte necesario para el desempeño de sus funciones legítimas de tutela de la salud pública"[36].

Ahora bien, la exención de consentimiento no implica la relajación respecto de otras obligaciones y garantías fijadas en la nueva normativa de protección de datos, como la protección desde el diseño y por defecto que implica que considerando el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplique tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización[37]. Además, la minimización en el tratamiento de la información personal, entendida como el tratamiento de datos adecuados, pertinentes y limitados a los necesarios en relación con la finalidad[38], implicará que en la medida de lo posible la información personal sea siempre utilizada de modo seudonimizado si es compatible este método con la finalidad determinada.

Como ya hemos expuesto, no es posible en este ámbito el uso de información disociada, por lo que la mejor manera de garantizar los derechos fundamentales del afectado es tratar la información de modo seudonimizado, mediante la vinculación de un código numérico como el perito ingeniero manifestó en su informe, tan dura e ilógicamente tratado por el Tribunal Supremo.

No obstante, cabe aclarar que si bien el procedimiento de seudonimización es más tuitivo con la protección de la intimidad del afectado, no garantiza en absoluto la intimidad a ultranza ya que la revelación de la identidad del afectado es muy sencilla al existir un vínculo al que se puede acceder mediante esfuerzos no desproporcionados, por lo que no se dejan de tratar datos de carácter personal motivo por el cual no cabe relajar las garantías ni un ápice y menos en el manejo de datos tan sensibles como los relativos a la salud en

[35] Idem, pg. 8
[36] Idem, pg. 9
[37] Art. 25 RGPD.
[38] Art. 5.c RGPD.

general y, en concreto, a los que hacen referencia al VIH/SIDA, cuyo tratamiento está más que justificado por el interés público inherente a la salud pública.

6. Bibliografía

APD. Informe Jurídico 0283/2008 sobre el carácter de dato personal del número de historia clínica que pueda asociarse con la identidad del paciente.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2008-0283_El-n-uu-mero-de-historia-cl-ii-nica-que-pueda-asociarse-con-la-identidad-del-paciente-es-un-dato-de-car-aa-cter-personal.pdf

APD. Informe Jurídico 073667/2018 sobre la incidencia que en el ámbito de la investigación biomédica va a producir la aplicación de la nueva normativa de protección de datos.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2018-0046_Investigaci-oo-n-biom-ee-dica.pdf

APD. Orientaciones y garantías en los procedimientos de anonimización de datos personales.

https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

BELTRÁN AGUIRRE, J.L., GARCÍA LÓPEZ, F.J., NAVARRO SÁNCHEZ, C., *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, SESPAS, Barcelona, 2017.

http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/

Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la Farmacovigilancia.

http://www.farmaindustria.es/web/documento/codigo-tipo-de-farmaindustria-de-proteccion-de-datos-personales-en-el-ambito-de-la-investigacion-clinica-y-de-la-farmacovigilancia-2/

Dictamen 5/2014 del Grupo de Trabajo sobre Protección de Datos de Carácter Personal del artículo 29, de 10 de abril de 2014.

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

GIL MEMBRADO, C., *La historia clínica. Deberes del responsable del tratamiento y*

derechos del paciente, Comares, Granada, 2010.

Plan de Inspección de oficio al Registro Nacional del SIDA.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/REGISTRO_NACIONAL_DEL_SIDA-_2000.pdf

SÁNCHEZ CARAZO, C., *La intimidad y el secreto médico,* Díaz de Santos, Madrid, 2000.