



**2<sup>a</sup>**  
**sesión**  
**anual**  
**abierta**  
**de la** AGENCIA  
ESPAÑOLA DE  
PROTECCIÓN  
DE DATOS



# PRINCIPALES NOVEDADES Y DESARROLLOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES CONSULTAS RELEVANTES REALIZADAS EN 2008

**AGUSTÍN PUENTE ESCOBAR**  
**Abogado del Estado-Jefe del Gabinete**  
**Jurídico de la AEPD**

- **Delimitación del concepto de fichero**
  - Cancelación en Libros de bautismo
  - Existencia de fichero en caso de conservación y actualización periódica de datos
- **Protección de datos y libertad de información**
  - No ampara la creación de un fichero de infracciones penales o procesos en curso
- **Consentimiento**
  - Si se recaban y se ceden posteriormente datos sin probar el consentimiento existen dos infracciones de la LOPD
- **Encargado del tratamiento**
  - Necesidad de contrato escrito que acredite su contenido y el cumplimiento del art. 12 LOPD

- **Caducidad del procedimiento.**
  - **Cómputo de los seis meses a partir de la fecha del Acuerdo de Inicio.**
- **Recursos contencioso-administrativos contra resoluciones de archivo.**
  - **El denunciante debe probar que la apertura del procedimiento puede producir un efecto positivo en su esfera jurídica o eliminar una carga o gravamen (en el supuesto analizado se rechaza la legitimación).**

- **Ámbito de aplicación.**
  - Debe probarse la existencia de fichero o tratamiento.
    - Envío a un antiguo paciente.
    - Informes elaborados en un procedimiento administrativo.
    - Informes que no están grabados en un ordenador
  - Deben existir datos personales.
    - El DNI siempre es un dato personal.
    - El simple tratamiento de número de teléfono no implica necesariamente la existencia de datos.
  - Aplicación de la LOPD a profesionales no empresarios.
    - Médicos, arquitectos, farmacéuticos.

# Sentencias de interés de la Audiencia Nacional

- **Conceptos generales.**
  - **Dato de salud.**
    - **No lo es la mera indicación de la fecha de baja.**
  - **Fuentes accesibles al público.**
    - **Pueden serlo los listados de profesionales médicos de una compañía de asistencia sanitaria.**
    - **Internet, en general no puede ser considerado un medio de comunicación a los efectos de la LOPD.**
    - **Irrelevancia de la procedencia de los datos en caso de “spam”. Será siempre necesario el consentimiento (LSSI).**
  - **Ficheros de titularidad pública.**
    - **Lo son los de un hospital constituido como fundación, aún no siendo fundación pública sanitaria.**
    - **En los ficheros de los Colegios profesionales se estará al ejercicio de competencias administrativas para que sus ficheros sean de titularidad pública.**

- **Calidad de datos.**
  - **Fin compatible.**
    - **Asimilación a “*fin distinto*”.**
    - **Casos.**
      - **Uso por un banco de los datos del deudor hipotecario para la generación de un contrato de seguro de vida asociado por la aseguradora del grupo (incompatible).**
      - **Revelación del dato del titular de un bien embargado a la entidad mediadora en su venta (compatible).**
  - **Exactitud. Casos reiterados.**
    - **Solvencia.**
    - **Designación del conductor habitual.**
  - **Fraude.**
    - **Necesidad de prueba adicional que acredite su existencia.**
    - **La AEPD puede valorar mínimamente la existencia de contratos en la investigación de contrataciones fraudulentas.**

- **Legitimación para el tratamiento.**
  - Admisibilidad de la habilitación legal no expresa (sector de hidrocarburos).
  - Casos especiales.
    - Prevención de riesgos laborales.
    - Mediación de seguros privados.
- **Consentimiento.**
  - Carga de la prueba (al menos indiciaria) del responsable.
  - Exigibilidad en datos añadidos por empresas de recobro.
  - Revocación.
    - Es posible en caso de clientes para fines no relacionados con el contrato (envío de publicidad). No cabe invocar la relación jurídica.
    - No pueden exigirse requisitos formales adicionales.

# Sentencias de interés de la Audiencia Nacional

- **Deber de información.**
  - **Procede siempre que los datos “se recaben” del afectado.**
    - **Valoración de la doctrina previa en caso de uso de tarjetas. Caso específico no extrapolable.**
- **Tutelas de derechos. Reclamaciones de personas de relevancia pública contra medios de comunicación.**
  - **Las imágenes obtenidas o divulgadas son datos de carácter personal.**
  - **No prevalece la libertad de información en caso de que los datos divulgados no sean veraces.**
  - **Necesidad de atender a la pretensión en cada caso y la naturaleza de las alegaciones (no referidas al honor o intimidad).**

- **Medidas de seguridad.**
  - La historia laboral es un conjunto de datos que valora la personalidad: nivel medio.
  - Documentos en la vía pública.
    - Obligación de resultado: no basta la existencia de medidas sino su efectividad real.
    - Supone también una vulneración del deber de secreto (concurso medial).
    - Necesidad de que pueda vincularse a un responsable concreto.
  - En caso de subcontratación, el encargado responderá en caso de incumplimiento de las medidas por el “subencargado”: deber de diligencia.

# Sentencias de interés de la Audiencia Nacional

- **Vulneración del deber de secreto. Casos.**
  - **Existencia.**
    - Revelación por un Juez de datos de bajas de un funcionario de un Juzgado a la Fiscalía.
    - Publicación de datos en la fachada de un Ayuntamiento.
    - Notificación por un órgano arbitral con datos de no intervinientes en el procedimiento arbitral.
    - Revelación a un detective de datos de consumo eléctrico.
    - Acceso por un funcionario de la Seguridad Social a la historia laboral de su hija.
  - **Inexistencia.**
    - Envío de información bancaria a ex-cónyuge en sobre cerrado.
    - Comunicación a otros vecinos de los datos de un vecino que demanda a la comunidad.

- **Ficheros del artículo 29.2 LOPD.**
  - **Requisitos de la deuda.**
    - **No procede la inclusión si:**
      - **Existe reclamación arbitral o reclamación ante la OMIC.**
      - **La deuda ha sido consignada judicialmente.**
      - **La deuda ha sido incluida en un convenio de quita.**
    - **Si existen reclamaciones directas al acreedor negando la existencia de la deuda es exigible una especial diligencia y cautela.**
  - **Requerimiento previo. Principio antiformalista.**
  - **Necesidad de prueba al menos indiciaria de**
    - **Requerimiento de pago previo.**
    - **Notificación de inclusión.**

- **Ficheros de publicidad y prospección comercial.**
  - **Principio general: “la externalización de servicios no puede crear zonas de impunidad de la LOPD”.**
  - **Aplicación de la doctrina del TS sobre el beneficiario de la publicidad como responsable del tratamiento.**
    - **Deber de diligencia en relación con el origen de los datos y la constatación de la existencia, en su caso, de consentimiento.**
  - **El “listbroker” que actúa en nombre propio con el beneficiario de la publicidad y que le factura directamente es un responsable del fichero que debe contar con el consentimiento de los afectados.**

# Sentencias de interés de la Audiencia Nacional

- **Procedimiento sancionador.**
  - **Aplicación del principio de confianza legítima.**
    - **Inspección para comprobar normalización lingüística en centros sanitarios.**
  - **Cambio de criterio.**
    - **Si los hechos son anteriores falta culpabilidad aunque la conducta sea contraria a la LOPD.**
  - **Duración de actuaciones inspectoras.**
    - **Criterio de la duración inferior a doce meses.**
    - **Apreciación del incremento de la carga de trabajo de la AEPD.**
  - **Publicación de las resoluciones (instrucción 1/2004 de la AEPD).**
    - **La publicación no es en sí misma una sanción añadida.**
    - **Sólo procede disociar los datos de personas físicas.**

# Sentencias de interés de la Audiencia Nacional

- **Aplicación 45.5 LOPD.**
  - **Es necesario atender siempre a las circunstancias del caso concreto.**
  - **Posibles criterios.**
    - **Medidas correctoras.**
    - **Falta de reincidencia.**
    - **Falta de perjuicio para el afectado.**
    - **Falta de beneficio para el infractor.**
    - **Intencionalidad de la conducta.**
    - **Existencia de un nivel de diligencia mínimo.**
    - **Precedentes en resoluciones de la AEPD referidas al mismo infractor.**

- **Ámbito de aplicación.**
  - **Criterios de aplicación de los artículos 2.2 y 2.3 RDLOPD.**
    - **Especial importancia de la finalidad del tratamiento.**
    - **Limitación de los datos en el artículo 2.2.**
    - **La exclusión no opera si la LOPD sólo es aplicable a algunos datos.**
  - **Aplicación de la Ley española.**
    - **El criterio del establecimiento se aplica sólo si el responsable está en la UE.**
    - **Delimitación del uso de “medios” en España si el responsable no está en la UE.**

- **Conceptos legales.**
  - **Responsable.**
    - **Aplicación a entidades sin personalidad (Grupos Municipales).**
    - **Lo son, en general, las empresas contratadas para la gestión de servicios públicos.**
  - **Fuentes accesibles al público.**
    - **Las listas de profesionales pueden no ser de Colegios Profesionales (listado de médicos de compañía aseguradora en Internet).**
  - **Datos especialmente protegidos.**
    - **No tiene este carácter la opción por la Iglesia Católica en la declaración del IRPF.**

- **Calidad de datos.**
  - **Confidencialidad en sistemas de denuncias.**
  - **Conservación de datos de empresarios que ya no desarrollan la actividad (límites temporales).**
  - **Proporcionalidad.**
    - **Acceso a datos de historias clínicas.**
    - **Accesos en aplicaciones (proporcionalidad para evitar la cesión).**
- **Deber de informar.**
  - **Suficiencia si se han adoptado medidas adecuadas en intentos previos.**
  - **Presunción de exactitud del dato del domicilio.**

- **Legitimación para el tratamiento.**
  - **Excepción legal: interés legítimo derivado de la garantía de la libre competencia.**
  - **Interés legítimo vinculado a urgencia vital.**
  - **Otros casos.**
    - **Prevención de riesgos laborales.**
    - **Publicación de sentencias de maltrato.**
    - **Aplicación de un sistema educativo autonómico.**
    - **Grabación de conversaciones.**
    - **Acceso por aspirante rechazado al expediente del proceso selectivo.**
    - **Listados de morosos en comunidades de propietarios.**

- **Derecho de cancelación.**
  - No opera en relación con datos que se derivan de actos administrativos (Registro Central de Personal).
- **Seguridad: Alcance de las excepciones del artículo 81 RDLOPD.**
  - Criterio general.
  - Supuestos.
    - Ficheros de nóminas y personal.
    - Ficheros relacionados con declaraciones del IRPF.
    - Ficheros de personas con movilidad reducida.
    - No aplicación a confesiones religiosas, partidos o sindicatos.

- **Historias clínicas.**
  - **Proporcionalidad.**
    - **En el contenido.**
    - **En el acceso a los datos.**
  - **Accesos.**
    - **Por personal sanitario (criterio extensivo).**
    - **Por inspección sanitaria.**
    - **Por personal religioso.**
    - **Respecto a personas fallecidas.**
  - **Uso por el facultativo (tutela judicial efectiva).**
  - **Conservación y ejercicio de derechos.**
    - **Sistemas en relación con la medicina privada.**

- **Transferencias internacionales.**
  - No la hay si se produce dentro del Espacio Económico Europeo.
  - La hay en la comunicación desde una sucursal en España a la empresa ubicada fuera de la UE (línea aérea).
- **Aplicación LSSI.**
  - Ampara a las personas jurídicas.
  - Comunicación comercial.
    - No vulnera la LSSI la efectuada por sindicatos en el ejercicio de la libertad sindical.
    - Puede haberla aún cuando se realice por una entidad sin ánimo de lucro (software “libre”).

- **Comunicaciones electrónicas.**
  - **Posibilidad de directorios inversos.**
    - Siempre que el abonado haya dado su consentimiento para figurar en ellos.
  - **Aplicación de la Ley 25/2007 y la LOPD.**
    - Respecto de personas físicas resulta plenamente aplicable la LOPD.
    - Respecto de personas jurídicas son aplicables las normas de protección de datos del artículo 8 de la Ley 25/2007.
  - **Secreto de la comunicaciones.**
    - Acceso por la AEPD a datos de tráfico (informe de la Abogacía General del Estado).

## PRINCIPALES CASOS DE 2008

**JOSÉ LÓPEZ CALVO**  
Subdirector de Inspección de la AEPD

La transparencia se garantiza habilitando el acceso a la información a los participantes en el proceso. Por el contrario se considera que prevalecerá el derecho a la protección de datos en el caso de que se permita el acceso a la información a terceros no afectados por el proceso mediante su inserción en una página web o tablón de anuncios accesible libremente. Ejemplos:

a) Publicación en tablón de anuncios accesible a terceros de baremación para la *adjudicación de plazas de colegios concertados* incluyendo datos de renta o enfermedad.

- b) Inserción en el tablón de anuncios de un colegio del listado de *alumnos beneficiarios de becas*.**
- c) Inclusión en una Web de un partido político de los *adjudicatarios de viviendas de protección oficial con irregularidades (DNI)*. Incluyendo información personal.**
- d) publicación en Web de apellidos, indicación de admitido o excluido, DNI, nº de móvil, domicilio y titulación de *candidatos a plaza en un Universidad*.**
- e) incumplimiento del deber de secreto, al publicar en su Diario Oficial una resolución en la que figuraban los nombres, apellidos y DNI de treinta *personas beneficiarios de ayudas para el tratamiento de drogodependencias*.**

**La utilización de mecanismos para el otorgamiento de consentimiento a distancia debe ser combinado con las garantías necesarias para que quede garantizado.**

***- Necesidad de prueba en la contratación.***

**Necesidad de disponer de mecanismos probatorios suficientes como grabación telefónica de la conversación, comunicación de bienvenida y/o documento escrito debidamente rubricado.**

**Es la empresa contratante quien debe probar que ha recaído consentimiento.**

- ***Contratación de menores.*** Se han dictado resoluciones sancionando la contratación con menores como titulares en el ámbito de telefonía móvil.

Se sancionó a una editorial y se declaró una infracción de la LOPD por parte de un colegio público, por utilizar y publicar en un libro los datos de un alumno de primaria sin el consentimiento de sus padres.

- ***Consentimiento tácito.***

Dos sanciones a sendas Asociaciones constituidas por antiguos miembros de dos Cámaras Urbanas de la Propiedad del País Vasco, disueltas por Decreto, que habían utilizados los datos de miles de antiguos asociados llegando a cargar cuotas.

**Se tuvo en cuenta la ambigüedad de la carta enviada a los antiguos asociados que hacía imposible deducir la finalidad del consentimiento y el hecho de que no concedía plazo alguno (debe ser de 30 días) para que los afectados pudieran oponerse al tratamiento sin que pudiera inducirse que hubiera habido consentimiento inequívoco y libre, como se exige para que pueda concurrir consentimiento tácito.**

- **Diferenciación entre datos profesionales y privados. Tanto el representante sindical como el directivo empresarial tienen derecho, a pesar de los deberes que derivan de su condición, a mantener su esfera de privacidad, que alcanza a la no divulgación de sus datos particulares.**
- **Envío por correo electrónico a los trabajadores de información sindical. Los sindicatos pueden enviar correos electrónicos a los trabajadores pertenecientes al ámbito empresarial que representan. El derecho de oposición deberá ser atendido salvo en caso de periodo preelectoral.**

## a) *Internet*

- Visualización en tiempo real de imágenes. Deben cumplir requisitos de videovigilancia. No pueden mostrarse en abierto si incluyen imágenes identificables de personas.
- Videos en páginas web (YouTube).

Multa a los responsables de la grabación y posterior publicación en “*YouTube*” de imágenes en las que se podía identificar a transeúntes en la calle Montera de Madrid.

## b) *Espacio captado por cámaras de vídeo.*

Cámaras de videovigilancia en el Instituto público que incluye baños. Necesidad de aplicar el principio de proporcionalidad.

**En 2008 se acometió un “Plan Sectorial de Oficio sobre publicidad telefónica”, y se han recibido múltiples denuncias. Entre otros criterios:**

- No caben llamadas automáticas sin consentimiento.**
- No caben llamadas con operador a fijo si se ha indicado en las guías telefónicas el deseo de no recibirlas.**
- No cabe el envío de SMS comerciales sin consentimiento expreso o relación comercial en los mismos servicios.**

**Al respecto, cabe resaltar el archivo durante 2008 de una investigación contra una clínica al constatar que la información personal contenida en residuos clínicos se encontraba en bidones herméticos y opacos que fueron incautados por la Guardia Civil en el transcurso de una inspección sin que constara acceso no autorizado, ni puesta a disposición de terceros, ni que la información se encontrase en vía pública. Junto a ellos se han localizado en la vía pública documentos con datos referentes a menores inmigrantes, tarjetas sanitarias o bufetes de abogados.**

## a) En materia de cancelación.

- **Buscadores en Internet.** La cancelación no solo afecta a buscadores sino que los webmaster deben cooperar evitando la indexación.
- **Cancelación en los registros de la Fiscalía de Menores de ficheros que incluyen denuncias frente a menores que fueron finalmente archivadas.**
- **No cabe invocar derecho de cancelación a informes técnicos realizados por profesionales. Son informes subjetivos.**
- **Cancelación de datos en foros de Internet si no son insertados por quien está vinculado por deber de secreto.**

## b) derecho de acceso.

- **No incluye valoración de solvencia económica.**
- **Imágenes tomadas por cámaras de videovigilancia.**

**c) Rectificación.**

- Bases de cotización contenida en ficheros de la Seguridad Social.

**d) Oposición.**

- Acuses de recibo se refleja el DNI del personal del Servicio de Correos y Telégrafos que realiza la entrega del correo.
- Publicidad de una empresa con la que se tiene contrato.

# DESARROLLOS INTERNACIONALES

## RAFAEL GARCÍA GOZALO

**Coordinador del Área Internacional**

- **Principales novedades producidas en ámbito UE.**
- **España como sede de la XXXI Conferencia Internacional de Privacidad.**
- **AEPD líder del proceso de redacción de Propuesta Común de Estándares Internacionales de Protección.**

Aprobados 3 Documentos de Trabajo (junio 08), que aclaran o complementan el régimen de ordenación de BCR establecido en anteriores documentos (WP 74 y 108).

[www.ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2008\\_en.htm](http://www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm)

- **Documento de trabajo estableciendo la Estructura de BCR (WP154)**  
Resume en 23 puntos el contenido básico que toda BCR debe incluir para ser aprobada por las autoridades europeas de supervisión.
- **Documento de trabajo. Preguntas Frecuentes (FAQs) relativas a BCR (WP155).**
  - Da respuesta a algunos de los errores o preguntas más comunes en relación con las BCR.
  - 9 “preguntas con respuesta” publicadas, si bien está previsto incrementar este número progresivamente.
- **Documento de trabajo. Cuadro de Elementos y Principios de BCR (WP153).**
  - Tabla que ordena, clasifica y explica las obligaciones fijadas en la media docena de documentos adoptados por el GT29 sobre BCR.
  - Constituye el documento que siguen las autoridades de protección de datos para comprobar la viabilidad y adecuación de cada BCR que es sometida a su autorización Documentos sobre BCR.

**Acuerdo alcanzado en septiembre y comunicado al GT 29 en octubre**

- **Supone una mejora del procedimiento de coordinación ya existente (WP 107).**
- **Contenido → Cuando una empresa solicite autorización para unas BCR ante una de las autoridades participantes (autoridad líder), la decisión de ésta será aceptada por las demás autoridades participantes afectadas por tener la empresa actividad en su territorio.**
- **El mecanismo es un compromiso político que:**
  - **no altera la necesidad de iniciar los respectivos procedimientos nacionales**
  - **no modifica la necesidad de que las BCR se ajusten a las especificidades de tales legislaciones.**
- **Grupo inicial formado por principales DPA europeas:**

- Francia	- Reino Unido	- Irlanda
- Alemania (Federal y estados)	- España	- Italia
- Holanda	- Luxemburgo	- Letonia
- **Posteriormente: Islandia, Chipre, Noruega, Eslovenia, Rep. Checa, Liechtenstein y Malta (Total 16 APD).**

Opinión adoptada 4.4.08 (WP 148)

[www.ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2008/wp148\\_es.pdf](http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_es.pdf)

- **Directiva de Protección de Datos se aplica a los tratamientos de datos personales por buscadores aun cuando sus empresas centrales estén fuera de Europa.**
- **Datos personales sólo se recogerán para finalidades legítimas y los datos que se recojan tienen que ser relevantes y no excesivos respecto a las finalidades a desarrollar**
- **Directiva de Retención de datos no se aplica a los buscadores.**
- **Los buscadores deben eliminar o anonimizar de una forma irreversible estos datos una vez que dejen de ser útiles para la finalidad para la que fueron recabados.**
- **El GT29 recomienda un periodo máximo de retención de 3 a 6 meses para los datos de los usuarios .**
- **Los buscadores de Internet deben proporcionar a los usuarios una información clara e inteligible sobre:**
  - **identidad y localización,**
  - **datos que intentan recoger, guardar o transmitir,**
  - **finalidad.**
- **Usuarios deben tener derecho a acceder, inspeccionar y corregir, de forma gratuita todos sus datos personales incluyendo perfiles e historial de búsqueda.**

## Documento de Trabajo 1/2008

([www.ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2008/wp147\\_en.pdf](http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf))

- **Directrices generales que deben seguir quienes tratan y manejan datos de menores para proteger su privacidad.**
- **Centrado en el ámbito escolar.**
- **Enumera y define los principios fundamentales aplicables en este ámbito:**
  - **generales (principio del interés superior del menor, reconocimiento del derecho a su intimidad, obligación de adaptación al grado de madurez del menor),**
  - **específicos derivados de la Directiva 95/46/CE.**
- **Aplica principios a situaciones concretas:**
  - **datos almacenados en los expedientes y ficheros escolares,**
  - **colocación de circuitos cerrados de televisión,**
  - **tratamiento de datos sensibles,**
  - **publicación de fotos de los estudiantes,**
  - **uso de videoteléfonos dentro de los colegios.**
- **Conclusión: disposiciones existentes garantizan eficazmente la protección de los datos de los niños, debiendo siempre aplicarse de conformidad con el principio nuclear del interés superior del niño.**
- **Pendiente de versión definitiva tras consulta pública.**

## Decisión Marco 2008/977/JAI 27-11-08

- **Objetivo: Cubrir parcialmente vacío de Directiva Protección de Datos (excluye datos que tengan por objeto seguridad pública y actividades del estado en materia penal), buscando alto nivel de protección en datos personales involucrados en cooperación policial y judicial.**
- **Se establece un régimen de principios y derechos de interesados paralelo al de la Directiva.**
- **Se regulan transferencias a estados, organizaciones e incluso particulares.**
- **Se prevén actividades de inspección y actuación por parte de agencias independientes.**

- **Modificación Decisión Cláusulas Contractuales (responsable – encargado).**
- **Estudio Redes Sociales.**
- **Inspección coordinada sobre aplicación Directiva 2006/24/CE de retención de datos (WP 152).**

Investigación desarrollada en todos los EEMM y dirigida a conocer las medidas de seguridad y el cumplimiento con los límites de conservación de datos.

- **Opinión sobre prácticas “pre-trial discovery”.**
- **PNR Europeo.**

# CONSULTAS DE LOS ASISTENTES

**JESÚS RUBÍ NAVARRETE**  
Adjunto al Director de la AEPD

¿Quién autoriza la publicación de una esquila de un difunto y, por tanto, los datos contenidos en ella?

- La LOPD no se aplica a los datos de personas fallecidas
- La publicación de datos en la esquila del difunto cuando la realizan personas físicas puede considerarse como un tratamiento de la información realizado en el marco de la vida privada o familiar de los particulares, al que tampoco se aplica la LOPD.

¿Qué criterio tiene la AEPD sobre la consideración como dato de carácter personal de los teléfonos móviles o las direcciones IP después de la SAN de 17 de septiembre de 2008 que señala que un número de teléfono móvil no es un dato personal si no puede asociarse a una persona identificada o identificable?

Las empresas que tienen páginas web y monitorizan las visitas tratando las IP's de sus usuarios: ¿cómo se recaban legalmente estos datos?, ¿basta un aviso legal en una página secundaria de la web?

- La AEPD, en aplicación de la LOPD, considerará la IP o el número de teléfono móvil como dato personal cuando pueda asociarse a una persona identificada o identificable (ver Dictamen 4/2007, de 20 de junio, del GT 29, sobre el concepto de dato personal. WP 136).

- **En la mayor parte de las ocasiones la legitimación para tratar las direcciones IP se basará, bien en el consentimiento informado (por ejemplo, usuarios registrados en la página web), bien en la relación jurídica en sentido amplio entre el titular de la web y el usuario de sus servicios (por ejemplo, usuarios no registrados de un buscador en Internet). En ambos casos el aviso legal puede no estar en la página principal siempre que sea identificable, fácilmente accesible y comprensible.**
- **Sin embargo deben tenerse en cuenta que tanto la LGT como la LSSI reconocen derechos y garantías específicos cuando se utiliza un número de móvil o se trata una dirección IP que son independientes del concepto de dato personal, siendo exigibles incluso cuando sus titulares son personas jurídicas.**

Cuando un médico utiliza el quirófano de un hospital privado para operar facilitándole el hospital servicios de anestesia y enfermería, entendemos que existen dos responsables de los datos distintos, ¿sería necesario el consentimiento del paciente para la cesión de sus datos por parte del médico con anterioridad a la operación para la reserva del quirófano y demás gestiones o estaría amparada en el artículo 11.2.c) LOPD?

- El tratamiento y cesión de datos de salud sólo puede ampararse en el consentimiento expreso del afectado o en una habilitación legal (art. 7.3 LOPD), y no en la existencia de una relación jurídica que implique necesariamente la conexión con ficheros a terceros.
- El tratamiento de los datos por parte del centro sanitario donde se va a realizar la intervención quirúrgica puede ampararse en el artículo 7.6 de LOPD (siempre que se realice para profesionales sanitarios sujetos al secreto profesional u otros con una obligación equivalente de secreto) y en el art.8 LOPD que legitima el tratamiento por las instituciones y centros sanitarios (públicos y privados) y los profesionales correspondientes, de los datos de las personas relativos a la salud que acudan a ellos o hayan de ser tratados en los mismos, de acuerdo con la legislación sanitaria.
- En el caso planteado, existirán dos responsables distintos.

¿Cómo debe recabar el consentimiento un autónomo para que sea válido en el caso de que en algún momento decida constituir una sociedad cuya actividad sea la misma y la finalidad del consentimiento también? ¿sería necesario recabar un nuevo consentimiento?

- Cuando hay una modificación del responsable del fichero como consecuencia de una reestructuración societaria, manteniéndose la misma actividad y los datos se utilizan para la misma finalidad, no es necesario un nuevo consentimiento. En tal caso basta con informar a las personas afectadas de los extremos contemplados en el artículo 5 LOPD.

¿Qué tipo de contrato o cláusula debería regular la relación contractual entre una empresa de trabajo temporal (ETT) y una empresa usuaria de sus servicios en relación a la LPOD?

- **La comunicación por la ETT de los datos de las personas vinculadas a ella al tercero usuario de sus servicios constituye una cesión que está legitimada por las relaciones jurídicas que la ETT mantiene con unos y otros.**
- **El tratamiento de los datos por parte de la tercera empresa, usuaria de los servicios de la ETT, se encuentra, también, legitimada por ser necesaria para el mantenimiento o cumplimiento de dicha relación jurídica. Por tanto, no es necesario un contrato de prestación de servicios con la ETT como encargado del tratamiento.**

¿Qué obligaciones respecto a la protección de datos tenemos las organizaciones de formación que damos a nuestros alumnos accesos temporales a contenidos, informes, etc... a través de un campus virtual, así como lo que damos a los formadores/tutores de los mismos, incluyendo datos de los estudiantes?

- **El tratamiento de datos por los formadores/tutores estaría legitimado por la relación jurídica establecida con los alumnos.**
- **El acceso a contenidos debería excluir los datos personales a terceros, salvo que el mismo estuviera legitimado conforme a las reglas generales de la LOPD y el RLOPD.**

**Guardar el resultado de un “macheo” de listas de clientes contra listas oficiales de terroristas, ¿va en contra de la LOPD? ¿Y guardar un listado de clientes sobre los que se solicita información por parte del juzgado para analizar operaciones sospechosas?**

- **La normativa que regula la prevención y bloqueo de la financiación del terrorismo (Ley 12/2003, de 21 de mayo) y la prevención del blanqueo de capitales (Ley 19/1993, de 28 de diciembre) imponen a las personas y entidades obligadas que enumeran, a examinar cualquier operación que pueda estar relacionada con la financiación de actividades terroristas o vinculada al blanqueo de capitales.**
- **Entre las obligaciones que impone a los sujetos obligados está la de conservar durante un periodo mínimo de 6 años los documentos acreditativos de las comprobaciones que deban realizar (RD.925/1995, de 9 de junio).**

**Por tanto, dicha conservación no va en contra de la LOPD al estar amparada legalmente en los dos casos planteados siempre que la información sea relevante para cumplir las obligaciones que le imponen las leyes citadas.**

**Corresponsabilidad de ficheros:** En el ámbito de la educación y entre los Departamentos o Consejerías de Educación de las Comunidades Autónomas y los centros docentes públicos, ¿se puede entender que existe una corresponsabilidad del art. 57 RLOPD, respecto del fichero de alumnos?

- **No es posible admitir la corresponsabilidad del fichero de alumnos conforme al art.57 RLOPD dado que uno de los aspectos básicos de la creación y registro de ficheros es la finalidad y las relacionadas con las competencias de la Consejería y las funciones del colegio no son coincidentes, ya que las primeras son más amplias.**
- **Sin embargo, se puede atribuir la responsabilidad de los ficheros a la Consejería o al colegio público. En el caso de ser necesaria una comunicación de datos esta sería legítima en el marco de sus competencias y funciones.**
- **En el caso de los centros privados concertados debe diferenciarse entre el fichero de la Consejería y el centro de enseñanza, ya que el hecho de ser concertado no altera la responsabilidad de uno y otro. Cabrían, no obstante cesiones de datos entre ambos que fueran proporcionadas a sus competencias y responsabilidades, respectivamente**

En el caso de que contractualmente el responsable del fichero no informe al encargado del tratamiento de los tipos de datos que va a tratar y, por tanto, no informe sobre las medidas de seguridad que deben implantarse, ¿implica que el encargado del tratamiento se exime de las responsabilidades porque desconoce estos datos, o debe solicitar al responsable del fichero esa información hasta que la obtenga?

- **La implantación de las medidas de seguridad exigibles es una obligación tanto del responsable del fichero como del encargado del tratamiento (art.79 RLOPD)**
- **El responsable del fichero tiene una obligación específica de diligencia en orden a estipular en el contrato de prestación de servicios las medidas de seguridad que debe implantar el encargado del tratamiento (art.12 LOPD y 20.2 RLOPD). Por ello el encargado debe solicitar al responsable la indicación de las medidas.**

- **Si, pese a ello, no las estipula y el encargado del tratamiento puede conocer la tipología de datos objeto de la prestación de servicios deberá implantar las medidas de seguridad exigibles, sin perjuicio de la responsabilidad de quien lo contrató y no las indicó.**
- **Si el conocimiento de toda la tipología de datos objeto de la prestación de servicios fuera desproporcionado y el responsable no responde a sus requerimientos podría limitar o excluir la responsabilidad remitiendo al responsable una comunicación sobre el nivel de medidas de seguridad que va a implantar con la información de que dispone.**

En entidades de recobro, ¿qué uso se puede hacer de la información facilitada por el cliente, relativa al impagado que hayan obtenido otras entidades de recobro contratadas anteriormente? Si un cobrador va a la dirección de un moroso que aparece en páginas blancas, ¿puede tomar del buzón la escalera, piso y letra de la casa para remitir la carta?

- Con carácter general, las empresas de recobro desarrollan su actividad como encargadas del tratamiento debiendo limitarse a tratar los datos personales facilitados por el acreedor que les contrató.
- Para la obtención de datos adicionales han de estar legitimados conforme a la LOPD (consentimiento, habilitación legal, relación comercial...) siendo lo más habitual que obtengan datos de fuentes accesibles al público, como son las guías telefónicas.
- La obtención de datos adicionales no está, en principio, amparada en la prestación de servicios de recobro por lo que la empresa que los obtenga tendrá la condición de responsable de su tratamiento.

- **En tal condición las anteriores empresas de recobro sólo podrán ceder datos a las que intervengan posteriormente si tienen legitimación para la cesión que, probablemente, sólo existirá cuando se hayan obtenido de fuentes accesibles al público.**
- **En las guías telefónicas no consta, salvo consentimiento del afectado la escalera, piso y letra de la casa por lo que estos datos, al no figurar en una fuente accesible al público no pueden ser tratados sin consentimiento (u otra legitimación específica)**

Los clientes han cancelado todos los contratos con la entidad pero no han manifestado su negativa a recibir comunicaciones comerciales. No han manifestado su consentimiento expreso pero sí el tácito para recibir publicidad puesto que en otras ocasiones, cuando eran clientes, han sido llamados por teléfono y nunca se han opuesto. ¿Se les puede realizar una llamada telefónica no automática con intervención humana para intentar como clientes?

- La regla general, (en aplicación de la LOPD) si se tratan datos personales asociados al número de teléfono, es que sólo pueden recibir publicidad si se ha obtenido un consentimiento informado para ello o los datos se obtienen de fuentes accesibles al público.
- La mera realización de llamadas mientras eran clientes, sin que se hayan opuesto a ellas, es insuficiente para considerar que se ha obtenido el consentimiento.

- **Las llamadas no automáticas sin intervención humana (es decir, a través de una operadora), si están asociadas a datos personales, deben cumplir la regla general descrita, ya que se aplica la LOPD. Además, antes de realizarlas deberán consultarse los ficheros de exclusión que puedan existir (“listas Robinson”, art. 49 LOPD)**
- **Conforme al artículo 69.2 del RSU (RD 424/2005) tampoco se podrán realizar este tipo de llamadas, incluso si no están asociadas a datos de personas físicas (llamadas aleatorias) o afectan a personas jurídicas, respecto de aquellas que no figuran en guías telefónicas o que, figurando, aparezcan marcadas con el signo “U”, que significa que no quieren recibir publicidad. Al margen de estos casos, si no se tratan datos personales protegidos por la LOPD, pueden realizarse las llamadas pero los ciudadanos tienen la posibilidad de oponerse a ellas.**
- **Sin embargo, si se realizan, no podrán sancionarse al no existir un tipo de infracción específico para la vulneración de las garantías recogidas en el artículo 69.2 del RSU.**

¿El artículo 49 del RLOPD obliga al responsable del fichero a identificar de forma concreta cuáles son los ficheros comunes de exclusión, o bastaría con señalar que tales ficheros constan inscritos en la AEPD y que pueden consultarlos? ¿El artículo 49 se refiere al supuesto en el que los datos del afectado provengan de una fuente accesible al público?

- **El responsable del fichero ante el que el afectado manifiesta su negativa u oposición a que sus datos se traten con fines de publicidad o prospección comercial, deberá informar sobre los ficheros comunes de exclusión con indicación del responsable, su domicilio y la finalidad del tratamiento.**
- **No cabe, por tanto, la mera remisión al RGPD ya que dichos responsables pueden conocer la existencia de ficheros de exclusión, aunque no estén inscritos en el RGPD (por ejemplo, por haberlos constituido una asociación de la que forman parte).**
- **En todo caso, la información del RGPD, que es accesible a terceros, puede ser útil para cumplir la obligación del informar.**
- **La obligación de consultar previamente los ficheros de exclusión es exigible en los casos en que los datos personales figuren en fuentes accesibles al público.**

De acuerdo con el artículo 49 RLOPD, ¿es necesario consultar los Ficheros comunes de exclusión comercial para la realización de campañas de publicidad sobre clientes propios de un responsable de fichero frente al que no hayan ejercitado esos clientes el derecho de oposición?

- Si dispone de un consentimiento específico para realizar publicidad a los clientes, en principio, no habría que consultar.
- Sin embargo, si existen ficheros comunes de exclusión para las personas que no quieran recibir, en absoluto, ninguna publicidad, deberían consultarse estos ficheros.

Tengo una página web con un formulario de petición de datos y/o una base de datos de usuarios. La empresa española con la que contrato el mantenimiento y alojamiento de la página decide alojarla en un “hosting web” en EEUU ¿cómo regularizo la situación si la tercera empresa no está adherida a Acuerdo de Puerto Seguro? ¿Debo declarar una transferencia internacional? ¿Debo pedir el consentimiento a los afectados?

- El alojamiento en EEUU constituye una transferencia internacional de datos a un encargado del tratamiento en dicho país.
- El consentimiento informado de los afectados exime de la obligación de solicitar a la AEPD una autorización de transferencia internacional de datos.
- Si no se ha obtenido el consentimiento es preciso que el responsable titular de la página web solicite autorización para la transferencia internacional, que puede obtenerse suscribiendo las cláusulas contractuales tipo previstas en la Decisión de la Comisión Europea, 2002/16/CE de 27 de Diciembre de 2001.
- Las cláusulas contractuales deben ser suscritas por el responsable, el encargado del tratamiento en España y la tercera empresa que presta sus servicios en EEUU.

Se ha obtenido una autorización para realizar una transferencia internacional de varios ficheros y para una serie de datos. Si posteriormente se decide suprimir esos ficheros por realizar una reorganización interna de los mismos e inscribirse un nuevo fichero que refunda los antiguos ¿cómo comunicar a la AEPD para que la autorización de transferencia internacional tenga efectos para el nuevo fichero?

- No puede darse una respuesta unívoca de carácter general pues depende de los términos de refundición de los ficheros, los sujetos intervinientes en la transferencia y las condiciones de la autorización.
- No obstante, cabe la posibilidad de admitirla. Por ejemplo: Un operador de telecomunicaciones pasa a ser responsable de los ficheros de clientes que ha adquirido de otros dos operadores como consecuencia de una operación de reestructuración societaria. Cada uno de ellos tenía autorizadas las TID a un encargado del tratamiento en países distintos. El operador quiere refundir los ficheros de clientes con un solo encargado de los preexistentes. Podría modificar un fichero de clientes incorporando los restantes y conservar la autorización de TID.

**Respecto de los documentos en soporte papel. ¿ Es necesario inventariar todos los documentos con datos de carácter personal que tenga el responsable del fichero o basta con inventariar los expedientes o carpetas en las que se encuentren archivados los documentos?**

- **Respecto de los ficheros no automatizados el RLOPD exige (art. 92 y 106):**
  - La identificación del tipo de información de los documentos.
  - Su inventario.
  - El archivo (que puede estar regulado o ser definido por el responsable) conforme a criterios que garanticen la conservación, localización y consulta, así como que posibiliten el ejercicio de derechos.

Estas obligaciones deben ponerse en relación con el tipo y finalidad del sistema de información y de los ficheros existentes.
- **Así, por ejemplo, en un registro de entrada y salida deberá inventariarse cada documento como unidad diferenciada (una solicitud de empleo y el currículum anexo sería un documento).**
- **Pero en un fichero de expedientes o procedimientos el inventario puede hacerse por carpetas o expedientes en los que se archivan los documentos (por ejemplo el expediente laboral de un empleado, o la historia clínica de un paciente).**

En el caso de una federación cuya finalidad es el asesoramiento a entidades que trabajan con personas discapacitadas para la consecución de ayudas o programas diseñados por la Administración Pública (Estatal, Autonómica o Local), en ocasiones, para la tramitación de las ayudas deben solicitarse y aportarse los certificados de discapacidad de los solicitantes. ¿El certificado estaría incluido en la excepción del artículo 81.6 del RLOPD (medidas de seguridad de nivel básico)?

- El tratamiento del certificado de discapacidad, si se limita a incluir el grado de discapacidad o la declaración de la misma o de la invalidez, para la obtención de las ayudas citadas, puede considerarse como realizado “con motivo del cumplimiento de deberes públicos”, siendo exigible la implantación de medidas de seguridad de nivel básico.

**La herramienta de trabajo de los medios de comunicación es la información ¿Qué medidas de seguridad han de implantar los medios de comunicación audiovisuales para cumplir la LOPD?**

- **El nivel de seguridad (básico, medio o alto) depende de la naturaleza de los datos que se traten conforme al artículo 81 del RLOPD.**
- **Los medios de comunicación (audiovisuales o no) tratan con frecuencia informaciones relacionadas con la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual de las personas, en cuyo caso sería exigible implantar, además de las medidas de seguridad de nivel básico y medio, las de nivel alto.**



# AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

