TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO JURISDICCIONAL

I. INTRODUCCIÓN:

La exigencia de una adecuada ponderación entre bienes jurídicos dignos de protección es un elemento inherente de la misma idea de impartición de la justicia, presente en el ejercicio de la labor jurisdiccional desde sus orígenes.

Uno de los campos más fértiles en los que esa ponderación se despliega en su plenitud es aquél en el que se dilucidan los límites entre lo público y lo privado.

La relación entre estas dos vertientes subyacentes al Estado Social y Democrático de Derecho dista de ser pacífica, como nos disponemos a comprobar, produciéndose un incontable número de casos en los que ambas se entreveran en una coexistencia no exenta de fricciones. Esto ocurre con especial intensidad en el ejercicio de la función jurisdiccional, por lo que, con el ánimo de evitar posibles desafueros, en el actual sistema se han articulado una serie de límites, entre los que destaca naturalmente el principio de legalidad, ya que las mismas fuentes de legitimación del poder judicial se identifican por completo con él y con el sistema de las garantías, es decir, con los vínculos dirigidos a reducir al máximo el arbitrio de los jueces para tutelar así los derechos de los ciudadanos.

II. MARCO NORMATIVO

A modo de establecer un criterio interpretativo de la normativa aplicable en materia de protección de datos y en especial en lo que afecta al tratamiento de datos personales en el ámbito jurisdiccional, debemos mencionar la siguiente relación de preceptos que nos ayudarán a entender mejor la normativa vigente y aplicable en este contexto:

Citando en primer lugar, como no podría ser de otra manera, a nuestra Carta Magna, norma suprema del Ordenamiento Jurídico Español, debemos mencionar el artículo 18.4 de la Constitución Española, el cuál establece 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”. Este precepto contiene el instituto de garantía sobre el que va a residenciarse el nuevo derecho fundamental a la protección de datos personales reconocido por el **Tribunal Constitucional en la sentencia 292/2000.**

La misma norma contiene en su artículo **24** el derecho a la tutela efectiva de jueces y tribunales y la necesidad de publicidad del proceso, del mismo modo que hace el artículo **120**. Junto a lo anterior, no ha de olvidarse que también la Constitución reconoce en su **Título VI** el ejercicio de la potestad jurisdiccional a juzgados y tribunales, así como la necesidad de colaboración con los jueces en el curso del proceso.

Por otro lado es loable destacar la **Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial**, cuyo articulado recuerda que los Juzgados y Tribunales protegerán los derechos e intereses legítimos, tanto individuales como colectivos, sin que en ningún caso pueda producirse indefensión (artículo **7**).

El mismo texto legal establece en su artículo **230** que los juzgados se verán limitados en el ejercicio de su actividad por los dictados de la legislación de protección de datos y los principios derivados de ésta.

En último lugar, pero no menos destacable, debemos mencionar la **Ley Orgánica 15/1999 de Protección de Datos (en adelante LOPD)**, cuyo artículo **11**, relativo a la comunicación de los datos, uno de los apartados de la Ley que se presta a mayores indagaciones y, en ocasiones, dudas interpretativas, establece que los datos 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, salvo cuando la comunicación que deba efectuarse tenga por destinatarios al Defensor del Pueblo, Ministerio Fiscal, Jueces o Tribunales o el Tribunal de Cuentas (apartado 2, letra d)).

Perteneciente a la propia **LOPD**, su artículo **7.5** nos indica 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, lo que ha provocado, como se verá, no poca controversia. En esta misma línea, el artículo **22** adscribe a esta ley los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal, apuntando que 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.

Por último, debemos referirnos a los artículos **13 a 16** de la **LOPD**, 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.

Hay que advertir junto a este compendio de normas citadas, que la LOPD se ha visto desarrollada por el **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su reglamento de desarrollo (en adelante RLOPD)**, cuya entrada en vigor se produjo a los tres meses de su publicación en el Boletín Oficial del Estado (enero de 2008), es decir en abril de 2008.

III. CONCEPTOS GENERALES

A) CONCEPTOS LEGALES

Centrándonos en la normativa aplicable en materia de protección de datos personales (LOPD) aludiremos a varios conceptos que vienen listados tanto en la LOPD como en el RLOPD y que a la hora de interpretar la amplia casuística que se ha ido produciendo nos van a permitir clarificar los diferentes hechos objeto de análisis. En este sentido cabe destacar los siguientes términos:

Los artículos **3 d) LOPD y 5.1 q) RLOPD** establecen como **Responsable del fichero o tratamiento a la "**Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros **decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente".** Establece el RLOPD como aclaración, que "podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

Son los **artículos 3 g) y 12 LOPD y 5.1 i) RLOPD** los que definen al **Encargado del tratamiento** como la **"**persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, **trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".** Del mismo modo establece el RLOPD que "podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

B) ACUERDOS DEL PLENO DEL CGPJ

Dentro del marco terminológico mencionado y a efectos de conocer la opinión del órgano de Gobierno del Poder Judicial español, el Consejo General del Poder Judicial (en adelante CGPJ), a través de sus diferentes Acuerdos, ha venido estableciendo no sólo qué órganos dentro del Poder Judicial han de ser considerados como responsables de los ficheros y tratamientos pertenecientes al Poder Judicial en cada caso, así como el órgano que ha de asumir la figura del encargado del tratamiento. Del mismo modo se han definido perfectamente los diferentes tipos de ficheros cuya responsabilidad corresponde al Poder Judicial, tanto jurisdiccionales como no jurisdiccionales, la finalidad de los mismos, las medidas de seguridad que han de implementarse en cada una de las bases de datos inscritas en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos y en definitiva la aplicación de los principios de finalidad, calidad, información previa a la recogida de datos junto a la posibilidad del ejercicio de los derechos ARCO (acceso, cancelación, rectificación y oposición). Principios y normas que han de tenerse en cuenta en la gestión y manejo diario de ficheros que contienen datos de carácter personal.

En este sentido debemos destacar el **Acuerdo del CGPJ de 20/09/2006** por el que se crean los ficheros de datos personales dependientes de órganos judiciales, diferenciándose los **ficheros "jurisdiccionales" y "no jurisdiccionales"**.

- A su vez, los ficheros jurisdiccionales se dividirán en ficheros de "Asuntos jurisdiccionales" y ficheros de "Registro de Asuntos", estableciéndose las siguientes categorías dentro de cada fichero:
  - **Fichero "Asuntos jurisdiccionales":**
    - **Responsable del fichero**: CGPJ
    - **Responsable del tratamiento:** órgano judicial que conozca del procedimiento, bajo dependencia del Secretario/a Judicial.
    - **Encargado del tratamiento:** Administración Pública competente en la dotación de bienes materiales (centros, locales, equipos, sistemas, programas, personal técnico,…).
  - **Fichero "Registro de Asuntos":**
    - **Responsable del fichero:** CGPJ
    - **Responsable del tratamiento:** Secretario Judicial encargado del registro.

C) RELACIÓN RESPONSABLE-ENCARGADO (art.20 RLOPD):

Definidos los conceptos sobre los que va a pivotar gran parte de la interpretación normativa en materia de protección de datos, debemos hacer una parada necesaria a efectos de destacar las posibles relaciones que pueden establecerse entre los responsables de ficheros y tratamientos y los encargados de tratamientos (en adelante ET) o prestadores de servicios.

Estas relaciones vienen marcadas por las siguientes particularidades, todas ellas recogidas en la LOPD y en el RLOPD:

- La existencia del encargado del tratamiento viene marcada por el acceso necesario que se produce para la prestación de un servicio al responsable del tratamiento (todo ello bajo la aplicación del principio de proporcionalidad que deberá considerar el responsable).
- Podrá tener o no carácter remunerado y ser temporal o indefinido.
- Existirá comunicación cuando el acceso tenga como objeto establecer nuevo vínculo entre quien accede y el afectado.
- Existe encargo de tratamiento cuando la cesión de datos esté amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado.
- El artículo **12** de la **LOPD** establece una serie de **Garantías** exigibles, entre las cuáles debemos destacar:
    - El tratamiento por cuenta de terceros (ET) debe estar regulado en un contrato escrito o en “alguna otra forma que permita acreditar su celebración y contenido” (firma electrónica, no facturas o comprobantes).
    - El ET tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
    - En el contrato se estipularán las medidas de seguridad que el ET deberá implementar.
    - El responsable del tratamiento deberá velar porque el ET reúna las garantías para cumplir con la LOPD y RLOPD. No podrá eludir responsabilidades o hacer que las mismas recaigan en otras personas físicas o jurídicas.
    - El ET no se convierte en responsable del tratamiento sino que asume consecuencias de ilicitud de tratamiento de datos, de destinar datos a finalidad distinta, comunicarlos o incumplir las estipulaciones del contrato.

- La obligación de inscripción de ficheros corresponde al responsable, si bien cabe la excepción cuando la prestación del servicio exija la creación de un fichero del que el ET será responsable.

IV. OBLIGACIONES LEGALES:

Entre las obligaciones que recoge la normativa aplicable y que los responsables y encargados (éstos últimos según los casos) debemos destacar las siguientes:

• **Creación, modificación y supresión de ficheros (art. 20 LOPD y 55 RLOPD):** establecen los preceptos indicados que esta obligación se materializará por medio de disposición general o acuerdo publicados en el "Boletín Oficial del Estado" o diario oficial correspondiente, indicando: la finalidad y usos previstos, las personas o colectivos sobre los que se pretenda obtener datos personales o que resulten obligados a suministrarlos, el procedimiento de recogida, la estructura del fichero y los tipos de datos incluidos, las cesiones y transferencias previstas, los órganos responsables, los servicios ante los que pudiesen ejercitarse los derechos ARCO y las medidas de seguridad implementadas (indicando el nivel correspondiente a cada fichero).

• **Notificación e Inscripción de ficheros (ante el RGPD):** establece el artículo **55** del **RLOPD** que en el plazo de 30 días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente deberá cumplirse con esta obligación.

• **El deber de información** viene recogido en el artículo **5 LOPD,** el cuál establece que "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

*A modo de ejemplo práctico cabría citar el expediente sancionador abierto por la Agencia (**Resolución de la AEPD AAPP 15/2006**) en el que se imputaba tanto al Consejo General*

del Poder Judicial como al Ministerio de Justicia una posible infracción legal consistente tanto en la creación de ficheros en los que se almacenaban datos personales de los ciudadanos sin la cobertura de una disposición legal que debía haber sido publicada en el Boletín Oficial del Estado (artículo 20.1 LOPD), como en la falta de cumplimiento del deber de información (artículo 5.1 LOPD) a las personas afectadas por la existencia del fichero y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición que prevé la ley. Asimismo, se comprobó que no existía ningún fichero registrado en el Registro General de Protección de Datos del que fuesen responsables esos órganos judiciales.

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.

El artículo 37 de la Ley Orgánica del Poder Judicial regula la aportación de medios materiales para el adecuado funcionamiento de la Administración de Justicia, disponiendo que corresponde al Ministerio de Justicia o al órgano de la Comunidad Autónoma con competencias en materia de justicia proveer a los juzgados y tribunales de los medios precisos para el desarrollo de su función con independencia y eficacia. De este modo la competencia ya aparecía localizada, lo que hacía del Ministerio de Justicia el responsable del fichero, ya que de los contratos establecidos con diversas empresas relativos a la vigilancia y seguridad de los órganos judiciales se desprendía que la empresa contratada iba a actuar como responsable del tratamiento.

Habiendo quedado acreditada la comisión de ambas infracciones, tipificadas como leve (5.1) y grave (20.1) en los artículos 44.2.d) y 44.3.1 LOPD, se requirió al Ministerio de Justicia para que adoptase las medidas de orden interno necesarias para que en el futuro pudiese producirse una nueva infracción de los citados artículos.

• **Implementación de medidas de seguridad e incorporación de las mismas al Documento de Seguridad correspondiente:** El artículo 9 de la 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.

Haciendo una breve alusión nuevamente a la figura del encargado del tratamiento, en relación con las Medidas de seguridad que han de implementarse, los artículos 82 y 83 RLOPD establecen que la prestación del servicio puede realizarse en los locales del responsable o mediante acceso remoto, o bien se puede realizar en

los locales del ET. Cuando la prestación de servicios se realice sin acceso a datos personales (limpieza, mantenimiento, etc…) la prohibición de acceso debe recogerse en el contrato y en caso de existir la posibilidad de acceso debe establecerse la obligación de secreto.

V. SENTENCIA COMO FUENTE PÚBLICA

- **¿Pueden considerarse las sentencias "Fuente de acceso público"?**

En primer lugar debemos diferenciar los conceptos de "fuente pública" y "fuentes accesibles al público", muy diferentes desde el punto de vista de la LOPD pero que en ocasiones su errónea interpretación ha generado una gran controversia: ellos son. Las sentencias judiciales son efectivamente fuente pública, o, dicho de otro modo, gozan del efecto de publicidad procesal general en los términos reconocidos en la Ley Orgánica del Poder Judicial, pero ello no quiere decir que sean "*fuentes accesibles al público* " en el sentido reconocido por la LOPD a los efectos de su tratamiento automatizado, pues es evidente que las sentencias judiciales no se encuentran entre las fuentes accesibles al público que taxativamente enumera el artículo 3 j) de la LOPD.

Consecuentemente con lo anterior, el tratamiento de datos de carácter personal que figuran en sentencias judiciales por persona o entidad distinta a los interesados, en cualquier caso necesitaría para su tratamiento el consentimiento previo de los mismos, no pudiendo considerarse fuente de acceso público general.

Aun así, la Doctrina establece que en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste pueda oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

La última ley de reforma de la Ley Orgánica del Tribunal Constitucional también se ha ocupado del asunto al marcar que el tribunal podrá disponer que las sentencias y demás resoluciones dictadas sean objeto de publicación a través de otros medios, y adoptará en su caso las medidas que estime pertinentes para la protección de los derechos reconocidos en el artículo 18.4 de la Constitución.

- **Potencial editorial de sentencias convertidas en objetos de tráfico comercial.**

En este sentido debemos mencionar la Resolución 00486/2004 de la AEPD a raíz de la queja de una ciudadana que informaba, en relación con una sentencia de la Audiencia Provincial de Las Palmas, publicada en Internet por una Editorial, a través de una página web contratada para la prestación de un servicio concreto, 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 la Editorial argumentaba que en este caso el error procedía de un órgano de la Administración del que se presume un correcto proceder en sus actuaciones. El CENDOJ alegó, no obstante, que en el contrato celebrado con la Editorial, ésta se había comprometido a proceder a la anonimización de los datos personales que apareciesen en las sentencias. La AEPD estimó en este caso una infracción del artículo 6 LOPD calificado como "grave", imponiendo la multa correspondiente a dicha Editorial.

VI. PRINCIPIOS GENERALES

- **Finalidad, Calidad y Proporcionalidad (Art. 4 LOPD):**

Establece el precepto citado que los datos se tratarán de forma leal y lícita, debiendo ser las finalidades que justificaron la recogida de datos determinadas, explícitas y legítimas.

Además los datos recabados deberán ser adecuados, pertinentes y no excesivos en relación con la finalidad que justificó su recogida, debiendo el responsable garantizar que los datos sean en todo momento exactos y veraces en relación con la situación actual. En este sentido se consideran datos exactos los recogidos directamente del afectado.

Si se examinan los principales límites que el juez encuentra en su actuación, es evidente la preponderancia del principio de proporcionalidad, que goza de una especial operatividad en este campo.

- **Información previa a la recogida de datos personales (Art. 5 LOPD):**

Uno de los principios de protección de datos que el juez ha de tener en cuenta en el proceso es el que determina que las partes

hayan de ser informadas del tratamiento que se haga de sus datos. 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 un informe emitido en el año 2000.

Sin embargo, en ocasiones el juez se ve habilitado a realizar una excepción a la publicidad del proceso y la necesidad de información, justificada en la protección de otro bien constitucionalmente relevante y ser siempre congruentes y proporcionadas con el fin que se pretende conseguir. En estos casos, el juez debe actuar con una extraordinaria cautela, pudiendo un error llevarle a su separación o suspensión.

> *Recuérdese, a estos efectos, el caso del magistrado de un juzgado de instrucción de Salamanca que decidía en 2002 que* ***constase en autos el domicilio y patrimonio de una mujer que había sido objeto de violencia de género****, para imponerle así una multa por el régimen de visitas de la hija al ex marido de la misma, cuyo conocimiento de este extremo acarreaba en buena lógica una mayor vulnerabilidad de ésta, toda vez que éste había sido reconocido como autor de los maltratos que se habían ido produciendo durante la convivencia matrimonial*

- **Consentimiento previo (Art. 6 LOPD):**

Uno de los pilares básicos de la normativa reguladora del tratamiento de datos personales es el principio del consentimiento o autodeterminación, cuya garantía estriba en que el afectado preste su consentimiento consciente e informado para que la recogida de datos sea lícita. 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.

El consentimiento del afectado que se exige para el tratamiento de los datos de carácter personal habrá de ser un **consentimiento inequívoco**, salvo que la ley disponga otra cosa, por lo que no cabe un consentimiento tácito. Esto supuso una novedad de la actual ley con respecto a la anterior, en la que el adjetivo “inequívoco” no aparecía.

En este sentido hay que destacar que el consentimiento recabado se caracteriza por ser **Libre**, **Inequívoco** (no presunto), **Específico** e **Informado**. De acuerdo con la normativa vigente, la recogida de datos de menores (inferiores a 14 años) deberá contar con el consentimiento de los padres o tutores correspondientes.

- Finalmente, los artículos **7 y 8** LOPD establecen un régimen específico para los **datos especialmente protegidos**, diferenciando dentro de los mismos dos categorías: los datos que revelen la ideología, afiliación sindical, religión y creencias, los cuáles sólo podrán ser objeto de tratamiento cuando previamente se recabe el consentimiento expreso y por escrito del afectado; y los datos personales que hagan referencia al origen racial, la salud y a la vida sexual, que podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

VII. DERECHOS ARCO -Acceso, Rectificación, Cancelación y Oposición- (Arts 15 a 18, 6.4 y 30.4 LOPD):

Tanto el derecho de acceso, por el que el titular de los datos puede solicitar y obtener información de sus datos personales (origen, cesiones, usos y finalidades), como el derecho de rectificación y cancelación por el que su titular tiene derecho a que se rectifiquen o cancelen sus datos, en los supuestos establecidos en la LOPD, así como el derecho de oposición, por el que el afectado tiene derecho a oponerse al tratamiento de sus datos en los casos en que no sea necesario su consentimiento o bien, previa petición y sin gastos, al tratamiento de sus datos con fines de publicidad y prospección comercial, se caracterizan por los siguientes rasgos: son derechos **Personalísimos** (se ejercen por afectado o representante acreditado), **Independientes** (no se exige ejercicio previo de otros derechos) y cuyo ejercicio ha de facilitarse a través de **medios sencillos y gratuitos**, debemos destacar que tales derechos se ejercen **ante el responsable o encargado del tratamiento** (salvo los derechos de Información, Indemnización y Consulta).

El procedimiento para el ejercicio de los mismos y sus peculiaridades se han desarrollado mediante el **RLOPD**.

Haciendo una breve alusión a la figura del encargado del tratamiento, establece el artículo 26 del RLOPD dos posibilidades en relación con el ejercicio de los derechos ARCO ante dicha figura, permitiendo que el propio encargado atienda la solicitud del titular como parte de la prestación del servicio o bien le da traslado al responsable para que actúe en consecuencia. Esta circunstancia deberá quedar prevista en la relación mantenida entre el responsable y el encargado.

VIII. INFORMES Y RESOLUCIONES AEPD, SSAN:

La práctica jurídica ha venido demostrando a lo largo de la historia de nuestro ordenamiento, que es la mejor manera de valorar la eficacia y validez de una norma a la hora aplicar la misma a los

diferentes objetos y ámbitos correspondientes, todo ello aderezado con un compendio muy extenso de resoluciones e informes por parte de los organismos reguladores así como por la propia jurisprudencia de los tribunales, la cuál ha aplicarse en última instancia.

En este sentido se ha considerado conveniente traer a colación una serie de casos prácticos reales, sobre los que la AEPD ha informado o resuelto, según el momento y las circunstancias, así como una serie de Sentencias de la Audiencia Nacional, organismo que resuelve aquellos recursos interpuestos contra las resoluciones de la AEPD, al agotar éstas la vía administrativa previa.

- En primer lugar destacaremos el **Informe del Gabinete Jurídico de la AEPD 99/2009** donde se planteaba una consulta relativa a la vigilancia a través de sistemas de cámaras o video cámaras en las alas de interrogatorios y otras dependencias policiales.

Realizadas las consideraciones oportunas sobre la normativa aplicable, si bien es cierto que la Ley 4/1997 regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, su Reglamento de desarrollo y ejecución (Real Decreto 596/1999), establece que " *Las unidades de Policía Judicial reguladas en la legislación de Fuerzas y Cuerpos de Seguridad, cuando, en el desempeño de funciones de policía judicial en sentido estricto, realicen captaciones de imágenes y sonidos mediante videocámaras, se regirán por la Ley de Enjuiciamiento Criminal y por su normativa específica*".

Hechas las anteriores aclaraciones, por las que se confirma que el Reglamento citado no es de aplicación al caso planteado y teniendo en cuenta que la actividad consultada pertenece al grupo de funciones propias de la Policía Judicial, de acuerdo con los artículos 547 y 549 de la Ley Orgánica 6/1985, del poder Judicial, la AEPD consideró plenamente aplicable la LOPD.

En este sentido sería de aplicación el artículo 22.2 de la LOPD que regula la legitimación de las Fuerzas y Cuerpos de Seguridad para recoger y tratar datos personales con fines policiales sin obtener el consentimiento de los afectados siempre y cuando *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.*

El Gabinete Jurídico recuerda la obligación de aplicar los principios de calidad y proporcionalidad que regula la LOPD (art. 4) a la hora de proceder a la recogida de datos personales (imágenes).

Del mismo modo se recuerda la obligación de cumplir con el deber de informar (art. 5 LOPD, así como las normas correspondientes al ejercicio de los derechos correspondientes por parte de los titulares de los datos.

Finalmente se informa de las obligaciones que han de cumplirse en materia de creación, notificación e inscripción de ficheros al Registro General de la AEPD así como las medidas de seguridad que han de

implementarse en los ficheros y su recogida en el correspondiente documento de seguridad.

- En segundo lugar mencionaremos la **Resolución PS 684/2008 de la AEPD** que tuvo lugar a raíz de la queja de un ciudadano que informaba, en relación con una serie de sentencias publicadas en Internet por una Editorial a través de una página web donde figuraban datos que permitían su identificación.

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 la Editorial reconoció los hechos imputados alegando que se habían debido a la comisión de un error humano cuando la citada empresa era responsable de suprimir los datos personales que figurasen en las sentencias, circunstancia que se tuvo en cuenta a la hora de resolver. La AEPD estimó en este caso una infracción del artículo 6 LOPD, calificada como "grave", al haberse producido un tratamiento sin consentimiento y una infracción del art. 10, calificada como leve, por vulneración del secreto profesional, imponiendo la sanción correspondiente a dicha editorial pero únicamente por la infracción grave, tal y como establece el principio de subsunción de infracciones del art. 4 del Real Decreto 1398/1993 por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora.

- A continuación procede mencionar las **Resoluciones AP 53/2007, 15/2009 y 20/2009 de la AEPD**, correspondientes al hallazgo en la vía pública de documentación judicial perteneciente a diferentes juzgados:

Realizadas las inspecciones correspondientes sobre los ficheros y bases de datos de los que procedía la documentación hallada y evaluadas las medidas de seguridad implementadas por cada uno de los tribunales denunciados, la AEPD procedió a determinar las correspondientes responsabilidades en base a los Acuerdos del Consejo General del Poder Judicial, mediante los cuáles se establece en cada ámbito territorial correspondiente, que órgano o unidad judicial asume la figura de responsable del fichero o tratamiento así como la posibilidad de intervenir un encargado del tratamiento.

En este sentido debemos remitirnos al contenido de dichos Acuerdos del CGPJ, ya mencionados a lo largo de la exposición del presente documento.

La AEPD resolvió que el encargado del tratamiento había infringido el artículo 9 de la LOPD, al incumplir la obligación de adoptar las medidas de índole técnica y organizativa que garantizasen la seguridad de los datos personales.

- Las resoluciones que determinan la infracción de la LOPD por parte de una Administración Pública, si bien es cierto que no llevan aparejada una sanción económica, tienen una serie de efectos entre los cuáles destaca la notificación de la misma al Defensor del Pueblo, al responsable del fichero, al órgano del que dependa

jerárquicamente y a los afectados si los hubiera. Por otro lado, será de comunicación obligada a la AEPD las resoluciones que se dicten por el propio órgano o Administración responsable, en relación con las medidas y actuaciones adoptadas en el plazo de un mes. Además el Director de la AEPD tiene la posibilidad de proponer la iniciación de actuaciones disciplinarias.

- Entre las Sentencias dictadas por la Audiencia Nacional hemos querido destacar la **SAN de 3 de noviembre de 2004** donde se desestimó el recurso contencioso-administrativo presentado por la entidad recurrente y que previamente había sido sancionada por la AEPD por una vulneración del deber de secreto profesional (art. 10 LOPD).

El presente caso se inicia con la petición a una entidad financiera por parte de un Juzgado de Instrucción de Sevilla, de los movimientos de varias cuentas bancarias a nombre del denunciante.

La información no fue remitida al Órgano jurisdiccional solicitante sino a la Policía Nacional, dando a conocer de forma injustificada datos sobre movimientos bancarios de cuentas a nombre del afectado

La Resolución de la AEPD motivó la vulneración del secreto profesional demostrando que la entidad denunciada extralimitó el contenido del mandato judicial al remitir más cuentas de las solicitadas además de aportar un rango mayor de fechas del requerido por el juzgado. No pudiendo quedar amparada dicha información bajo la cobertura del artículo 11.2 d) que establece una excepción, por los destinatarios a los que se remite información con datos personales sin recabar el consentimiento del titular de los mismos.

La Audiencia Nacional, desestimó el recurso interpuesto contra la resolución de la AEPD y confirmó dicho acto por considerarlo conforme al ordenamiento jurídico.

- Finalmente procedemos a citar la **SAN de 9 de octubre de 2009**, por la que se estimó el recurso contencioso administrativo interpuesto por el Ministerio Fiscal contra Resolución de la AEPD, procedimiento de tutela de derechos TD 592/2008 por el que se tutelaba la cancelación de datos de un menor en poder de la Fiscalía de Madrid.

La Sentencia no pone en duda la falta de legitimación del padre del menor (representante), ni de la competencia de la AEPD para entender de la reclamación presentada por el padre ante la AEPD, una vez que le ha sido denegada la cancelación de los datos de su hijo menor de edad.

Sin embargo, y pese a los argumentos de la AEPD, considerando que deben aplicarse los principios de Calidad y Finalidad (art. 4 LOPD) y en base a los mismos, proceder a la cancelación de los datos del menor, la Audiencia estima que no procede tramitar la solicitud de cancelación de los datos del menor hasta que éste alcance la mayoría de edad. Esta decisión ampara el argumento de la Fiscalía que defendía que los datos del menor debían conservarse hasta que alcanzase la mayoría de edad ya que además de cumplir con la finalidad de su hipotética utilización para el adecuado ejercicio de las competencias atribuidas por Ley al Ministerio Fiscal, sirven

para acreditar la actividad del Ministerio Fiscal y el concreto desarrollo de sus funciones.

La Audiencia falla estimando el recurso contencioso-administrativo interpuesto por el Ministerio Fiscal contra la resolución de la AEPD, anulando ésta por considerarla contraria a Derecho.

IX. COOPERACIÓN JUDICIAL

Fruto de la estrecha relación laboral que existe entre la Administración y los Tribunales de Justicia, no sólo por el conocimiento de los recursos que frente a las resoluciones del órgano administrativo deben resolver los tribunales correspondientes, sino porque los jueces han de establecer un balance, en ocasiones más bien una prioridad, entre los derechos que pudieran entrar en conflicto y determinar los principios generales aplicables; la Cooperación Judicial, tanto a nivel nacional como internacional ha de ocupar una posición prioritaria en el devenir de una adecuada protección de los Derechos Fundamentales, como es el de la Protección de Datos Personales.

En este sentido destacan las iniciativas que a nivel internacional como nacional se han venido desarrollando:

- **A nivel europeo**, dentro del marco de las políticas de libre circulación se pretende posibilitar a empresas y particulares el ejercicio de derechos en cualquier Estado miembro y bajo las mismas condiciones (mejorando el acceso a la Justicia, reconocimiento mutuo de decisiones judiciales y aumento de convergencia en el ámbito de las leyes procesales). Desde 2002 existe una Red Judicial Europea para asuntos civiles y comerciales.

- **A nivel nacional**, y como iniciativa más reciente, debemos mencionar el **Convenio de Colaboración** firmado entre la **AEPD y el Consejo General del Poder Judicial (3 mayo 2010), sobre inspección de órganos jurisdiccionales.**

Destacan entre los objetivos de este Convenio los siguientes:

- reforzar la protección de datos en la Administración de Justicia (actuaciones de inspección conjuntas y reuniones periódicas para promover la efectiva vigencia de la normativa de protección de datos).
- efectiva implantación de las medidas y garantías a adoptar por quienes conforman la Administración de Justicia.

No hay que olvidar, a la hora de analizar la actividad de los tribunales jurisdiccionales y su relación con el tratamiento de datos

personales, una particularidad digna de mención, que no es otra que la de considerar la doble condición de los jueces: como garantes de derechos y libertades en el ejercicio de sus funciones pero al mismo tiempo como responsables de la información personal que se trata en los ficheros y bases de datos dependientes de las unidades que ellos dirigen.

X. CONCLUSIONES:

El creciente interés por el problema de la tutela de la persona frente al tratamiento de sus datos personales es una realidad que no podemos omitir**. Además del esfuerzo legislativo es necesaria una reflexión del propio sistema de justicia.** Con lo realizado hasta la fecha se ha pretendido dar respuesta a lo recomendado en el preámbulo de la Carta de Derechos del Ciudadano ante la Justicia, en la que expresamente se indica: *"En los umbrales del siglo XXI la sociedad española demanda con urgencia una Justicia más abierta que sea capaz de dar servicio a los ciudadanos con mayor agilidad, calidad y eficacia, incorporando para ello métodos de organización e instrumentos procesales más modernos y avanzados."* **Pero para lograr la consecución de estos objetivos, la función jurisdiccional enfrenta aún una serie de retos entre los que cabe destacar los siguientes:**

En primer lugar, y a la luz del nuevo Reglamento de la LOPD, se hace necesario **incorporar por completo las medidas de seguridad** indicadas para todas las aplicaciones informáticas de gestión procesal, teniendo en cuenta la estructura de la oficina judicial que ha surgido tras la aprobación del nuevo Reglamento 1/2005, que ha supuesto la adaptación de la vieja secretaría a las nuevas tecnologías, y a un programa eficiente y racional de ordenación de recursos humanos y de servicios comunes procesales, alentando el establecimiento de un sistema de organización más ágil y eficaz.

En segundo lugar, **los jueces deberán conocer mejor la legislación sobre protección de datos,** evitando contradecir en sus sentencias los criterios ya consolidados en materia de protección tanto por la Jurisprudencia como por la propia Agencia Española de Protección de Datos. El juez deberá además velar especialmente por la protección de datos personales que se obtengan de las estadísticas judiciales, tal y como rezan los principios del Plan de Transparencia Judicial de 2005.

Por último, también **el propio legislador tiene aún ante sí un haz de retos en materia jurisdiccional** y de seguridad, teniendo presente que cualquier despliegue de fórmulas que pretendan armonizar el tratamiento de datos personales con fines

policiales, introduciendo la obligación de retener determinados datos, incluso mediante la creación de nuevas bases de datos, unido a la intención u obligación de poner a disposición esta información a las autoridades con competencia en materia de seguridad, debe estar sujeta al cumplimiento de especiales garantías, sobre todo en términos de seguridad jurídica, cumplimiento del principio finalidad y proporcionalidad.

En definitiva, todavía existen cuestiones que precisan de un tratamiento normativo con rango suficiente. Por eso es cada vez más necesaria la elaboración de disposiciones legales que regulen de una manera completa y sistemática el régimen jurídico de la protección de datos y muy especialmente de la gestión de los ficheros.

La falta de de garantías del Poder Judicial puede trastocar el sentido original de éste, conscientes de que ser equilibrados en la aplicación de los principios en juego es y será una tarea enorme, no debiendo el Poder Judicial cesar en esta continua batalla por el respeto a los derechos individuales y el ejercicio de la responsabilidad del Estado.

Montevideo, 3 de junio de 2010.

Vicente M. González Camacho
Secretaría Permanente Red Iberoamericana
Agencia Española de Protección de Datos