_ LA GARANTÍA DEL DERECHO CONSTITUCIONAL A LA PROTECCIÓN DE DATOS PERSONALES EN LOS ÓRGANOS JUDICIALES

_ CONSTITUTIONAL RIGHT GUARANTEE TO PERSONAL DATA PROTECTION WITHIN THE JUDICIAL SYSTEM

Artemi Rallo Lombarte
Director de la Agencia Española de Protección de Datos
Catedrático de Derecho Constitucional. Universitat Jaume I de Castellón

sumario//summary

resumen//abstract

La Administración de Justicia no es inmune a las garantías que reclama el derecho fundamental a la protección de datos de carácter personal, por más que los principios y facultades individuales derivados de ese derecho puedan plantear dificultades en cuanto a su verificación cuando se proyectan sobre la Administración de Justicia y, muy en particular, sobre el ejercicio de la función jurisdiccional. No en balde, puede producirse un conflicto entre el mencionado derecho y ese otro que atiende a la tutela judicial efectiva de los ciudadanos, cuando no con los principios que conforman el estatuto constitucional del Poder Judicial, lo que obliga a una singular ponderación de todos los elementos concurrentes que posibilite la vigencia equilibrada de ambos. A este propósito, conviene tener presente que la protección de datos es un derecho de libertad que protege de las potenciales agresiones a la dignidad y a la libertad de la persona ocasionadas por un uso ilegítimo del tratamiento mecanizado de los datos. Lo cual atribuye al ciudadano un poder de disposición y de control de los datos personales que le habilita para decidir cuáles de esos datos pueden proporcionarse a un tercero, sea el Estado o un particular, o cuáles puede recabar ese tercero; como también le faculta para conocer quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Justice Administration is not immune to the guarantees demanded by the Basic Right to personal details protection even whenever the different principles and faculties derived from this right could cause some difficulties regarding their verification when they are projected over the Justice Administration, and specially, over the exercise of the jurisdictional function. No wonder it may arise a conflict between the aforementioned right and the one stating the due process of law or with those principles which conform the Judiciary constitutional statute, what forces to the adjustment of all the elements involved so as to make the validity of both rights possible.

In this purpose, we should bear in mind that data protection is that kind of liberty right that protects people against any potential aggression to individual dignity and freedom caused by an illegitimate use of the mechanized data processing, what confers on the citizen the power to control and dispose of personal details and which enables him to decide which of those details can be given to third parties such as the State or any other particular or which details can be collected by third parties; as well as who gives those third parties the authority to known who possesses those personal details and the reason why they require them, giving the citizens the possibility to side against their possession or use.

Palabras Clave:
- Protección de datos personales en la Administración de Justicia.
- Los datos personales en los procesos civiles y penales.
- Consentimiento del interesado en la obtención de pruebas
- Datos personales y principio de proporcionalidad.

Key Words:
- Data protection in Justice Administration.
- Personal details in civil and criminal trials.
- The interested parties' consent in proof obtaining.
- Personal details and the principle of proportionality.

1 ■ INTRODUCCIÓN: EL MARCO CONSTITUCIONAL Y LEGAL

La vigencia efectiva del derecho fundamental a la protección de datos de carácter personal alcanza de forma inexorable al Poder Judicial tanto en su vertiente jurisdiccional como en la no jurisdiccional. La Administración de Justicia no constituye, en modo alguno, un espacio jurídicamente inmune a las garantías inherentes a este derecho fundamental consagrado, inclusive, en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea donde se indica que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan, así como el derecho a acceder a los datos recogidos que la conciernan y a su rectificación".

Ahora bien, a nadie escapa que los principios y derechos que derivan del derecho fundamental a la protección de datos de carácter personal pueden plantear singulares dificultades de verificación cunado se proyectan sobre la Administración de Justicia y, muy en particular, cuando se proyectan sobre el ejercicio de la función jurisdiccional. El conflicto entre dos derechos fundamentales (protección de datos y tutela judicial efectiva) y los principios que conforman el estatuto constitucional del Poder Judicial obligan a una singular ponderación de los mismos que posibilite, salvo que resulte inevitable la preferencia de uno sobre otro, la vigencia equilibrada de ambos.

La **Constitución Española** consagra la "dignidad humana como fundamento del orden político y de la paz social" (art. 10 CE) y en ésta se entronca un derecho fundamental a la protección de datos de alcance personalísimo. Su artículo 18.4 CE indica que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus

derechos". Sobre esta singular garantía va a residenciarse el nuevo derecho fundamental a la protección de datos reconocido por el Tribunal Constitucional en su Sentencia 292/2000. El Tribunal estableció que este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquélla que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

Esas singularidades respecto a su objeto radican en el hecho de que su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino, también, a lo que en ocasiones este Tribunal ha definido en términos más amplios como los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre).

La protección de datos es, por tanto, un 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 los datos, lo que la Constitución llama "informática". Hablamos, a decir de la sentencia, de "un poder de disposición y de control de los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" (FJ 7 STC 292/2000).

Al tiempo, la Constitución Española proclama la vigencia de un Estado Social y Democrático de Derecho (art. 1.1 CE) sustentado, a modo de columna vertebral, sobre el reconocimiento y vigencia del derecho fundamental a la tutela judicial efectiva contenido en su artículo 24: "todos tienen derecho a un proceso público sin dilaciones indebidas y con todas las garantías, así como a utilizar los medios de prueba pertinentes para su defensa".

El Título VI de la Constitución, dedicado al Poder Judicial, detalla los principios y reglas constitucionales que informan el estatuto y actuación de jueces y tribunales que debe garantizar la tutela efectiva de los derechos y legítimos intereses de los ciudadanos. De entre ellos, conviene resaltar, a nuestros efectos, los siguientes:

- Independencia judicial: el artículo 117.1 CE establece que la justicia emana del pueblo y se administra en nombre del Rey por Jueces y Magistrados integrantes del poder judicial e independientes.

- Exclusividad judicial: en el artículo 117.3 CE se nos dice que compete juzgar y hacer ejecutar lo juzgado exclusivamente a Juzgados y Tribunales determinados por las Leyes, según las normas de competencia y procedimiento que las mismas establezcan.

- Principio de colaboración: "es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto". (art. 118 CE).

- Publicidad de las actuaciones judiciales: "El procedimiento será predominantemente oral, sobre todo en materia criminal" (art. 120.1 CE).

- Oralidad del proceso: "las actuaciones judiciales

serán públicas pero con las excepciones que prevean las leyes de procedimiento".(art. 120.2 CE).

- Publicidad de las sentencias: "Las sentencias serán siempre motivadas y se pronunciarán en audiencia pública" (art. 120.3 CE).

Por su parte, la **Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial** desarrolla las anteriores previsiones constitucionales en los siguientes términos:

- "Los juzgados y tribunales protegerán los derechos e intereses legítimos, tanto individuales como colectivos, sin que en ningún caso pueda producirse indefensión" (art. 7).

- "En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales" (art. 11).

- "Las actuaciones judiciales serán públicas, con las excepciones que prevean las Leyes de procedimiento. Excepcionalmente, por razones de orden público y de protección de los derechos y libertades, los jueces y tribunales, mediante resolución motivada, podrán limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones". (art. 232).

- La LOPJ limita a los juzgados en el ejercicio de su actividad por los dictados de la legislación de protección de datos y los principios derivados de ésta: "Los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establece la legislación de protección de datos y demás leyes que resulten de aplicación … Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley … Reglamentariamente se determinarán por el Consejo General del Poder Judicial los requisitos y demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos judiciales de forma que se asegure el cumplimiento de las garantías y derechos establecidos …" (art. 230) en la legislación de protección de datos.

Una más detallada y exhaustiva reproducción merecen, sin embargo, las referencias de la **Ley Orgánica 15/1999 de Protección de Datos** (LOPD) que afectan, de forma directa o indirecta, al Poder Judicial:

- En primer lugar, resulta clamorosamente elocuente el reducido elenco de ámbitos excluidos de la vigencia de la LOPD (ficheros con materias clasificadas o de investigación del terrorismo y de formas graves de delincuencia organizada) o sometidos a sus disposiciones específicas y supletoriamente a la LOPD (Registros Civil y Central de Penados y Rebeldes) que evidencia la plena expansión de su vigencia a la Administración de Justicia: Así, en la ley se expresa que "el régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas. c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos" (art. 2.2). Lo anterior nos permite comprobar que el Poder Judicial y los ficheros relativos a éste no están exentos de la regulación de la legislación de protección de datos.

- En segundo lugar, en lo relativo a la comunicación de los datos, éstos sólo podrán ser comunicados a un tercero para el cumplimiento de fines directa-

mente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado; consentimiento previo que se excusa cuando la cesión esté autorizada en una ley o la comunicación tenga por destinatarios, por ejemplo, al Ministerio Fiscal o a jueces o tribunales. "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud 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" (art. 11. 1 y 2).

- En tercer lugar, indica el artículo 7.5 que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras: "Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras" (art. 7.5).

- En cuarto lugar, quedan sometidos a la LOPD los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal; la recogida y tratamiento de dichos datos sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales: "1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas estén limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento" (art. 22).

- En quinto y último lugar, debemos referirnos a los artículos 13 a 16, que albergan los derechos de acceso, oposición, rectificación y cancelación, que se ven matizados a su vez en los artículos 23 y 24, y que enlazan directamente con las previsiones contenidas en el Reglamento 1/2005 de Aspectos Accesorios de las Actuaciones Judiciales, cuyos artículos 2 y 4 prevén los modos de acceso a los libros, archivos y registros judiciales que no tengan carácter reservado.

La relación normativa anterior se limita a apuntar, con trazo grueso, los anclajes legales básicos de la problemática que nos ocupa pero no agota, sin duda, las numerosas referencias legales que merecerían ser traídas a colación para abundar en la exégesis. Ahora bien, algunas otras remisiones permiten dar a entender el alcance concreto de la voluntad de conciliar la garantía de ambos derechos fundamentales. Así, nos encontramos con legislación específica, sectorial o general, que introduce singularidades en la actuación judicial que afecta la protección de datos de carácter personal:

a) Ley Orgánica 10/2007 reguladora de la Base de Datos Policial sobre Identificadores obtenidos a partir del ADN, cuyos preceptos encuentran su justificación en las peculiaridades de la base de datos que regula. Según esta ley, los datos identificativos obtenidos en el contexto de una investigación criminal a partir del ADN sólo podrán ser utilizados por las unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado y por las Autoridades judiciales en la investigación de determinados delitos.

b) La Ley 25/2007 de Conservación de Datos Relativos a las Comunicaciones Electrónicas contiene también unas normas generales básicas sobre la cesión de datos a la policía judicial; advirtiendo que sólo podrán ser cedidos para los fines determinados en la misma y siempre mediando una previa autorización judicial.

c) Adicionalmente, en ocasiones, las legislaciones de carácter específico determinan los parámetros de desenvolvimiento de la actividad jurisdiccional, como ocurre, por ejemplo, con la legislación de carácter sanitario: Ley 41/2002 de Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica.

2 ■ LA PROTECCIÓN DE DATOS EN LA ACTIVIDAD NO JURISDICCIONAL DE LA ADMINISTRACIÓN DE JUSTICIA

La Agencia Española de Protección de Datos ha tenido oportunidad de actuar como garante de la adecuación de las actuaciones del Poder Judicial susceptibles de contravención de la normativa de protección de datos; extendiéndose su acción a materias no jurisdiccionales como son la creación e inscripción de ficheros, su seguridad o la publicidad de las sentencias o resoluciones judiciales.

A) Caso "Control y registro de accesos a la Audiencia Nacional y al Tribunal Supremo". Resolución de la AEPD nº 00193/2007

La actuación de la Agencia fue consecuencia de una denuncia presentada en mayo de 2004 por un abogado que puso en conocimiento de ésta que, al intentar entrar en el Tribunal Supremo para un asunto profesional, los miembros de un servicio de seguridad privado le habían exigido su DNI, además de pedirle una explicación de qué iba a hacer en el Tribunal con determinación de la persona a la que iba a visitar, y la realización de una fotografía, datos que quedaron almacenados en un ordenador.

A la Agencia le correspondía en este caso determinar en primer lugar a cuál de las dos entidades le correspondía la responsabilidad de las antedichas infracciones, ya que el deber de información corresponde al responsable del fichero o tratamiento.

Identificando al Ministerio de Justicia como la entidad que había decidido sobre la creación, la finalidad y el uso (al haber sido el Ministerio el que había fijado las condiciones para el acceso al edificio del Tribunal Supremo y la Audiencia Nacional en los contratos suscritos con las empresas seguridad) quedó acreditada la comisión de sendas infracciones, tipificadas

como leve (5.1) y grave (20.1) en los artículos 44.2.d) y 44.3.1 LOPD.

B) Caso "Documentación judicial en contenedores de basura del Tribunal Superior de Justicia del País Vasco". Resolución de la AEPD nº 00283/2004

El artículo 9 LOPD establece el principio de "seguridad de los datos" imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, y añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el acceso no autorizado. Sin embargo, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Es, en consecuencia, una obligación de resultado que se le impone al órgano responsable del fichero o, en su caso, al encargado del tratamiento.

Tras una información aparecida en la prensa, la AEPD procedió a la investigación de lo acontecido en el TSJPV, en cuyos contenedores de basura habían aparecido sin destruir, cientos de documentos judiciales. Tras la personación de los inspectores en sus dependencias, se acordó iniciar procedimiento de infracción al Departamento de Justicia, Empleo y Seguridad Social del Gobierno Vasco (ya que ése era el organismo responsable de la recogida de las bolsas de plástico que contenían el papel desechado) por la presunta infracción del artículo 9 LOPD, tipificada como muy grave en el artículo 44.3h) de la misma. Sin embargo, la indefinición de las responsabilidades comportó la imposibilidad de imputación de sanción alguna.

C) Caso "Documentación judicial del Juzgado de Algeciras en la vía pública". Resolución de la AEPD nº 00306/2008

En la vía pública de Algeciras fue hallada documentación con datos personales pertenecientes a un juzgado de dicha ciudad. El juzgado alegó que se trataba de un error involuntario por parte del servicio de limpieza del Juzgado que había trasladado una caja que contenía diversa documentación, depositándola después junto a un contenedor de basuras. El Consejo General del Poder Judicial aparecía como el "responsable de los ficheros", mientras que el órgano judicial oficiaba como "responsable del tratamiento". La investigación llevada a cabo por la AEPD determinó que la cesión de datos a terceros que se produjo (pues la documentación fue hallada por un medio de comunicación) se debió a la falta de implementación de "medidas de seguridad" por el "responsable del tratamiento", es decir, del Juzgado, que no había obrado con la diligencia suficiente para evitar que una actuación del servicio de limpieza pudiese provocar ese resultado.

D) Caso "Documentación de la Junta Electoral de Zona de Puertollano en la basura". Resolución de la AEPD nº 00074/2008

Como en los casos precedentes, en esta ocasión fue hallada en la basura una abundante cantidad de documentos relativos a las elecciones de los años 2003,2004 y 2005 conteniendo, entre otros datos personales, nombres, direcciones, DNIs, afiliaciones políticas e incluso informes médicos de los componentes de las mesas electorales. Correspondiendo la custodia de los documentos al Secretario de la Junta, se incoó un procedimiento de declaración de infracción de Administraciones Públicas que acabó en una declaración de infracción del artículo 9 LOPD, requiriéndose a la Junta para que adoptase las necesarias medidas de orden interno[1].

E) Caso "Entrega a portero de finca de una citación judicial sobre proceso de divorcio". Resolución de la AEPD nº 00068/2007

Los responsables de los ficheros están sujetos al deber de secreto profesional que, recogido en el

[1] En la actualidad, la AEPD mantiene abierta una investigación a varios juzgados de Madrid, Barcelona, Sevilla, Valencia y A Coruña con motivo de la localización por parte de un equipo de reporteros de "Informativos Telecinco" de documentación judicial en las basuras de las inmediaciones de éstos.

artículo 10 LOPD, se hace extensivo a todos aquéllos que intervengan en cualquier fase del tratamiento de los datos de carácter personal, comportando su obligación de no revelar ni dar a conocer su contenido. Este deber implica que los datos no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados, pues en eso consiste, precisamente, el secreto.

En este caso, el agente de notificaciones judiciales, perteneciente al servicio común de notificaciones del partido judicial, entregó al portero de la finca en la que vivía la reclamante una cédula de citación judicial, en un escrito sin sobre (siendo el objeto de la misma la ratificación de una petición de divorcio y conteniendo también el convenio regulador, la demanda de divorcio, la partida de nacimiento del marido y la de su hijo menor). Quedaba acreditado, en consecuencia, que el juzgado, a través de este agente, había vulnerado el deber de secreto que le incumbía como responsable en virtud del artículo 10, infracción tipificada como "grave" en el artículo 44.3g) de la LOPD.

F) Casos sobre "publicidad y acceso a datos personales contenidos en Sentencias o Resoluciones judiciales"

Como se ha destacado en la STC 68/2005, de 31 de marzo, «quien participa por decisión propia en un procedimiento público no puede invocar su derecho fundamental a la intimidad personal ni la garantía frente al uso de la informática (artículo 18.1 y 4 CE) por el mero hecho de que los actos del procedimiento en los que deba figurar su nombre sean, por mandato de la Constitución o con apoyo en ella, objeto de publicación oficial o de la publicidad y accesibilidad que la trascendencia del propio procedimiento en cada caso demande; ello sin perjuicio, claro es, de que el contenido mismo de tales actos incorpore, eventualmente, datos que puedan considerarse inherentes a la intimidad del sujeto, supuesto en el cual sí operan, en plenitud, aquellas garantías constitucionales».

A la hora de hablar de la publicidad de las sentencias, conviene empezar averiguando, en una primera aproximación, la respuesta a la siguiente cuestión: ¿están las sentencias sometidas a una regla general de publicidad que ampare el acceso a las mismas de cualquier ciudadano a través de cualesquiera medios? Para dar respuesta a esta pregunta debe afirmarse, en primer lugar, que las sentencias judiciales gozan del efecto de publicidad procesal general en los términos reconocidos en la LOPJ, pero ello no quiere decir que sean "*fuentes accesibles al público* " en el sentido reconocido por la LOPD pues las sentencias judiciales no se encuentran entre las fuentes accesibles al público que taxativamente enumera el artículo 3 j) LOPD.

El tratamiento de datos de carácter personal que figuran en sentencias judiciales por persona o entidad distinta a los interesados necesita para su tratamiento el consentimiento previo de los mismos, no pudiendo considerarse fuente de acceso público general. Así las cosas, siempre que una ley no disponga lo contrario, los interesados podrán oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

Es en este contexto en el que hay que situar la STC de 18 de Septiembre de 2006, que recoge la doctrina esencial sobre el concepto de "interesado": "el interés legítimo que es exigible en el caso, sólo puede reconocerse en quien, persona física o jurídica, manifiesta y acredita, al menos "prima facie", ante el órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso –y, por ende, de la sentencia que lo finalizó en la instancia–, bien con alguno de los actos procesales a través de los que aquel se ha desarrollado y que están documentados en autos". Esta conexión está sujeta a dos condicionamientos: 1) que no afectara a derechos fundamentales de las partes procesales o de quienes de algún modo hubieran intervenido en el proceso, para salvaguardar esencialmente el derecho a la privacidad e intimidad personal y familiar, el honor y el derecho a la propia imagen que eventualmente pudiera afectar a aquellas personas; 2) que, si la información es utilizada, como actividad mediadora, para satisfacer derechos o intereses de terceras personas y, en

consecuencia, adquiere un aspecto de globalidad o generalidad por relación no a un concreto proceso, tal interés se mantenga en el propio ámbito del ordenamiento jurídico y de sus aplicadores, con carácter generalizado, pues otra cosa sería tanto como hacer partícipe o colaborador al órgano judicial en tareas o actividades que, por muy lícitas que sean, extravasan su función jurisdiccional.

A este respecto, debe traerse a colación la STS de 3 de marzo de 1.995, en la que se confirmaban dos acuerdos de la Salas de Gobierno de los Tribunales Superiores de Justicia de Castilla y León (de 7 de noviembre de 1990) y de Canarias (de 21 de diciembre de 1990), por los que se impedía el acceso al texto de las sentencias en la forma en que había sido pretendido por una determinada sociedad mercantil, que solicitaba la toma de datos del texto de de las sentencias recaídas en procesos civiles de diversa naturaleza para la inclusión en su base de datos y su posterior facilitación a sus clientes, tratándose éstos principalmente bancos y empresas.. En esta sentencia, el Tribunal Supremo determinó que, del examen de la LOPJ y las leyes procesales, se desprende que el derecho y correlativo deber de conocimiento y acceso al texto de las resoluciones judiciales se gradúa en función de tres diversos ámbitos o esferas de afectación, regida cada una por diversos criterios: a) Máxima amplitud o de afectación generalizada; que comprende al público o los ciudadanos en general y que entronca con el principio de publicidad constitucionalizado, en el articulo 120.1. b) Una esfera, en el extremo opuesto, de máxima restricción del ámbito de conocimiento de las decisiones judiciales; donde se hallan los actos de notificación y comunicación dirigidos sólo a quienes revisten la condición de parte procesal en virtud de las leyes de procedimiento. c) Y, en una posición intermedia, las actuaciones procesales ya finalizadas, incluidas las sentencias, integradas en libros, archivos o registros judiciales, y respecto a las cuales, de una parte, el articulo 235 LOPJ determina que "los interesados tendrán acceso a los libros, archivos y registros judiciales que no tengan carácter reservado, mediante las formas de exhibición, testimonio o certificación que establezca la Ley" y señalando el art. 266.1, con relación a las sentencias, que "las sentencias, una vez extendidas y firmadas por el Juez o por todos los Magistrados que las hubieran dictado, serán depositadas en la Secretaría del Juzgado o Tribunal y se permitirá a cualquier interesado el acceso al texto de las mismas". Esta doctrina se vería además reiterada por la STS Sala 3ª, Sección 7ª, de 6 de abril de 2.001.

A mayor abundamiento, la posibilidad de excepcionar la publicidad de la integridad de una resolución judicial ha sido recientemente incorporada por la reforma operada en el artículo 266.1 LOPJ por la Ley Orgánica 19/2003, de 23 de diciembre, que ha añadido en dicho precepto un párrafo segundo en el que se establece: «el acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes". En el mismo sentido se expresa el artículo 3 del Reglamento 1/2005 de Aspectos Accesorios de las Actuaciones Judiciales al decir que se podrá restringir el acceso al texto de las sentencias o a determinados extremos de las mismas, cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas dignos de especial tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, y, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes.

Merecen traerse a colación en este punto diferentes casos conocidos por la AEPD de singular interés.

1º) "Aranzadi-Westlaw sobre anonimización de sentencias". Resolución de la AEPD nº 00486/2004.

En este procedimiento se sustanciaba la queja de una ciudadana que informaba, en relación con una sentencia de la Audiencia Provincial de Las Palmas,

que había sido publicada en Internet por la Editorial Aranzadi a través de la página www.westlaw.es, mostrándose de manera íntegra el nombre y dos apellidos de la afectada. Estas sentencias, según la editorial, eran proporcionadas por el CENDOJ, centro que lleva a cabo la recopilación y difusión de la Jurisprudencia del Tribunal Supremo, de las Sentencias de los Tribunales Superiores de Justicia y de las Audiencias Provinciales. La representación de Aranzadi argumentaba que en este caso el error procedía del órgano administrativo pero el CENDOJ alegó que en el contrato celebrado con Aranzadi, ésta se había comprometido a proceder a la anonimización de los datos de las sentencias. La Agencia Española de Protección de Datos estimó en este caso una infracción del artículo 6 LOPD al no contar con el consentimiento de la afectada para el tratamiento de sus datos (en este caso, mediante la publicación en Internet a través del servicio "Westlaw") calificado como "grave" y condenando a una multa a dicha editorial.

2º) Ficheros de Violencia de Género promovidos por Castilla-La Mancha, Barakaldo y Plasencia. Resolución de la AEPD de archivo de actuaciones nº 00310/2002 e Informe de 26 de marzo de 2008.

La publicidad de las sentencias plantea una problemática particular, especialmente, cuando pretende articularse a modo de fichero automatizado como pudo comprobarse al promover la Comunidad de Castilla-La Mancha en mayo de 2002 la creación de un fichero con las sentencias y datos personales de las personas condenadas por maltrato. Este anuncio provocó la actuación de la AEPD. que decidió en agosto archivar las actuaciones (E/00310/2002) ya que la publicación de dichas sentencias se realizaba en soporte físico no susceptible de tratamiento automatizado posterior ni estructurado de una forma que permitiese acceder al contenido del mismo tanto mediante técnicas automatizadas como manuales, por lo que los hechos investigados quedaban al margen del ámbito de aplicación de la LOPD.

Con el precedente de Castilla-La Mancha, los Ayuntamientos de Baracaldo, en noviembre de 2007, y Plasencia, en marzo de 2008, anunciaron su intención de publicar en las páginas Web de sus respectivos Ayuntamientos las sentencias con datos personales relativas a condenas por violencia de género. Ello motivó la emisión de un informe de la Agencia, de fecha 26 de marzo de 2008, en el que se recordó que, sobre los datos relacionados con la comisión de infracciones penales y administrativas (como sucedía en el supuesto objeto de análisis de aquellos hechos), el artículo 7.5 LOPD establece que sólo pueden ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras. El informe destacó que el artículo 32 de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género establece que los poderes públicos pueden elaborar planes de colaboración que garanticen la ordenación de sus actuaciones en la prevención, asistencia y persecución de los actos de violencia de género, que deberán implicar a las administraciones sanitarias, la Administración de Justicia, las Fuerzas y Cuerpos de Seguridad y los servicios sociales y organismos de igualdad. A tal efecto, la Agencia había informado favorablemente la Orden INT/1911/2007, de 26 de junio, por la que se creaba el fichero de datos de carácter personal «Violencia doméstica y de género», en el Ministerio del Interior. Sin embargo, los datos del fichero que se pretendía crear sólo podían ser objeto de acceso por una serie de autoridades e instituciones entre las que no se encontraban los ayuntamientos, de modo que el tratamiento de los datos de carácter personal a los que se refería la consulta únicamente podía producirse si una norma con rango suficiente otorgase dichas competencias a la Corporación consultante, algo que no hacía la Ley Orgánica 1/2004.

Resulta claro que existe una finalidad social basada en la demanda de seguridad que legitima la creación de registros de datos relativos a personas investigadas, procesadas o condenadas por delitos

singularmente repugnantes como son los relacionados con agresiones sexuales o violencia de género, para el acceso de las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio fiscal y Jueces y Magistrados en el ejercicio de sus respectivas competencias. Un acceso más amplio a otros sujetos podría verse igualmente habilitado por el legislador aunque resultaría inexcusable limitarlo conforme lo requieran los principios de calidad, finalidad y proporcionalidad en los términos exigidos por la LOPD.

3 ■ PROTECCIÓN DE DATOS Y FUNCIÓN JURISDICCIONAL

3.1. LOS PRINCIPIOS DE PROTECCIÓN DE DATOS EN EL PROCESO JUDICIAL

3.1.1. EL DEBER DE INFORMACIÓN A LOS CIUDADANOS SOBRE LA OBTENCIÓN Y TRATAMIENTO DE SUS DATOS PERSONALES

El derecho a consentir el conocimiento y tratamiento de los datos personales requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo. La información constituye el fundamento ontológico para que los afectados puedan ejercitar los derechos de acceso, rectificación, cancelación y oposición. Por eso, uno de los primeros principios de protección de datos que ha de tener en cuenta en es el que determina que los ciudadanos hayan de ser informados del tratamiento que se haga de sus datos. Hay que decir, no obstante, que el artículo 24.1 de la LOPD contiene dos reservas al deber de información al decir que "lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas".

Especial importancia tiene en este punto el tratamiento por abogados y procuradores de los datos de las partes en un proceso, cuestión sobre la que la AEPD se ha pronunciado en el informe 2000-0000 donde se esbozan las imbricaciones de esta materia con el derecho de defensa.

Según se expuso en Informe 2000-0000 de la AEPD sobre tratamiento por abogados y procuradores de los datos de las partes en un proceso, en lo referente a los datos de los clientes, éste podrá efectuarse sin consentimiento del afectado, a tenor de lo establecido en el artículo 6.2 de la Ley Orgánica 15/1999, que excluye del consentimiento los supuestos en que los datos "se refieran a las partes de un contrato o precontrato de una relación negocial (…)". La duda se plantea en el supuesto de que los datos se refieran a los oponentes de los clientes del abogado o procurador, con quienes también se encuentra legitimado a comunicarse, dado que en ese caso el tratamiento resulta absolutamente imprescindible para la asistencia letrada al cliente (tal y como señala el artículo 24 de la Constitución española).. El legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida. A decir de este informe, "la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de

"los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva" (artículo 24 CE) y "coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho". Sigue diciendo este informe que, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes, por lo que existirá, desde el punto de vista de la Agencia, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.

3.1.2. EL PRINCIPIO DE COLABORACIÓN CON LA ADMINISTRACIÓN DE JUSTICIA. LA OBTENCIÓN DE DATOS PERSONALES EN EL MARCO DEL PROCESO CIVIL Y/O PENAL: CASO "PROMUSICAE Y TELEFÓNICA"

La Sociedad de Productos de Música de España (Promusicae) acudió al juez con las IPs de algunos usuarios que habían descargado películas y música desde sus ordenadores pidiéndole que instase a Telefónica a identificarles. El juez procedió a solicitar esos datos a Telefónica pero la compañía se opuso alegando que la legislación española lo impedía al ser datos que, según la ley, sólo deben ser desvelados si son requeridos por un juez en el marco de una investigación criminal o por un asunto que afecte a la seguridad nacional.

El fundamento legal de la posición de Telefónica residía en el artículo 12 de la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que prescribe: "los operadores de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo". Esta ley indica, también, que los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la ley y deberán adoptar las medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado de los mismos. En particular, el apartado tercero del artículo 12 LSSI establece: "los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los jueces o tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales".

Telefónica apreció que, en virtud de este artículo, la comunicación de los datos no podía tener lugar en el marco de un procedimiento civil o de las medidas preparatorias de un procedimiento civil, como era el caso. Por su parte, Promusicae alegaba que el mencionado artículo de la LSSI debía interpretarse conforme a las Directivas 2001/28, 2004/48 y 2000/31 que, a su entender, no permiten a los Estados miembros restringir únicamente a los fines a los que se refiere el tenor de esta ley el deber de comunicar los datos de que se trata.

Posteriormente, el juez de los mercantil planteó al Tribunal de Justicia de la Unión Europea una cuestión prejudicial sobre la existencia de Directiva europea que obligase, aun tratándose de un pleito civil, a iden-

tificar a quienes descargan archivos en Internet. Con anterioridad al pronunciamiento del Alto Tribunal se evacuó un informe de conclusiones elaborado por Juliane Kokot, Abogada General del Tribunal, en el que se señalaba que la normativa europea permite que los Estados miembros excluyan la comunicación de datos personales de tráfico para la persecución por la vía civil de infracciones de los derechos de autor. Promusicae alegaba que, en efecto, cabía exigir judicialmente a una operadora la identificación de usuarios de la Red aun tratándose de un asunto civil, ya que el artículo 6.6 de la Directiva 2002/58 permite pedir este tipo de datos si ello ayuda a resolver litigios.

Finalmente, el Tribunal de Luxemburgo, en su Sentencia TJCE 2008/11 de 29 de enero de 2008, consideró que, en efecto, los Estados miembros no estaban obligados a imponer el deber de comunicar datos personales con objeto de garantizar los derechos de autor en el marco de un procedimiento civil, sin que ello impida que los Estados miembros deban basarse, a la hora de adaptar las directivas de referencia, en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario.

3.1.3. EL CONSENTIMIENTO DEL INTERESADO EN LA OBTENCIÓN DE PRUEBA

Uno de los pilares básicos de la normativa de protección de datos es el principio del consentimiento o autodeterminación informativa. Este consentimiento cederá en determinadas circunstancias expuestas en el artículo 6.2 LOPD, y actuará con especial vigor en el supuesto de las cesiones de datos cuando se trata del ámbito jurisdiccional. La Agencia ha tenido oportunidad de dictaminar su criterio a la luz de una cuantiosa relación de casos[2], en los que ha entrado en conflicto el principio de consentimiento con **el derecho procesal de defensa:**

A) Caso "Despido por uso indebido de tarjetas en autopista". Procedimiento Sancionador de la AEPD 00038/2003

La parte actora, acusada de apropiación de fondos, consideraba que la base de las imputaciones para el despido del que había sido objeto era un informe de un área de la empresa que aportó a juicio documentación sobre él (datos de utilización de tarjetas en peajes de autopista), obtenida sin su consentimiento y contraviniendo por tanto el artículo 6 LOPD. La Agencia consideró, sin embargo, que existía una vinculación laboral entre el denunciante y la empresa de la que derivaron las actuaciones judiciales que originaron el tratamiento de datos, por lo que resultaba plenamente aplicable la excepción del artículo 6.2 LOPD. La Agencia acordó el archivo de actuaciones al considerar que la cesión o comunicación al juzgado se enmarcaba además plenamente en las excepciones al consentimiento en la cesión que contiene el artículo 11.2.LOPD, ya que, como ha quedado dicho, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos supondría dejar a su disposición el almacenamiento de la información necesaria para que el denunciante pudiese ejercer en plenitud su derecho a la tutela judicial efectiva.

B) Caso "Datos de un tercero en cuenta bancaria compartida". Procedimiento Sancionador de la AEPD 00126/2007

Un juzgado de Vigo solicitó a una entidad bancaria, en el marco de un procedimiento de liquidación de sociedad de gananciales, información sobre las cuentas de las que los cónyuges fuesen titulares; siendo remitida por la entidad bancaria documentación que incluía información de una cuenta en la que figuraba, junto al ex-marido, como titular, una

2 El criterio de la AEPD en materia de consentimiento ha sido recientemente confirmado por las sentencias de la sala de lo Contencioso-Administrativo de la Audiencia Nacional de 12, 20 y 27 de febrero de 2008.

tercera persona –información que según los denunciantes no era de interés para el juzgado–. Denunciaban, por tanto, un trato inconsentido de los datos de la misma. La entidad bancaria alegó haberse ceñido al escrito del juzgado, ya que la solicitud iba referida a todo tipo de cuentas en las que figurase alguno de los miembros de la sociedad conyugal como titulares. La AEPD estimó que la actuación del juzgado se incardinaba dentro de las capacidades que la ley le reconoce a dicho órgano jurisdiccional en el marco de la Ley de Enjuiciamiento Civil, como concreción del derecho a la tutela judicial efectiva y, por ello, se procedió al archivo de actuaciones.

C) Caso "Aportación de historia clínica". Procedimiento Sancionador de la AEPD nº 00796/2006

Una entidad aportó, sin autorización de la denunciante, el historial clínico de ésta en el ejercicio de su derecho de defensa ya que en la demanda contra ésta se cuestionaba el seguimiento de la evolución y el tratamiento recibido por la denunciante en el instituto médico dependiente de esta entidad por lo que la presentación del historial clínico para su defensa era tan necesario como insustituible, Así lo entendió el juzgado admitiéndolo como prueba en el proceso. De igual modo, se estimó que la falta de comunicación de los datos a la contraparte podía implicar una merma en la posibilidad de aportación por el interesado de los medios de prueba pertinentes para su defensa, procediéndose al archivo de las actuaciones.

D) Casos de "Obtención de datos personales por la policía judicial sin previo mandamiento judicial o requerimiento del Ministerio Fiscal"

Plantean un problema singular en materia de consentimiento las solicitudes de datos que la policía judicial realiza sin mandamiento judicial o requerimiento previo del Ministerio Fiscal. El supuesto dio lugar a una petición de Informe solicitada a la AEPD por diversas empresas en 1999 al haber sido requeridas para la facilitación de datos a la policía, por propia iniciativa o a instancia de su superior jerárquico.

La Agencia, en Informe de 14 de julio de 2005, había ya precisado la distinción entre las actuaciones de la Policía Judicial llevadas a cabo en cumplimiento de un mandato judicial o de un requerimiento efectuado por el Ministerio Fiscal de aquéllas otras que se llevan a cabo por propia iniciativa o a instancia de superior jerárquico. Respecto de las primeras, adujo el informe que resulta aplicable el artículo 11.2 d), no requiriéndose el consentimiento del interesado por cuanto los efectivos de la policía obran aquí como meros transmisores de la solicitud efectuada por el Ministerio Fiscal o el órgano jurisdiccional. El problema se planteaba en relación con aquellos supuestos en que la policía requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, al no existir en este caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión. En este caso, estábamos ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identificaban con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado. Dicho Informe añadió que resultaba aplicable lo dispuesto en el artículo 22.2 de la LOPD, según el cual "la recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad". Este artículo habilita a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan una serie de condiciones, como que, en cumplimiento del artículo 22.4 de la LOPD, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento". También en este caso apreció la AEPD la

excepción al consentimiento del artículo 11.2d), por lo que dispuso que la cesión solicitada encontraba amparo legal.

3.1.4. LA CALIDAD DE LOS DATOS Y EL PRINCIPIO DE PROPORCIONALIDAD

La LOPD, en el artículo 4, afirma que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Esta exigencia ha de entender junto a la prohibición de la recogida de datos por medios fraudulentos, desleales o ilícitos, lo que en el ámbito del proceso puede cifrarse en la proscripción de la denominada "prueba ilícita", que en este contexto aparecería cuando los medios aportados al proceso se han obtenido mediante infracción de la legislación de protección de datos. Lo que la LOPD denomina "exceso de los datos" con respecto a la finalidad que ha justificado su tratamiento no es sino una reformulación del principio de proporcionalidad, que sigue siendo, empero, la forma bajo la que aparecen la mayor parte de las transgresiones a este pilar básico.

Si se examinan los límites que el juez encuentra en su actuación jurisdiccional, se constata que el principio de proporcionalidad adquiere especial relevancia por cuanto, como señalara la Sentencia del Tribunal Constitucional 186/2000, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales ha de cumplir los requisitos de idoneidad, necesidad, y equilibrio. Los siguientes casos ilustran los conflictos en que opera este principio:

A) Caso "Cuentas corrientes del BBVA". Resolución de la AEPD nº 00445/2002 y Sentencia de la AN de 3 de noviembre de 2004

En el año 2002, en el curso de una investigación policial, la policía solicitó al juzgado que pidiese la remisión de los movimientos bancarios del denunciante desde el 1 de enero de 2000 hasta 29 de marzo de ese mismo año. La entidad BBVA facilitó a la Policía Nacional, sin consentimiento del denunciante, datos sobre la existencia de movimientos en tres de sus cuentas para justificar la participación de éste en un presunto delito de apropiación indebida. En el supuesto examinado resultaba claro que el juzgado dictó ese auto para fechas concretas pero, a pesar de ello, la entidad no sólo remitió a la policía nacional informe relativo al movimiento de cuentas bancarias no incluidas en el citado auto, sino que lo hizo por un período más amplio que el requerido (desde el 7 de enero de 1999). Dicha información en exceso no estaba amparada por el 11.2.d) y, en consecuencia, el BBVA vulneró el artículo 10 LOPD. La AEPD sancionó al BBVA con multa por infracción del artículo 10 LOPD calificado como grave en el 44.3g) LOPD. La Sentencia posterior de la Audiencia Nacional señaló, también, que al hacer entrega de los datos a la Policía y no al Juzgado se vulneraba el artículo 10 al no haber sido acreditado el preceptivo consentimiento.

B) Caso "Volcado de información notarial". Resolución de la AEPD nº 00595/2008.

En el marco de la instrucción de un procedimiento penal, una oficina notarial fue objeto de un registro cuya pretensión era la de intervenir documentación sobre una investigación autorizada por auto del juez de instrucción en el que ordenaba "intervenir la documentación en la que hayan intervenido las personas físicas y jurídicas" que constaban en un anexo. Se procedió mediante un disco duro portátil a realizar un volcado general sin discriminar la información que se refería al objeto de la investigación, incluyéndose en dicho volcado datos sobre escrituras públicas, testamentos, etc, relativos a personas ajenas a la investigación en curso. Bajo la premisa brindada por el artículo 4 LOPD, según el cual los datos de carácter personal sólo se podrán recoger para su tratamiento y someterlos al mismo cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se han obtenido, la AEPD inició actuaciones contra la AEAT para dilucidar esa posible

extralimitación. Deduciendo que el hecho de que se produjera un volcado de toda la información no quería significar necesariamente que se produjera un tratamiento de datos excesivo y desproporcionado (al haber sido habilitado expresamente por el citado auto y dada la complejidad de una depuración apriorística de la documentación que resultase de interés en el marco de una investigación), la AEPD concluyó que la apreciación de una posible extralimitación en la función del auxilio judicial no correspondía a la AEPD sino al órgano jurisdiccional pertinente mediante el sistema previsto de recursos judiciales – lo que llevó al archivo de actuaciones–.

C) Caso "Historia clínica completa". Declaración de Infracción de Administración Pública nº 28/05

En el seno de un proceso de anulación del los pactos establecidos en el convenio regulador del divorcio, deseando el recurrente probar que los citados pactos se habían desarrollado en un contexto de intimidación por parte de su esposa, solicitó a través del juzgado una certificación de un hospital en la que quedase acreditado que ésta había sido ingresada en el mismo en unas determinadas fechas y, además, que informase, en caso afirmativo, del diagnóstico y tratamiento recibido por aquélla. Sin embargo, el hospital remitió al juzgado el historial clínico completo de esta ciudadana.

El hospital alegó que no se había extralimitado al atender el requerimiento cursado por el Juzgado de Primera Instancia porque la historia clínica remitida tenía por destinatario dicho órgano judicial, sometido al deber de secreto y que, asimismo, las partes del proceso judicial, que tenían acceso a la referida documentación, estaban también sometidas al deber de secreto. En el presente caso constaba que el hospital se había extralimitado en la información suministrada sobre los datos de salud requeridos por el Juzgado, careciendo, en consecuencia, de la habilitación legal que ampara dicha actuación, dado que no constaba el consentimiento de la denunciante para la revelación de sus datos de salud. Finalmente, la Agencia declaró la comisión de una infracción por el hospital del artículo 10 LOPD (que impone la obligación de guardar secreto) conducta tipificada como "muy grave" por esta ley.

D) Informe de la AEPD de 2 de abril de 2008 sobre el tratamiento de datos sobre interrupción voluntaria del embarazo en el marco de investigaciones judiciales

Como prueba el caso anterior, existen determinados datos cuyo tratamiento puede implicar consecuencias más graves para la esfera íntima de la persona, que exigirán extremar el cuidado para evitar la merma del derecho fundamental. Es el caso de los datos de salud, cuya regulación ilustra la modulación del acceso judicial a datos de naturaleza sensible. Los datos relacionados con la salud, específicamente, están sometidos por el legislador comunitario y español a un régimen de protección especial, por su condición de datos sensibles o especialmente protegidos. En virtud de lo anterior, el artículo 7.3 LOPD recuerda que "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados, y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente, estableciendo en particular en el artículo 11.2f) la licitud de la cesión de determinados datos relacionados con la salud si la misma es "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 autónoma".

Según ha tenido oportunidad de señalarse en el Informe de la AEPD de 2 de abril de 2008 relativo al tratamiento de datos sobre interrupción voluntaria del embarazo (casos en que las garantías deberán extremarse, habida cuenta de las consecuencias perjudiciales que el conocimiento de los datos por terceros puede revestir en la esfera privada de la paciente), es en el tratamiento del historial clínico del paciente en el que operan una serie de garantías que implican una limitación de los supuestos en que procederá el tratamiento y comunicación de estos datos. Según ha afirmado este informe, la cesión de los datos en estos casos se encontrará sujeto a lo dispuesto en 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 quedando en particular la cesión de los datos limitada a los supuestos contemplados en su artículo 16, en cuyo apartado 3 se dice: "El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso". Este apartado indica además que "se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso". Como ilustra este Informe, el acceso judicial no puede entenderse ilimitado y extenderse a datos no vinculados a la necesidad que lo motivó. Imperando una regla general de anonimato, aun cuando el acceso se realizase con fines judiciales, la identificación personal será posible, como excepción, sólo en los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales en el marco concreto del proceso correspondiente y limitado estrictamente a los fines específicos de cada caso.

3.2. LOS DERECHOS DE PROTECCIÓN DE DATOS: EL ACCESO Y CANCELACIÓN DE DATOS OBRANTES EN DOCUMENTACIÓN JUDICIAL

A) Sentencia del Tribunal Supremo, de 18 de septiembre de 2006, que fijó límites de acceso a la documentación judicial

En el supuesto que culminó con la Sentencia referida del Tribunal Supremo, el recurrente seguía un procedimiento de juicio verbal contra el demandado que se encontraba suspendido por problemas de citación de éste. El recurrente, habiendo tenido conocimiento de la posible existencia de otros procedimientos contra el mismo demandado ante los mismos juzgados – lo que podría facilitar la citación e incluso la adopción de medidas de aseguramiento–, solicitó que le fuesen comunicados los asuntos repartidos contra esa persona hasta esa fecha. El Alto Tribunal, tras recordar que los registros de los Juzgados no son fuentes accesibles al público en el sentido en que los define la LOPD en su artículo 3.j), añadió que, al estar los datos de carácter personal obrantes en los registros y archivos de los juzgados y tribunales protegidos frente a las pretensiones de acceso por terceros cuando no cuenten con el consentimiento del afectado o con autorización legal, y descansando el acceso a los libros, registros y archivos jurisdiccionales en la posesión de la condición de interesado de quien la pretende, resultaba evidente la posición de tercero del recurrente, por lo que resultaba improcedente la aplicación del artículo 11.2 LOPD al no estar la comunicación de datos solicitada por el recurrente autorizada y ser aplicables las normas de la Ley Orgánica del Poder Judicial. Además, el Tribunal estimó que se apreciaba, por un lado, falta notoria de finalidad al no tener relación con las dificultades de notificación la comunicación de todos los procesos seguidos contra esa persona y, por otro, ausencia de proporcionalidad –pudiendo haber limitado el recurrente su petición a los datos relativos al domicilio del demandado–.

B) Caso "Acceso a datos de libros-registro judiciales por el Colegio de Abogados de Madrid". Resolución de la AEPD nº 00069/1999

En dicho asunto quedó acreditado que el Servicio de Comprobación del Colegio de Abogados de Madrid había recabado datos que se introducían y almacenaban en un fichero con datos de carácter personal (nutrido con los contenidos en los libros-registro de los tribunales procedentes de procedimientos judiciales en los que han intervenido sus colegiados), que estaban siendo utilizados por el Colegio para reclamar cantidades económicas por intervención profesional La Agencia estimó que, habiéndose resi-

denciado reglamentariamente y en virtud de mandato legal en el Consejo General del Poder Judicial la competencia sobre la materia, atribuyéndose aquélla a la autoridad judicial y a sus órganos de gobierno, toda información requerida por tercero debía contar con el consentimiento del afectado o, en su caso, ser autorizada por el titular del órgano jurisdiccional, correspondiendo a éste velar por la defensa de los derechos reconocidos en el art. 18.4 de la Constitución En este caso, el acceso a ese fichero había sido autorizado por el Tribunal Supremo, Tribunal Superior de Justicia y Audiencia Provincial. Al corresponder la decisión sobre la licitud y alcance de los accesos autorizados a las autoridades judiciales citadas y a sus órganos de gobierno, se procedió al archivo de las actuaciones.

C) Caso "Cancelación de datos del Registro del Decanato de los Juzgados de Instrucción de Madrid". Resolución de la AEPD 00539/2004

En el presente caso se solicitó ante la Oficina de Atención al Ciudadano del Decanato de los Juzgados de Instrucción de Madrid la cancelación de datos personales contenidos en el registro de dicho Decanato. El Decanato respondió que el citado Registro constituía un fichero sobre datos relativos a la comisión de infracciones penales o administrativas, establecido de conformidad con lo establecido en el artículo 7.5 LOPD, que contaba con una regulación legal específica en materia de acceso, rectificación y cancelación. Esta regulación exceptúa la cancelación de los datos incluidos en dicho registro salvo que sea ordenada su supresión por decisión judicial o por los propios órganos gubernativos del Poder Judicial. Añadía también la Resolución de la AEPD que el artículo 80 del Reglamento 5/1995, de 7 de junio, de los Aspectos Accesorios de las Actuaciones Judiciales referido a los Registros y Procedimientos de Juzgados y Tribunales bajo el epígrafe "Del establecimiento y gestión de los ficheros automatizados bajo la responsabilidad de los órganos judiciales" disponía: "Los datos de carácter personal incorporados se conservarán en tanto su supresión no sea ordenada por decisión judicial o de los órganos de gobierno propios del Poder Judicial dictada en el ejercicio de sus competencias gubernativas"; prevención que fue reproducida a su vez por el Reglamento 1/2005 en su artículo 89. En consecuencia, se procedió a la desestimación de la reclamación planteada por cuanto la denegación de la cancelación de los datos del afectado por parte del Decanato de los Juzgados de Instrucción de Madrid estaba amparada legalmente ■

Artemi Rallo Lombarte