European Pharmaceutical Law Group

Comentario a la Sentencia de la Audiencia Nacional de 24 de marzo de 2004 que anula la Orden de 18 de diciembre de 2000, sobre creación de fichero de datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH)

Francisco Almodóvar
Resp. Dept. Protección de Datos Eupharlaw (European Pharmaceutical Law Group)

Madrid, 18 de mayo de 2004

Estamos ante una de las Sentencias más destacadas que se han dictado contra un fichero de datos de carácter personal gestionado por una Administración Pública. La Audiencia Nacional lo anula por no cumplir con las medidas de seguridad (técnicas y organizativas) que requiere la legislación de protección de datos de carácter personal (Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal y Real Decreto 994/1999, de 11 de junio, de Medidas de Seguridad).

LA SENTENCIA DESAPRUEBA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN POR PARTE DE LA ADMINISTRACIÓN

El fichero en cuestión, regula la información relativa a las necesidades en materia de prevención, de gestión y prestación de servicios sanitarios a enfermos con infección por VIH y SIDA, al amparo del Real Decreto 2210/1995, de 29 de diciembre, de Creación de la Red Nacional de Vigilancia Epidemiológica.

Aparentemente, este fichero es legal, justifica su finalidad y razón de ser amparándose en varias normativas de carácter sanitario: art. 8.1 de la Ley 14/1996, de 25 de abril, General de Sanidad, "De la intervención pública en relación con la salud individual y colectiva" que justifica esta base de datos en aras del interés público y la salud pública; el RD 2210/1995 ya citado, donde se considera al SIDA como de declaración obligatoria,; y el art. 23 de la Ley Básica 41/2002, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo tenor dice así: *"Los profesionales sanitarios, [...] tienen 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".*

Además, la Agencia Española de Protección de Datos (AEPD) le dio cobertura en la fase de creación, ya que cumple con todos los requisitos de constitución. Al ser un fichero de titularidad pública, la creación, modificación o supresión sólo podrá hacerse por medio de disposición general, y fue creado por la Orden de 18 de diciembre de 2000.

Este es el cuerpo del fichero, según los datos obtenidos de Registro General de Protección de Datos:

Tipo de administración:	ADMINISTRACION GENERAL DEL ESTADO
Responsable del fichero:	MINISTERIO DE SANIDAD Y CONSUMO INSTITUTO DE SALUD CARLOS III CENTRO NACIONAL DE EPIDEMIOLOGIA
Nombre del fichero:	**SINIVIH**
Descripción:	SISTEMA DE INFORMACION SOBRE NUEVAS INFECCIONES POR VIRUS DE LA INMUNODEFICIENCIA HUMANA
Dirección de acceso:	C SINESIO DELGADO, 6 28029 MADRID

Finalidad: APORTAR INFORMACION ESPECIFICA A LA AMDINISTRACION SANITARIA SOBRE LA INCIDENCIA Y EVOLUCION DE LOS NUEVOS DIAGNOSTICOS DE INFECCION POR VIH, PARA CONOCER LOS FACTORES QUE LA DETERMINAN Y DEFINIR ESTRATEGIAS DE PREVENCION. REALIZACION DE ESTADISTICAS PERIODICAS Y CONTRIBUCION A INVESTIGACION CIENTIFICO-MEDICA

Disposición General: BOLETÍN OFICIAL DEL ESTADO Nº 00011

Fecha: **12-01-2001**

LA AEPD DEBE DE GARANTIZAR EL DERECHO A LA PROTECCIÓN DE DATOS

La Sentencia argumenta de una manera coherente, con respecto a la seguridad, la anulación de este fichero; ya que no reúne las condiciones de seguridad legalmente establecidas. Y permite identificar al paciente-ciudadano portador del virus del SIDA, facilita conocer quién es esa persona, dónde vive, a qué centro de salud acude normalmente, por qué médico es atendido, etc:: *"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 el contrario, dice el perito, en lugar de la identificación por las iniciales del nombre y apellidos, la seguridad estaría garantizada mediante el empleo de un código alfanumérico conocido sólo por la Administración y el afectado"*.

EL FICHERO SINIVIH PERMITE ASOCIAR A UNA PERSONA LOS DATOS RECOGIDOS CON ALTO GRADO DE EVIDENCIA. ES NECESARIO EL EMPLEO DE CÓDIGOS ALFANUMÉRICOS

Las tecnologías de la información y de la comunicación están rediseñando el mundo, las relaciones personales, sociales, políticas y económicas. Pero esta transformación tiene un precio. Vivimos en la sociedad de la información, y esto quiere decir que es justamente la información la que viene a constituir ahora la materia prima más importante y que, dentro de la información, los datos personales son especialmente preciados.

SOCIEDAD DE LA INFORMACIÓN + SEGURIDAD + ORGANIZACIÓN = SOCIEDAD DEL CONOCIMIENTO

Como manifiesta Gonzalez de Pablo, A., en su libro "El SIDA enfermedad moral", *"la concepción del SIDA como enfermedad moral y enfermedad vergonzosa seguirá operando con toda su fuerza hasta que una vacuna o una cura efectiva sea descubierta"*. Tiene razón. El perfil que nos hacemos de este tipo de enfermos gira en torno a la promiscuidad sexual, la duda de si será homosexual, si podrá trabajar en las mismas condiciones, la imagen que dará a mi empresa o institución, etc.

Al mismo tiempo, el Estado es garante de la seguridad pública y del interés social. Necesita estudiar, controlar, prevenir este tipo de enfermedades, destructivas del ser humano.

El Poder Estatal, aprovechando las nuevas tecnologías de almacenamiento y tratamiento de la información, necesita de este tipo de bases de datos. Ahora bien, todo tiene su parte negativa y positiva. Lo positivo: interés general y razones de salud pública. Negativo: no hay garantías para el ciudadano-paciente del control y disponibilidad de la información relativa a su salud. Es ésta la razón por la cual la protección de datos asume una importancia creciente, que la conduce cada vez más hacia el centro del sistema político-institucional.

En esta Sentencia se da un toque de atención importante al poder político. Si el Estado necesita de datos personales, es correcto que los tenga, pero debe tratarlos de forma que se

respete la dignidad del ser humano y sus libertades fundamentales. En este caso, no es la intimidad el derecho fundamental más perjudicado, ni el honor incluso, sino el derecho fundamental a la protección de datos. El control y el acceso de la persona a la información que le identifica y le hace identificable, debe ser el límite a la vigilancia.

EL DERECHO FUNDAMENTAL PERJUDICADO ES EL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, EJE DE LA SOCIEDAD DE LA INFORMACIÓN

Las modernas técnicas de rastreo por diferentes bases de datos electrónicas y de configuración de perfiles personales son muy poderosas. Y cada vez lo serán más. La Administración ya no sólo tiene que velar por el interés general y salud pública en cuanto a este tipo de enfermedades, sino también, y en igual medida, debe garantizar el derecho fundamental a la protección de datos personales. Debe investigar y adquirir las últimas tecnologías de seguridad de la información. Disociar y re-disociar este tipo de datos en múltiples capas de acceso y perfiles de tratamiento, utilizar las modernas técnicas de cifrado, formar al personal y garantizar el deber de secreto y la confidencialidad de los usuarios de estos datos.

ENCRIPTACIÓN + DISOCIACIÓN = SEGURIDAD DE LA INFORMACIÓN

Nace así un "habeas data", una nueva comprensión de los derechos de la personalidad. Los efectos sociales de la utilización de nuevas tecnologías de la información y la comunicación son poderosos. Innovar tiene sus consecuencias, pero si se hace uso de estas nuevas herramientas hay que mantener un mismo criterio y unidad de actuación.

El número de sentencias de este estilo se incrementará en los próximos años, a medida que el derecho fundamental de la protección de datos de carácter personal vaya tomando cuerpo y sustancia.

Precedentes jurisprudenciales más relacionados con esta Sentencia:

- Tribunal Supremo: Sentencia 18 de febrero de 1999. Asunto: publicación en un medio periodístico sobre personas afectadas por el síndrome en modo que resultan identificables; incurriéndose en un delito contra la libertad informática o habeas data, tipificado en el artículo 197.2 del Código Penal, al ponerse en contacto datos personales cruzados extraídos de dos ficheros informáticos.

- Tribunal de Justicia del Principado de Asturias (Sala Contencioso-Administrativo): Tras un recurso contra el Registro de SIDA de la Consejería de Servicios Sociales del Principado de Asturias, la Sentencia acuerda suspender la el registro recurrido en cuanto lleva aparejada la identificación personal de los presuntos afectados al constar nombre y apellidos de los mismos, por lo que se acuerda la suspensión en lo que se refiere a la constancia de tales datos.

Inspección de la **Agencia Española de Protección de Datos** en 1998 al Registro Nacional del SIDA, inscrito en dicha Agencia en 1994 por el Ministerio de Sanidad. La AEPD hizo varias Recomendaciones que giraron en torno al mantenimiento de equilibrio entre la confidencialidad y el interés general.

Informe de la Segunda Consulta internacional sobre VIH/SIDA y derechos humanos de la ONU: "Es evidente que la inscripción del nombre de una persona en un registro llevado por una autoridad pública de los que en la práctica sería considerado como una lista de individuos posiblemente peligrosos para la comunidad constituiría una grave violación de la vida privada de aquella persona".

La Sentencia que estamos comentando argumenta la anulación del citado fichero en el derecho fundamental a la intimidad, pero basándose en la legislación de protección de datos de carácter personal. Se equivoca. Estas situaciones no afectan sólo al derecho a la intimidad, al honor, sino también al de la igualdad, al de la integridad física y moral, etc. Por lo tanto, no es una cuestión única de protección a la intimidad, es algo más, es el nuevo

derecho fundamental a la protección de datos de carácter personal. Podemos decir, en palabras de Stefano Rodotà, Presidente de la 'Autorità per la Privacy' y Ex Presidente del Grupo de Trabajo de Autoridades Europeas de Protección de Datos, que *"la protección de los datos personales se presenta como una precondición por la actuación de estos derechos 'viejos' y como elemento básico de los derechos 'nuevos' en la edad de la tecnología. Es restrictivo y peligroso decir que 'nosotros somos nuestros datos'. Pero es verdad que, en la protección de datos, se refleja ya una dimensión esencial de la libertad de los contemporáneos".*

DERECHOS VIEJOS----D. PROTECCIÓN DE DATOS----DERECHOS NUEVOS

De esta manera, nos encontramos que la Administración, por el bien común, necesita manejar datos, de manera personalizada en algunas ocasiones, pero también es cierto que todavía no está preparada ni garantiza el nuevo derecho fundamental. Para ello es necesario: utilización de las últimos avances en tecnologías de la seguridad de la información (cifrado, perfiles de acceso, antivirus y demás), formación del personal, asunción de responsabilidades jurídicas y organización-gestión adecuada de la información.

INVERSIÓN EN TECNOLOGÍAS + FORMACIÓN EN TRATAMIENTO DIGITALIZADO DE LA INFORMACIÓN = PROGRESO TECNOLÓGICO

La Administración ya se está dando cuenta de las nuevas necesidades derivadas del progreso de las tecnologías de la información y la comunicación, y viéndose desbordada, acude al denominado "outsourcing", contratar empresas privadas para ofrecer el servicio de gestión de la seguridad de la información. Se une así lo público y lo privado. Cobran una enorme importancia los contratos de confidencialidad y deber de secreto. Nace la necesidad de la autorregulación, es decir, elaborar códigos tipo de conducta que concilien, organicen y responsabilicen de una manera dialogada los intereses públicos y privados, en aras del respeto a la protección de datos de carácter personal.

PUBLICO + PRIVADO = CÓDIGOS TIPO

El Ministerio de Sanidad, actualmente, tiene inscritas muchas bases de datos (Interrupción Voluntaria del Embarazo, Registro Estatal de Lepra, Registro Nacional de SIDA, Registro Enfermedad Declaración Obligatoria, entre otras) con finalidades similares al fichero que ha sido anulado, que deberían cumplir con las garantías jurídicas requeridas.

Los datos tienen que ser actualizados, pertinentes, no excesivos. Se ha de informar al paciente-ciudadano-usuario de los servicios sanitarios de sus derechos de acceso, oposición, cancelación, rectificación e impugnación.

La utilización de este tipo de base de datos, debe de guiarse por una finalidad explícita, de salud e interés público, y cuando no sea así, habrá que requerir la actuación del Poder Judicial, siempre en aras de respetar la dignidad de la persona y sus libertades fundamentales, que en este caso vienen representadas por el nuevo derecho fundamental a la protección de datos de carácter personal, que engloba, justifica y cuida, de otros tantos derechos. El fichero SINIVIH sólo seguirá vigente siempre y cuando se subsane.

SI APOSTAMOS POR LA SOCIEDAD DE LA INFORMACIÓN, HEMOS DE RESPETAR LA DIGINIDAD DE LA PERSONA