CUADERNOS AUTELSI DE REGULACIÓN

Cuaderno nº 1

LA PROTECCIÓN DE DATOS PERSONALES

Novedades del derecho dictado sobre esta materia.

Octubre 2007

Oscar López

Socio Director de
Urbetec Abogados y Consultores

Vocal Portavoz GRA
Área Sociedad de la Información

Informes realizados por los miembros
del Grupo de Regulación de AUTELSI (GRA)
sobre el marco legislativo aplicable a Telecomunicaciones,
Sociedad de la Información y Audiovisual

autelsi
Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información

INDICE

PRESENTACIÓN

La Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (Autelsi) es una entidad de ámbito nacional, sin ánimo de lucro, que representa a los usuarios profesionales de las telecomunicaciones y de las tecnologías de la información. Es el resultado de la ampliación, en junio de 2003, del ámbito de actuación de Autel, constituida en Barcelona el 24 de julio de 1987 e inscrita en el Registro de Asociaciones del Ministerio del Interior con el número 75.713, como portavoz de los usuarios profesionales de las telecomunicaciones. En 1989, trasladó su domicilio social a Madrid.

La Asociación tiene como objeto el promover, en la sociedad en general y entre los usuarios profesionales en particular, el estudio, la investigación y la difusión objetiva de conocimientos en los temas relacionados con los servicios de telecomunicaciones y de la Sociedad de la Información

Autelsi desarrolla su labor a través de Comisiones y Grupos de Trabajo que cubren el espectro temático de mayor interés para el sector empresarial en el campo de las Tecnologías de la Información y las Comunicaciones (TIC). Estos grupos, constituidos por representantes de las Administraciones y de las empresas –fabricantes, proveedoras y usuarias de productos y servicios TIC– más importantes del país, conforman el núcleo de actividad de la Asociación y constituyen una red de conocimiento inigualable en el tejido empresarial nacional.

Las Comisiones y Grupos de Trabajo llevan a cabo una amplia gama de actividades que incluyen constitución de foros de encuentro y centros de debate, generación de capital intelectual y creación de opinión; prestación de cooperación y servicios a los usuarios y entre las acciones de difusión que desarrollan se pueden enumerar:

- Elaboración de estudios y documentos sobre aquellos temas relevantes en el mundo de las telecomunicaciones y sistemas de Información.
- Edición de publicaciones u ofertas de servicios a la sociedad en general, derivados de las actividades realizadas por algún Grupo de Trabajo/Comisión.
- Desarrollo de un portal de Internet que albergue, entre otros, un *repository* de capital intelectual.

Todas estas actividades se acompañan de planes de comunicación que habilitan la difusión de las mismas en el tejido empresarial nacional y, en general, en la sociedad española.

Concretamente el **Grupo de Regulación Autelsi**, en adelante **GRA**, lo integran los principales despachos de abogados y las áreas jurídicas de las empresas más dinámicas del Sector. El GRA, dirige sus esfuerzos al ámbito legal y normativa en el ámbito de las TIC y, más concretamente a:

- Trasladar la postura de Autelsi sobre las principales cuestiones de regulación del sector de las comunicaciones electrónicas y de la sociedad de la información, con el fin de hacerla llegar a la Administración o la opinión pública en general.
- Prestar apoyo a los representantes de la Asociación en la Comisión Permanente del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.
- Análisis práctico de cuestiones de regulación del sector de las comunicaciones electrónicas y de la sociedad de la información, teniéndose en cuenta no sólo las iniciativas de regulación sino también su aplicación o las que deberían adoptarse atendiendo a las necesidades de tales sectores.

- Integrarse o colaborar en los trabajos que estén realizando otras Comisiones o Grupos de Trabajo dentro de la Asociación, aportando la visión desde la perspectiva reguladora.

Con la publicación de la Colección "Cuadernos Autelsi de Regulación", la Asociación quiere divulgar y abordar el estudio de temas de gran actualidad e interés en las tres áreas en que se divide el GRA: Telecomunicaciones, Sociedad de la Información y Audiovisual. Por ello los cuadernos tienen un objetivo fundamentalmente informativo y sus contenidos reflejan la opinión de sus autores. Aunque constituyen herramientas de trabajo del GRA, éste no se identifica con dichas opiniones. De hecho, para profundizar en el análisis de algunos temas, pueden existir planteamientos divergentes que respondan a puntos de vista diferentes.

El presente cuaderno, dedicado a LA PROTECCIÓN DE DATOS PERSONALES ha sido elaborado por Oscar López, abogado y Socio Director del Despacho Urbetec Abogados y Consultores, y Vocal Portavoz del área de Sociedad de la Información del GRA.

Oscar López es Licenciado en Derecho por la Universidad Complutense de Madrid, con especialización en Tecnologías de la Información. Doctorando en Filosofía del Derecho. Miembro del Colegio de Abogados de Madrid.

Atesora mas de nueve años de experiencia en asesoramiento, defensa jurídica y consultoría en Tecnologías de la Información y la Comunicación, siendo desde, el año 2.002, profesor en los cursos de formación impartidos por AENOR en materia de Gestión de la seguridad y derecho de las Tecnologías de la Información (Análisis de riesgos jurídicos asociados a la información y aplicación práctica de la LOPD).Ha impartido cursos de formación personalizados en esta materia a importantes compañías y Organismo Públicos como Repsol, Iberia, Grupo PSA, Universidad Complutense de Madrid y la *Consellería* de Telecomunicaciones de la *Generalitat* Valenciana.

En la actualidad es socio Director del bufete Urbetec Abogados y Consultores, despacho de abogados especializado en Tecnologías de la Información y las Comunicaciones (TIC). Urbetec ofrece servicios de asesoramiento, defensa jurídica y consultoría legal en el ámbito de las tecnologías de la información y su marco jurídico en continúa evolución.

En nombre de la Asociación y muy especialmente del GRA, agradezco muy sinceramente la desinteresada colaboración de Oscar, y de su empresa, para la edición de este primer cuaderno de la colección.

César Rico
Presidente del GRA

RESUMEN EJECUTIVO

El presente número de la Colección "Cuadernos Autelsi de Regulación", editado por la Asociación y cuyo contenido ha sido elaborado por el abogado Oscar López, del despacho Urbetec Abogados y Consultores, en el seno del GRA (Grupo de Regulación Autelsi), tiene por objeto actualizar la información sobre las disposiciones en materia de protección de datos de carácter personal, como son la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), su desarrollo reglamentario (Real Decreto 994/1999 de 11 de junio), y el futuro Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y demás normativa aplicable al efecto, así como analizar el conjunto de novedades relacionadas con el tema, dictadas en los últimos meses.

El tema es del máximo interés para las entidades asociadas a Autelsi porque el desarrollo e implantación de las Tecnologías de la Información (TIC) ha motivado que las mismas estén presentes en la práctica totalidad de las actividades económicas y empresariales, interviniendo inevitablemente en la configuración de las relaciones que mantienen las empresas entre sí y con los particulares, lo que a su vez origina y plantea nuevos retos legales, encaminados a proporcionar una mayor protección de los derechos e intereses de los ciudadanos.

El cuaderno se ha estructurado en tres capítulos: en el primero se analizan las medidas reguladoras de carácter general en materia de protección de datos personales, tanto comunitarias como del marco legislativo aplicable en España; el segundo, breve pero específico para el sector de las telecomunicaciones, describe las obligaciones actuales, tanto de los Prestadores de servicios de la SI como de los Operadores de redes y servicios. El tercero, que representa más de las dos terceras partes del cuaderno, recoge las principales novedades y aportaciones normativas en el ámbito de la protección de datos de carácter personal, producidas en el período 2006-2007, en el marco legislativo español y en el de la Unión Europea.

Hay que recordar que una de las primeras preocupaciones fue la necesidad de garantizar y proteger la privacidad e intimidad de las personas, dando lugar a lo que se conoce como Protección de Datos de Carácter Personal, ámbito que cobra especial relevancia debido a que los avances experimentados en los últimos años (principalmente de tipo técnico) ponen a disposición de empresas y usuarios instrumentos, medios y herramientas, cada vez más sofisticados, que permiten, no sólo acceder a los datos de carácter personal, sino hacer uso de los mismos para finalidades que los ciudadanos, titulares de los datos, pueden desconocer, derivándose de ello un importante riesgo para la intimidad. Muchos de estos tratamientos están caracterizados por ser automatizados, si bien también son de relevancia los no automatizados.

La respuesta del legislador frente a dicha problemática consistió en la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, conocida como LORTAD. Esta ley fue derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, conocida como LOPD y que viene a constituir la principal norma reguladora de la Protección de Datos de Carácter Personal en España, y que constituye el punto de partida del análisis del capitulo primero.

Concretamente, la citada Ley Orgánica 15/1999 tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, estableciendo una serie de obligaciones en aras a la protección de los datos personales contenidos en ficheros automatizados que poseen empresas y administraciones públicas, y que son tratadas por éstas con diferentes finalidades; gestión de personal, proveedores, clientes, campañas de marketing, etc. En ella expresamente se recoge como obligados a su cumplimiento, las personas físicas y jurídicas, que en el marco de sus actividades traten datos de carácter personal (personas físicas identificadas o identificables) registrados en cualquier tipo de soporte físico (manual o informático). Cuando una empresa decide recabar datos de carácter personal debe, para poder utilizarlos, contar con el consentimiento de la persona que los cede. Ello supone que el consentimiento del afectado deberá ser precedido por una declaración del Responsable del Fichero (la empresa que los recaba) en la que se indiquen, de forma clara y fácilmente comprensible, los datos que van a ser objeto de tratamiento y las finalidades a que van a ser destinados, para que los interesados indiquen, sin ningún género de dudas, su conformidad con su tratamiento o su oposición al mismo. No obstante, hay una serie de excepciones y de determinadas materias que se rigen por disposiciones específicas, que es necesario conocer y que se especifican en el texto.

Entre las novedades relativas al período 2006-3007 analizadas en el capitulo tercero, destaca el análisis que se hace del futuro Nuevo Reglamento de desarrollo de la LOPD, todavía en tramitación, y que sustituirá al Reglamento de Medidas de Seguridad (RD 994/1999). Hay que tener en cuenta que la Información Corporativa (información relativa a los productos, servicios, clientes, proveedores, personal, método de trabajo, organización, estrategias empresariales, información económica y financiera, etc...) se considera como uno de los principales activos de negocio de cualquier empresa, y como tal, debe ser protegida adecuadamente con medios técnicos y legales, de forma que se evite, en la medida de lo posible, que cualquier persona física o jurídica pueda acceder/obtener/tratar/difundir la misma, fraudulenta o ilícitamente, causando perjuicios más o menos graves a su titular, por lo que es imprescindible conocer las medidas de carácter técnico u organizativo a adoptar / implementar por la empresa o profesional que los almacene para garantizar la seguridad de los datos de carácter personal.

Sin embargo, se da la circunstancia de que aún son muchas las empresas que hoy en día desconocen sus obligaciones frente a los titulares de los datos personales que manejan, resultando imprescindible estar perfectamente asesoradas, con el objeto de cumplir y respetar la normativa, aportando todo ello un valor añadido y ofreciendo mayores garantías al consumidor, usuario o cliente que acude a ellas en busca de productos o servicios; y al mismo tiempo, los consumidores, usuarios o clientes deben contar con un nivel de información que les permita conocer sus derechos frente a quienes recogen y poseen sus datos y poder ejercitarlos, de modo que su intimidad no resulte afectada por el uso de esos datos. Por todo ello, la información que se suministra en el presente Cuaderno puede ser de enorme utilidad para muchas empresas.

Verónica Fernández
Secretaria del GRA

LA PROTECCIÓN DE DATOS PERSONALES
Novedades del derecho dictado sobre esta materia

1. LA REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES. ÁMBITO GENERAL.

El tratamiento de datos personales en la Ley Orgánica 15/1999 (LOPD)

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece un marco armonizado en relación con la protección y el tratamiento de los datos personales susceptibles de automatización, persiguiendo que los sistemas de tratamiento de datos estén al servicio del hombre y se alcance la protección de los derechos fundamentales de las personas.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), incardina al Ordenamiento jurídico español la anterior Directiva comunitaria, siendo en la actualidad la norma básica de referencia en España en relación con la protección del derecho fundamental a la protección de datos personales. Esta ley y el resto de normativa reglamentaria vigente, regulan las obligaciones de empresas y administraciones públicas en el tratamiento de datos personales en sus ficheros.

La LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar y se aplica a los tratamiento de datos personales y ficheros, tanto públicos como privados, que contengan datos de carácter personal.

No obstante, el régimen de protección de los datos de carácter personal que se establece en la LOPD 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 de Protección de Datos

Además, determinadas materias se regirán por sus disposiciones propias:

- **Régimen electoral**:

  Ley Orgánica 5/85 de 19 de junio

  Ley Orgánica 13/94 de 30 de marzo, que modifica a la anterior.

- Los datos que sirvan exclusivamente para fines estadísticos amparados por la ley 12/89 de 9 de mayo de la **Función Estadística Pública o legislación autonómica**.

- Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del **Régimen del personal de las Fuerzas Armadas.**
- **Registro Central de Penados y Rebeldes**
- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Obligaciones establecidas en la Ley

La LOPD establece una serie de obligaciones para aquellas empresas y organismos públicos o privados que gestionan ficheros organizados[1] y automatizados de datos personales[2] con diferentes finalidades (gestión de personal, gestión de clientes o proveedores, campañas comerciales o de marketing, seguridad y control de accesos,… etc)

Las obligaciones básicas impuestas por la LOPD a los responsables de los ficheros[3] se pueden resumir en:

Exigencia de Legalidad y legitimidad en los Tratamientos de datos[4]. (art. 4 LOPD). Prohibición de recogida de datos por medios fraudulentos, desleales o ilícitos.

Cumplimiento de una serie de principios básicos

- Calidad de los datos (Art. 4 LOPD) que hace referencia a que los datos recogidos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido. Explícitamente este precepto establece que los datos personales:
  - No podrán usarse para finalidades incompatibles con aquellas para las que fueron recogidos.
  - Deberán ser exactos y puestos al día, respondiendo con veracidad a la situación actual del afectado o interesado.
  - Si no son exactos o están incompletos deben ser cancelados o sustituidos por los correctos.
  - Serán cancelados cuando dejen de ser necesarios.
  - No podrán ser conservados (salvo en el caso en que se decida su mantenimiento por valores históricos, científicos o estadísticos) una vez que dejen de ser útiles para la función prevista, con excepción de los plazos de prescripción que determine la legislación específica prevista al efecto (Obligaciones fiscales, Seguridad social, Seguros...).

[1] Fichero (art. 3 letra b): Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
[2] Dato personal (art. 3 letra a): Cualquier información concerniente a personas físicas identificadas o identificables.
[3] Responsable del fichero o tratamiento (art. 3 letra d): Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
[4] Tratamiento de datos (art. 3 letra c): Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- También recoge la exigencia de información previa (Art. 5 LOPD) clara, precisa y comprensible acerca de la finalidad (o finalidades) a la que van a ser destinados los datos personales objeto de tratamiento, con el fin de que los afectados manifiesten su conformidad o su oposición al mismo.
- Determina la exigencia de recabar el consentimiento informado para el tratamiento de los datos tácito, expreso o por escrito (Art. 6 y 7 LOPD) entendida como la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de los datos personales que le son recabados.
  - La ley exige el consentimiento expreso para recabar, tratar o ceder los datos que hagan referencia al origen racial, a la salud y a la vida sexual.
  - También exige la ley el consentimiento expreso y por escrito del afectado cuando puedan ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. En relación con el tratamiento de estos datos, existe una obligación de advertir al interesado su derecho a no prestar su consentimiento y la prohibición de crear o mantener ficheros con la finalidad exclusiva de almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico y vida sexual.
  - Este consentimiento podrá ser revocado en cualquier momento por causa justificada, pero no se le podrán atribuir efectos retroactivos a la revocación.

  No obstante la ley faculta a las organizaciones a tratar datos personales sin obtener el consentimiento previo de interesado cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento tenga por finalidad proteger un interés vital del interesado o cuando los datos figuren en fuentes accesibles al público ... (art. 6.2 LOPD)
- Respecto a la cesión [5] o comunicación a terceros de los datos personales (art. 11 LOPD) tratados por el responsable, la LOPD exige tener en cuenta las precauciones a adoptar porque exige el consentimiento previo del afectado, salvo excepciones como, entre otras, que la cesión esté autorizada en una Ley, que los datos tratados hayan sido recogidos de fuentes accesibles al público o 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. No obstante lo anterior, el consentimiento será nulo cuando no conste la finalidad a la que se destinarán los datos o el tipo de actividad de aquel a quien se pretendan comunicar o si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en anteriormente.

  También exige la ley (art. 12 LOPD) definir en un contrato una serie de obligaciones y responsabilidades cuando un tercero (Encargado de tratamiento[6]) necesita acceder y tratar los

[5] Cesión o comunicación de datos (art. 3 letra i): Toda revelación de datos realizada a una persona distinta del interesado.

[6] Encargado del tratamiento (Art. 3 letra g): La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

datos personales gestionados por el responsable porque va llevar a cabo una prestación de servicios por cuenta de él.

- En caso de transferencias internacionales (arts. 33 y 34 de la LOPD) o comunicación de datos personales a países que no proporcionen un nivel de protección equiparable al nuestro, la ley exige como regla general la obtención de la autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. También permite la ley una serie de excepciones ante esta obligación de autorización previa, de las que podemos destacar las siguientes:
    - Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
    - Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea.
    - Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
    - Cuando la transferencia sea necesaria para la ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- La ley recoge expresamente la exigencia del "deber de secreto" (art. 10) cuyo deber afectará y será exigible al responsable del fichero y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del fichero.

Derechos que asisten a los afectados

La Ley instaura una serie de derechos que el responsable deberá facilitar su ejercicio. Los derechos que asisten a los afectados, y que podemos destacar, son los siguientes:

- Derecho de Acceso (art. 15 de la LOPD, arts. 12 y 13 del R.D. 1332/94, normas 1ª y 2ª de la Instrucción 1/1998 de la Agencia), que es la facultad o capacidad que se reconoce al afectado de recabar información de sus datos de carácter personal sometidos a tratamiento, el origen de los mismos y las cesiones o comunicaciones realizadas o que se prevean realizar.

  El responsable resolverá la petición de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud y si la contestación fuera estimatoria el acceso se hará efectivo en el plazo de diez días. Si se incumple esta obligación, el afectado podrá interponer la reclamación oportuna, o, en su caso, la denuncia ante la Agencia Española de Protección de Datos (AEPD)

- Derechos de Rectificación y Cancelación (art. 16 de la LOPD y art. 15 del R.D. 1332/94, normas 1ª y 3ª de la Instrucción 1/98 de la Agencia), que es la facultad o capacidad del afectado por la que puede instar al responsable del fichero a cumplir con la obligación de mantener la exactitud de los datos, rectificando o cancelando los datos de carácter personal cuando resulten incompletos o inexactos, o bien sean inadecuados o excesivos, en su caso, o cuyo tratamiento no se ajuste a la Ley. Cuando los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable deberá notificar la rectificación y cancelación efectuada al cesionario. No obstante lo anterior, los datos de carácter personal deberán ser conservados

durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado, hasta alcanzado su plazo de prescripción.

El responsable hará efectivo el derecho de rectificación y/o cancelación dentro de los diez días siguientes al de la recepción de la solicitud.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Todos estos derechos a los que se ha hecho referencia tienen un carácter personalísimo, por lo que sólo pueden ejercerse por parte del afectado. Podrá no obstante actuar su representante legal cuando el afectado se encuentre en situación de minoría de edad o esté declarado incapaz para el ejercicio de sus derechos.

- Por último, y como nota destacable, en el artículo 9 de la LOPD, se exige el establecimiento de las medidas de seguridad índole técnicas y organizativas necesarias para salvaguardar la seguridad de los datos personales, para lo que el legislador español ha desarrollado un Reglamento[7] de medidas de seguridad (RMS) aplicable a los tratamientos de datos personales, diferenciando distintos niveles según el tipo de dato personal que se trata, atendiendo a su grado de sensibilidad desde el punto de vista de la intimidad de la persona.

  Las medidas exigidas por el Reglamento pueden ser de carácter técnico, porque se instrumentan dentro de los propios sistemas con la misión de proteger los datos y recursos de los mismos frente a las amenazas externas (interceptación de datos, la interrupción de los sistemas, la modificación o incluso la generación de información por terceros), de carácter organizativo porque persiguen la gestión en las organizaciones de la seguridad de la información e incluso de carácter físicas porque su implantación es fuera de los sistemas con el fin de proteger los mismos amenazas externas.

Reglamento de Medidas de Seguridad (RMS)

En síntesis, el RMS reconoce las siguientes medidas de seguridad:

Identificación y autenticación de usuarios: Es la verificación fehaciente de que el usuario que pretende acceder al sistema o aplicación donde reside la información es quién dice ser y está legitimado por la organización para trabajar en él (tradicionalmente mediante la utilización del sistema de usuario y contraseña, o incluso mas sofisticados, como la utilización de sistemas de control biométricos).

- El responsable de seguridad mantendrá una relación actualizada de usuarios con indicación de los derechos de acceso de cada uno
- El responsable de seguridad establecerá procedimientos de identificación y autenticación
- Si la autenticación se basa en contraseñas, éstas se asignarán, distribuirán y almacenarán de modo que se garantice su confidencialidad e integridad

[7] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan Datos de Carácter Personal.

- Si la autenticación se basa en contraseñas, éstas se cambiarán periódicamente (según se indique en el documento de seguridad) y durante su vigencia se almacenarán de forma ininteligible
- La identificación de los usuarios será inequívoca y personal
- Se limitará el número de intentos de acceso

Control de acceso: Es la medida que permite o denegar un cierto tipo de acceso a un recurso determinado, en función de la identificación fehacientemente comprobada por el mecanismo de autenticación, lo que permite a la Organización controlar quien, como y cuando se accede a la información por parte de quien este legitimado a hacerlo, y solo exclusivamente a aquellos datos y recursos que el usuario precise para el desarrollo de las tareas encomendadas. Esta medida exigirá previamente definir privilegios de acceso en relación con cada uno de los usuarios de los sistemas (según el artículo 12.4 del RMS, sólo el personal habilitado en el documento de seguridad podrá modificar estos derechos de acceso)

- Los usuarios podrán acceder sólo a los datos y recursos que precisen inexcusablemente para realizar sus cometidos (mínimo conocimiento)
- Existirán mecanismos para impedir el acceso a datos y recursos por parte de usuarios no habilitados para ello
- Sólo el personal relacionado en el Documento de seguridad podrá alterar los derechos de acceso de los usuarios, y siempre de acuerdo con lo establecido por el responsable del fichero

Cifrado de datos: Esta medida persigue conseguir la confidencialidad e integridad de los datos.

- La distribución de soportes se realizará previo cifrado de los datos
- La transmisión a través de redes de telecomunicación se realizará previo cifrado de los datos

Registro de accesos: Mediante esta medida, se anotan las acciones realizadas sobre el sistema, alertando, además, caso de que algunas de éstas supongan una violación real o potencial de la seguridad.

- Se registrará la identificación del usuario, fecha y hora, el fichero accedido, el tipo de acceso y si se ha autorizado o denegado
- Si el acceso se ha concedido, se almacenará la identificación del registro
- Los anteriores datos del acceso se almacenarán durante un mínimo de dos años
- El registro de accesos estará directamente controlado por el responsable de seguridad, que no los desactivará en ningún caso
- El responsable de seguridad revisará periódicamente la información registrada, emitiendo un informe de ello y los problemas hallados

Registro de incidencias: Esta medida exige establecer y documentar un procedimiento para notificar, gestionar y establecer mecanismos de respuesta ante las incidencias que se puedan generar en las empresas en relación con las medidas de seguridad adoptadas, permitiendo hacer un seguimiento de la misma, los efectos derivados y las medidas adoptadas para su resolución. El registro de incidencias deberá incluir:

- Tipo y hora de la incidencia
- Quién la notificó y a quién

- Procedimientos de recuperación, responsable y datos restaurados
- Autorización escrita del responsable del fichero para la recuperación

Copias de respaldo y recuperación: Esta medida exige formalizar y documentar el procedimiento de copias de respaldo (*Backups*) que prácticamente todas las empresas ya deben tener, pero que se caracterizará porque esta copia posibilite la recuperación de los datos en caso de pérdida. En el caso del proceso para llevar a cabo la recuperación, esta medida exige perseguir que, en caso de pérdida o destrucción de datos, el procedimiento nos debe permitir obtener como resultado la misma información que teníamos antes de generarse la contingencia. Esta medida se caracteriza por exigir:

- Reconstrucción de los datos al estado en que se hallaban
- Realización, al menos, semanal
- Almacenamiento en locales diferentes a aquellos en los que se tratan.

Pruebas con datos reales: Esta medida persigue evitar riesgos innecesarios que vulneren nuestro sistema de seguridad, al prohibir hacer uso de datos reales en las pruebas de desarrollo de programas informáticos. Para ello, sería fácil establecer en la empresa un mecanismo para disociar los datos reales, haciendo imposible acceder a ellos a través de la información resultante. Por lo que tendrá que tenerse en cuenta lo siguiente:

- Las pruebas de los programas no se realizarán con datos reales

Auditorias de seguridad: Esta medida exige a la empresa a llevar a cabo periódicamente una auditoría de control, de revisión del grado de adecuación de las medidas de seguridad implantadas, teniendo en cuenta el resto de las medidas exigidas en el Reglamento. Esta obligación determina que la empresa deberá contratar a algún auditor externo, a menos que tenga un grupo de trabajo interno e independiente, que permita revisar y examinar los tratamientos de información llevados a cabo por la empresa y las medidas implantadas para salvaguardar su seguridad, con el fin de garantizar el cumplimiento de la norma, detectar problemas de seguridad y recomendar cambios y medidas para el cumplimiento adecuado del Reglamento. Cabe destacar que esta medida exigirá:

- Realización bienal con dictamen de la adecuación de las medidas al Reglamento
- A disposición de la Agencia de Protección de Datos

Gestión de soportes: Esta medida exige que se lleve a cabo un control de los diferentes soportes que almacenan datos personales, en relación con cada uno de los tratamientos de información que gestiona la empresa. El art. 2.10 del Reglamento define soporte como “Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos”. Estos soportes hoy en día pueden ser de muy diversas clases (cintas, disquetes, dispositivos de usb) y la forma de distribuirse o “transmitir” su contenido se ha generalizado en el intercambio por medio de redes de telecomunicaciones, lo que hace muy complicado el control de esta medida. No obstante, en relación con esta medida, deben tenerse en cuenta estos aspectos:

- Deben estar inventariados, identificado el tipo de información y almacenados en locales controlados
- Sistema de registro de entrada (salida) con indicación del tipo de soporte e información que contiene, fecha y hora, emisor (destinatario), forma de remisión y responsable de recepción (entrega)
- Borrado de residuos
- Salida de soportes para operaciones de mantenimiento

Documento de seguridad: Esta medida obliga a la empresa a elaborar e implantar el resto de las medidas de seguridad que se adopten, mediante un documento (escrito o electrónico) que será de obligado cumplimiento para el personal que tenga acceso a los datos personales automatizados y a los sistemas de información y el cual exige, por el lógico cambio que puedan sufrir las medidas adoptadas, a una continua actualización. Esta medida caracteriza y debe incluir, al menos, los siguientes aspectos:

- Competencia del responsable del fichero
- Ámbito de aplicación
- Funciones y obligaciones del personal
- Estructura de los ficheros y sistemas de información
- Procedimientos de incidencias
- Ídem de copias de seguridad
- Identificación del responsable de seguridad
- Controles de cumplimiento
- Desecho de soportes

2.- PPROTECCIÓN DE DATOS EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS

Introducción

Tanto la **Directiva 95/46/CE** del Parlamento Europeo y del Consejo relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos como la **Directiva 97/66/EC** relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones, exigían como obligación de los estados miembros la protección del secreto de las comunicaciones por medio de normativas nacionales que garanticen la confidencialidad de las comunicaciones efectuadas a través de redes públicas de telecomunicaciones o de servicios de telecomunicaciones accesibles al público.

Por otro lado, la **Directiva 2000/31/CE**, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular el comercio electrónico en el mercado interior, recoge importantes disposiciones relativas a las obligaciones de los prestadores de servicios de la sociedad de la información en materia de privacidad, y a las medidas adoptables con relación al comercio electrónico (Directiva sobre el comercio electrónico)

El 12 de julio de 2002 se aprobó la **Directiva 2002/58/CE** del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada por la **Directiva 2006/24/CE** del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE

Nuestro marco legal de referencia, por haber llevado a cabo la transposición de la anteriores Directivas esta constituido por **La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)** y **la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT)**, que aborda una serie de temas, más o menos delicados, como la conservación de los datos de las conexiones electrónicas con fines de seguridad y vigilancia policial (retención de datos), el envío de mensajes electrónicos no solicitados (*spam*), el uso de «chivatos» (*cookies*) o la inclusión de datos personales en las guías públicas. Mediante está ley, los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la legislación vigente.

En efecto, el principal ámbito de protección de la privacidad electrónica gira en torno a la explotación de redes, prestación de servicios de comunicaciones electrónicas y los que se encuentran bajo la influencia del régimen jurídico de los servicios de la sociedad de la información (prestación de servicios de intermediación).

Desde tal perspectiva de transmisión de datos, la obligaciones reguladas en la LSSI y en la LGT, serán por tanto exigibles a todas aquellos empresas y organismos que, en el ejercicio de sus actividades, traten datos de carácter personal habilitando los medios necesarios para su transmisión y comunicación a través de las redes de telecomunicación, incluido Internet. Así, ya se trate de operadores que explotan redes públicas de comunicaciones electrónicas, proveedores de acceso a las mismas o prestadores de otros servicios de comunicaciones electrónicas disponibles al público distintos de la provisión de

acceso, lo cierto es que todos los operadores de telecomunicaciones y Prestadores de servicios de la sociedad de la Información, deben velar por la privacidad electrónica.

Obligaciones de los Prestadores de Servicios de la Sociedad de la Información

La LSSI y la LGT establecen una serie de obligaciones, que se pueden resumir en los siguientes puntos:

Obligaciones de los Prestadores de Servicios de la Sociedad de la Información

- Retención de los datos de navegación (Art. 12 LSSI art. 38.5 de la LGT). Este deber de retención de los datos de tráfico afecta en concreto a determinados prestadores intermediarios, por estar directamente vinculados a ellos los rastros o itinerarios electrónicos que dejan los usuarios a través de la Red (operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos) porque precisan contar con dichos datos de navegación para la prestación de sus servicios de intermediación, es a ellos a quienes compete la obligación de su retención, por ser justamente los sujetos con acceso directo a los mismos. La ley exige a los operadores y proveedores de acceso que conserven únicamente aquellos datos que sean necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información y a los prestadores de servicios de alojamiento de datos, los imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio, por un período máximo de doce meses en cualquiera de los supuestos. No obstante esta obligación en relación con el plazo de tiempo de retención esta pendiente de definición y desarrollo reglamentario.

- Dispositivos de almacenamiento y recuperación de datos en equipos terminales *(*art. 22.2 LSSI, en la redacción dada por la disposición final primera de la LGT). Si el Prestador de Servicios emplea dispositivos de almacenamiento y recuperación de datos en equipos terminales para la captación y tratamiento de datos vía *cookies* y otras técnicas afines de acceso y rastreo de información en el terminal del usuario, exige la obligación de informar a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

- El correo electrónico comercial (arts. 20 a 22.1 de la LSSI, según la redacción dada por la disposición final primera de la LGT).

La ley exige a los Prestadores de Servicios, con la finalidad de regular el *spam*, en el contexto de los servicios de la sociedad de la información, la obligación de recabar el consentimiento expreso y previo para el envío de comunicaciones comerciales[8] o mensajes de datos a terminales fijos o móviles con tales fines (SMS/MMS).

Este consentimiento expreso podrá revocarse en cualquier momento a través de un procedimiento sencillo y gratuito que deberá ser facilitado por el prestador de servicios, bajo el deber de informar sobre el mismo. No obstante la ley faculta al prestador a realizar esta actividad de envío de comunicaciones comerciales sin consentimiento del destinatario si previamente existe una relación contractual entre ambos pero siempre condicionada a que el prestador obtenga de forma lícita los datos de contacto del cliente y los emplee para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa y de características similares.

[8] Comunicación comercial»: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional".

También exige al prestador que las comunicaciones comerciales realizadas por vía electrónica sean claramente identificables como tales e indiquen la persona física o jurídica en nombre de la cual se realizan, y en el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra publicidad.

Las obligaciones recogidas en este apartado completan la obligación recogida en la LGT en relación con la protección del abonado frente a las llamadas automáticas y mensajes de fax con fines de venta directa.

Obligaciones de los Operadores de redes y servicios de comunicaciones, recogidas en la LGT

Las requisitos sobre protección de datos e intimidad establecidos en la LGT se detallan a continuación, atendiendo al ámbito de protección:

- Seguridad y secreto de las comunicaciones (arts. 33 a 36 de la LGT), Esta ley exige a los operadores la responsabilidad de la seguridad, seguridad de las redes y servicios y la confidencialidad en las comunicaciones electrónicas, de la información transmitida, incluidos los datos sobre tráfico, con la obligación de informar a los abonados sobre cualquier riesgo residual, recomendando la aplicación de tecnologías de cifrado como instrumentos de seguridad.

- Datos de tráfico, localización y opciones de facturación (art. 38.3 a 38.5 LGT). La ley exige a los operadores la obligación de facilitar el ejercicio del derecho de los abonados y usuarios a que los datos de tráfico, en cuanto información necesaria para la conducción de una comunicación, su facturación o los pagos de las interconexiones, se hagan anónimos o se cancelen una vez dejen de ser necesarios a los efectos de la transmisión, expire el plazo para la impugnación de la factura o exigencia del pago. De manera que para cualquier otro tratamiento de los mismos con fines comerciales o para la prestación de servicios de valor añadido se les exige obtener el previo consentimiento expreso e informado del abonado o usuario. Los datos de tráfico incluyen también aquellos datos de localización imprescindibles para la conexión, pero para su tratamiento la ley exige el previo consentimiento expreso e informado del abonado o usuario, o que los mismos se hagan anónimos. Conectado también con los datos de tráfico, se encuentra el derecho de los abonados a recibir facturas no desglosadas cuando así lo soliciten. También deben los operadores garantizar el derecho del interlocutor a reservarse la identificación de su línea tanto en las llamadas que genere como a impedir en las llamadas entrantes la presentación de la identificación de la línea de origen o a rechazar aquellas que no cuenten con tal identificación.

- Guías de abonados (art. 38.6 LGT). La ley exige a las empresas que asignen números de teléfono a los abonados a dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, incluyendo facilitar el derecho a no figurar en dichas guías. No exige la ley la obligación de recoger el consentimiento expreso para la elaboración y comercialización de las mismas (disposición adicional novena LGT), pero el abonado ha de tener la posibilidad de decidir si desea o no figurar en una guía pública y, en caso afirmativo, con cuáles de sus datos personales, a través de un derecho de exclusión que por supuesto no puede generar contraprestación alguna.

- Comunicaciones no solicitadas con fines de venta directa (o promocionales) (art. 38.3 h) LGT)

Esta Ley regula las comunicaciones no solicitadas con fines promocionales, incluyendo tan sólo los sistemas de llamadores automáticos sin intervención humana y fax, haciendo una remisión a las obligaciones recogidas en la LSSI sobre la regulación del *spam* por correo electrónico o medios equivalentes (la LGT remite al régimen sancionador de la LSSI, en cuanto a la vulneración del *spam* por correo electrónico o mensajes de datos a terminales fijos o móviles como SMS/MMS). Sin embargo, no regula ni hace referencia alguna a distintas formas de venta directa, como las llamadas personales de telefonía vocal. En relación a esta actividad, la ley exige el consentimiento previo e informado del abonado (no expreso) para remitir tales llamadas automáticas o mensajes de fax con fines comerciales.

Directiva 2006/24CE, de 16 de marzo de 2007

En el capítulo 3 (pagina 26 y ss) se analiza la Directiva de la Unión Europea sobre conservación de datos y el proyecto de ley para su transposición a la legislación española.

3.- DERECHO DICTADO EN RELACIÓN CON LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL.

Introducción

El presente capitulo recoge las principales novedades y aportaciones normativas en el ámbito de la Protección de Datos de Carácter Personal producidas en el periodo 2006/2007.

La información recogida puede dividirse en dos grandes bloques, según nos refiramos a España o a la Comunidad Europea:

Actividad normativa sobre protección de datos personales en el marco Legislativo Español

- En el ámbito de la Protección de Datos Personales, el periodo 2006/2007 ha estado sin duda marcado por el desarrollo del Nuevo Reglamento de desarrollo de la LOPD que durante este espacio de tiempo se ha llevado a cabo.

En el presente Informe se hace mención expresa al contenido de esta norma, actualmente en trámite de Información Pública.

Se trata de una norma fundamental que, con el empeño por conseguir una mayor seguridad jurídica, tendrá efectos muy positivos al proporcionar una regulación reglamentaria completa para la Ley Orgánica de Protección de Datos Personales (LOPD), recogiendo aspectos mejorables de la transposición de la Directiva 95/46/CE, la jurisprudencia elaborada por el Tribunal Constitucional y por los tribunales españoles y la experiencia práctica de la AEPD en la aplicación de la LOPD y dar solución a algunos aspectos que estaban necesitados de actualización.

El ejemplo más significativo es el de las medidas de seguridad aplicables a los tratamientos no automatizados.

Se recogen también los efectos que para el área de protección de datos han tenido distintas iniciativas legislativas como es el caso de la Ley para el Impulso de la Sociedad de la Información u otras normas que afectan a la materia analizada.

- Por otra parte, se han producido otras novedades significativas como han sido las disposiciones e instrucciones dictadas por la AEPD.

Así, hacemos referencia en el informe a la Instrucción 1/2006 de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras o a otros informes y disposiciones sobre temas específicos que se han desarrollado a lo largo del periodo recogido en este Informe.

- Por último, se hace una pequeña mención a la actividad desarrollada por la AEPD en otros ámbitos que han afectado en mayor o menor medida al desarrollo de la protección de datos en España.

Actividad normativa sobre protección de datos personales en el marco de las Comunidades Autónomas

En el plano autonómico, a lo largo del periodo analizado se ha confirmado la tendencia a la creación de entidades supervisoras en Comunidades como Valencia, Aragón o Andalucía y que a corto plazo se unirán a las Agencias de Protección de Datos de Madrid, País Vasco y Cataluña.

Actividad normativa sobre protección de datos personales en la marco de la Comunidad Europea.

Respecto al marco europeo, y teniendo como referencia la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, durante este periodo 2006/2007, se ha percibido una notable actividad normativa en las áreas de seguridad y cooperación (entre estados miembros y con terceros países) que implican áreas directamente relacionadas con la Protección de Datos. En este sentido se recogen distintas disposiciones y acuerdos en el presente Informe que son reflejo de una preocupación creciente en materia de seguridad.

El modo en el que esta preocupación puede afectar a la protección del derecho fundamental a la protección de los datos personales, se refleja en el contenido de la carta dirigida por el Supervisor Europeo de Protección de Datos a los responsables de los Ministerios de Justicia e Interior portugueses, previa la presidencia de este país. En ella, el Supervisor hace referencia a la idea que a su juicio se está extendiendo, según la cual "no puede haber derecho a la privacidad hasta que la vida y la seguridad estén garantizados" y hace constar su idea de que los derechos fundamentales no pueden ser considerados como un lujo cuando se pone en contacto con asuntos relacionados con la seguridad.

En este sentido, repasaremos en el presente Informe algunas de las principales decisiones e Informes emitidos tanto por el Supervisor Europeo de Protección de Datos como por el Parlamento Europeo. En concreto, se recogen los siguientes:

- Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.
- Transmisión de los datos de pasajeros de líneas aéreas a EEUU.
- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento 1073/1999 relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).
- Proyecto de Decisión Marco sobre protección de datos en la cooperación policial y judicial.
- Reglamento 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).
- Sanciones penales para garantizar el respeto a la protección de datos personales.

Como hemos mencionado la información recogida en este capitulo, en relación con la actividad normativa desarrollada durante este periodo, puede clasificarse en los bloques referidos, pero se estructura siguiendo el orden cronológico en el que se produjeron las novedades.

A modo de sumario, incluimos referencia a los puntos recogidos:

1. Preparación del nuevo Reglamento de Medidas de Seguridad
2. Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones
3. Transmisión de datos de los pasajeros (PNR) a EEUU

4. Dictamen del Supervisor Europeo de Protección de Datos (SEPD) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento 1073/1999 relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).
5. Proyecto de Decisión Marco sobre protección de datos en la cooperación policial y judicial.
6. Instrucción de la AEPD 1/2006, de 12 de diciembre sobre Videovigilancia y protección de datos personales.
7. Reglamento 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II).
8. Informe AEPD sobre sistemas "*whistleblowing*".
9. Sanciones penales para garantizar el respeto a la protección de datos personales.
10. Novedades Normativas
11. Agencia Española de Protección de Datos
12. Agencias Autonómicas de Protección de Datos

Preparación del nuevo Reglamento de Medidas de Seguridad

A lo largo del periodo 2006/2007, la preparación del nuevo Reglamento de Medidas de Seguridad ha sido sin duda uno de las preocupaciones principales para los actores implicados en la protección de datos personales.

En efecto, la necesidad de elaborar un desarrollo reglamentario adecuado a las necesidades de la LOPD y capaz de superar las limitaciones del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS), ha constituido una reclamación constante por parte las partes implicadas en el tratamiento de los datos personales (responsables de ficheros, empresas de servicios, etc).

La vigente LOPD declara subsistente el RMS en todo en cuanto no se opusiera a su contenido (Disposición Transitoria Tercera LOPD) el cual fue desarrollado con base en la derogada LORTAD (Ley Orgánica de regulación automatizada de datos 5/1992).

Por ello, y hasta el momento actual, el RMS ha mantenido su vigencia y todos los tratamientos de datos personales han aplicado las medidas contenidas en el mismo, lo que ha provocado algunos problemas.

En primer lugar, y como indica su denominación, el RMS no fue desarrollado para su aplicación a los ficheros de datos personales no automatizados, esto es, ficheros no informatizados "que permitan acceder sin esfuerzos desproporcionados a (…) datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica", según la descripción del Borrador del nuevo Reglamento de Medidas de Seguridad.

El artículo 1 RMS establece que la norma será aplicable únicamente a los ficheros automatizados y ha sido la LOPD la que ha ampliado su ámbito de aplicación a todos "los datos de carácter personal registrados en soporte físico susceptibles de automatización" (art. 2 LOPD).

Sobre esta base, el RMS es aplicable a todos los ficheros en soporte no automatizado que se hubieran creado con posterioridad a la entrada en vigor de la LOPD, el 14 de enero de 2000. Para los ficheros en

soportes no automatizados que existieran antes de dicha fecha se estableció un período de adaptación en la Disposición Adicional Primera LOPD (que finaliza en el mes de octubre de 2007).

No obstante, las medidas de seguridad contenidas en el RMS tienen la limitación de estar previstas para tratamientos automatizados, y por ello solo son aplicables a los no automatizados aquellas que por su naturaleza se adapten a los mismos como, por ejemplo, la exigencia de la elaboración e implantación del Documento de Seguridad.

Por otra parte, el hecho comentado de que las medidas incluidas en el RMS hicieran referencia a la LORTAD dejaba sin desarrollo reglamentario específico importantes aspectos de la LOPD.

Con el desarrollo del nuevo reglamento se trata, por tanto, de subsanar los dos aspectos mencionados.

A la espera de la versión definitiva, se han ido conociendo diferentes borradores de los que pueden deducirse los siguientes aspectos como principales novedades respecto al Real Decreto 994/1999.

Principales novedades

En primer lugar llama la atención la extensión del texto sobre el que se está trabajando. En efecto, nos encontramos ante un texto de 154 artículos repartidos en 9 títulos, superando con mucho la extensión del aún vigente Real Decreto 994/1999.

Ámbito de aplicación

El nuevo Reglamento (NR) en su artículo 2 establece que será de aplicación a todos los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos. Por consiguiente, tanto los tratamientos automatizados como los no automatizados serán regulados por el NR.

Como hemos comentado, la aplicación de medidas de seguridad a los ficheros no automatizados es uno de los aspectos más publicitados del NR y con seguridad implicará importantes costes asociados a las empresas, que a día de hoy realizan buena parte de sus gestiones en papel almacenado en extensos archivos que en muchas ocasiones son difícilmente controlables.

No obstante, el legislador entiende que la aplicación de estas medidas es imprescindible para la seguridad de los datos personales y por tanto para la garantía del respeto al derecho fundamental a su protección, ya que en la práctica son los datos contenidos en estos soportes los que provocan más violaciones de estos derechos.

La inclusión de estos tratamientos dentro del ámbito de aplicación del NR es clara. La misma se ve reforzada en el artículo 77 cuando detalla el alcance de las medidas de seguridad:

> "Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento"

Por otro lado, y todavía dentro del análisis del ámbito de aplicación, hay que mencionar que expresamente se dispone que el NR no aplica a los datos referidos a personas fallecidas, (salvo en las disposiciones relativas al acceso y cancelación de estos datos a instancia de las personas vinculadas)

Por último, y en lo que se refiere al ámbito territorial, hay que señalar que el NR aplicará en aquellos casos en los que aunque el responsable del fichero no esté ubicado en España, sí lo esté el encargado de tratamiento.

Cambios en el nivel de protección de los ficheros declarados

Una de las cuestiones que afectará directamente a las empresas es la modificación en algunos casos de los niveles de protección aplicables a los ficheros de datos personales.

El Borrador analizado incluye, por ejemplo, la siguiente disposición:

> "Artículo 79. Aplicación de los niveles de seguridad a los ficheros y tratamientos automatizados.
>
> (…) 5. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos".

El NR permite por lo tanto rebajar el nivel de protección a uno de los ficheros que se tratan en todas las empresas: el fichero de Empleados.

El legislador de esta forma viene a reconocer que la finalidad de este tipo de tratamientos no está relacionada en ningún caso con los datos sensibles que puedan recogerse en el mismo y por tanto elimina la necesidad de implantar las medidas de nivel alto, reduciendo con ello el coste que estas medidas implican a las empresas.

Nuevas medidas de seguridad

Evidentemente, una de las principales cuestiones para los responsables de ficheros será conocer cuáles son las nuevas medidas de seguridad que deberá implantar para su adecuación al NR. Como ya hemos comentado, habrá que fijarse especialmente en las medidas que deberán aplicarse a los ficheros no automatizados.

Respecto a estas nuevas medidas, hay que señalar que se mantienen los tres niveles conocidos hasta ahora (Básico, Medio y Alto) y que se añaden a la tipología de datos ya recogida en el actual RMS los siguientes:

- Datos de menores de 14 años (nivel de protección medio).
- Datos de víctimas de violencia de género (nivel de protección medio).
- Datos de tráfico de operadores (nivel de protección medio).
- Datos de localización de operadores (nivel de protección alto).
- Datos y claves necesarios para emitir certificados digitales (nivel de protección alto).
- Datos referentes a las obligaciones del retenedor o a transferencias dineraria a entidades de los que los interesados son asociados o miembros (nivel de protección alto).

Se detallan a continuación brevemente todas las nuevas medidas que los Borradores analizados incluyen.

<u>Medidas de nivel básico</u>

- Aplicables a todos los ficheros
  - Funciones y obligaciones del personal
  - Registro de incidencias

  - Control de acceso
  - Gestión de soportes y documentos
- Aplicables a ficheros automatizados
  - Identificación y autenticación (posibilidad de utilizar certificados digitales o medidas biométricas, periodicidad para cambio de contraseñas)
  - Copias de respaldo y recuperación (se añade una obligación de verificación)
- Aplicables a ficheros no automatizados
  - Almacenamiento de la información (mecanismos que obstaculicen su apertura, inventariado, almacenamiento en lugares controlados)
  - Criterios de archivo (para la conservación, localización y consulta de información, y posibilitar los derechos ARCO)[9]

Medidas de nivel medio

- Aplicables a todos los ficheros
  - Responsable de Seguridad
  - Realización de Auditoría:
    - Se mantiene la obligación de auditar cada dos años, salvo que modificación importante de los Sistemas de Información.
    - En caso de auditoría interna, la persona deberá tener asignadas funciones independientes del área auditada.
    - Se notificará a la AEPD la fecha del informe y si se ha tratado de una auditoría interna o externa
- Aplicables a ficheros automatizados
  - Identificación y autenticación (limitación de intentos fallidos)
  - Control de acceso físico
  - Registro de incidencias
  - Registro de accesos (se incluye la excepción de que el responsable del fichero sea persona física y garantice que sólo él es quien tiene acceso y lo trata)
  - Pruebas con datos reales
  - Cifrado de datos (cuando se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del fichero)
- Aplicables a ficheros no automatizados
  - Seguridad en los locales (dotación de mecanismos que impidan la destrucción y recuperación de la información, dispositivos ignífugos, equipamiento contra incendios)
  - Acceso físico (armarios y archivadores ubicados en áreas de acceso restringido o bajo vigilancia del personal designado en el documento de seguridad, mecanismos que impidan el libre acceso a los mismos por personas no autorizadas)

[9] Derechos de Acceso, Rectificación, Cancelación y Oposición recogidos en los arts. 15 a 17 de la LOPD.

  - Copia o reproducción (limitar la posibilidad de copiar documentos y acceder a las copias, control para evitar accesos no autorizados)

Medidas de nivel alto

- Aplicables a todos los ficheros
  - Distribución de soportes (aplica a dispositivos portátiles).
- Aplicables a ficheros automatizados
  - Copias de respaldo y recuperación
  - Telecomunicaciones
- Aplicables a ficheros no automatizados
  - Registro de accesos (solicitud de acceso, registro, plazo de conservación de dos años)
  - Almacenamiento de la información (armarios y archivadores con llave o similar, custodia de información en proceso de tramitación antes de ser archivada en el fichero)
  - Traslado de documentación (medidas para impedir su manipulación y controles que permitan detectar si se ha producido algún acceso no autorizado)
  - Copia o reproducción

Primeras acciones para los responsables de tratamiento

De acuerdo a las novedades y especialmente a las nuevas medidas enunciadas, ya podemos desglosar algunas acciones que los responsables de tratamiento deberán llevar a cabo de cara a su adaptación a la nueva norma.

- Identificar tratamientos no automatizados de datos personales.
- Valorar los posibles cambios de nivel de seguridad aplicable a los ficheros ya declarados.
- Revisión de los tratamientos realizados actualmente para adecuarlos a los nuevos requisitos legales de información, consentimiento y cesión.
- Actualización del Documento de Seguridad, incorporando las nuevas medidas de seguridad para los ficheros no automatizados.

Como conclusión al estudio de los distintos borradores del NR hay que mencionar en primer lugar la conveniencia de una norma única que aporte claridad y desarrolle el marco vigente dando seguridad a los distintos sectores y agentes implicados, evitando la dispersión en distintas normativas y el NR contribuye a solucionar dudas a los sectores más afectados, como son los de telecomunicaciones, financiero o de publicidad.

Por otra parte, debe destacarse la comentada inclusión de la regulación de los datos manuales o no automatizados, con una regulación específica y no asimilada a la de los automatizados. Estas medidas van a suponer sin duda un notable esfuerzo para los responsables de tratamiento y en este sentido debe matizarse que se establecerá un plazo de dos años para que las empresas se adapten la nueva legislación y actualicen estos ficheros no automatizados.

Otra novedad es la inclusión de menciones específicas a ciertos tipos de datos sensibles con el objeto de garantizar una mejor protección en estos ámbitos. Es el caso de los datos referidos a menores, a personas fallecidas, a las víctimas de la denominada violencia de género, a los datos de tráfico o a los de localización de comunicaciones electrónicas.

El NR incluye también la exigencia de determinadas formalidades que se añaden con el objeto de aportar mayor seguridad jurídica en relación con los deberes de información y de necesidad de ciertos consentimientos tácitos y expresos por parte de los titulares de los derechos.

Se trata por tanto de una norma necesaria, largamente demandada por todas las partes implicadas y que debe contribuir a proporcionar una protección más completa a los datos personales, garantizando el respeto de este derecho fundamental.

El borrador ha sido elaborado por la Secretaría Técnica del Ministerio de Justicia, y actualmente se encuentra en fase de audiencia pública, al haber sido remitido a un total de 70 entidades para su estudio y presentación de comentarios por parte de las mismas.

Por último y respecto a los plazos previstos para la entrada en vigor del NR, el Gobierno dió a conocer su intención de proceder a su aprobación en el otoño de 2007.

Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones

Con el objetivo declarado de proporcionar los medios técnicos necesarios para una persecución eficaz de los delitos que, cada vez en mayor grado, se sirven de elementos basados en las comunicaciones, el 15 de marzo de 2006 se promulgó la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

En concreto, el objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de ponerlos a disposición de los agentes autorizados (miembros de los Cuerpos Policiales, personal del Centro de Inteligencia y funcionarios de la Dirección Adjunta de Vigilancia Aduanera), siempre en el marco de investigaciones criminales.

Se trata de que todos éstos funcionarios públicos puedan obtener los datos relativos a las comunicaciones que, en el marco de una investigación, se hayan podido efectuar por medios telefónicos y por Internet.

Como era de esperar, este texto provocó numerosas reacciones en todos los sectores implicados. Citaremos como ejemplo, el caso del Grupo de Protección de Datos que adoptó el Dictamen 3/2006 en el que ponía de manifiesto sus reservas en relación con las, a su juicio, graves consecuencias que la Directiva tendrá para la privacidad de los ciudadanos europeos.

En el Dictamen, el GT29 exigía el máximo nivel posible de protección de datos, para lo que enunciaba una serie de garantías mínimas, entre las que, además de la implantación de las necesarias medidas de seguridad, se recogían las siguientes:

a) Respeto al principio de finalidad para el tratamiento (finalidad de la retención, en este caso), lo que implica la necesidad de una definición clara y precisa del concepto "delito grave" prohibiéndose o restringiéndose seriamente cualquier tratamiento posterior y reduciendo al máximo los datos tratados.

b) Necesidad de restringir el acceso únicamente a aquellas fuerzas de seguridad específicamente designadas públicamente y de que estos accesos sean autorizados caso por caso, por las autoridades judiciales.

c) Necesidad de que los accesos de las mismas queden registrados y a disposición de las autoridades de control.

d) Prohibición de técnicas de "minería de datos" sobre los datos retenidos.

e) Separación física entre los sistemas en los que se almacenan los datos retenidos y los que se utilizan habitualmente en la actividad comercial de los operadores.

Con el fin de llevar a cabo la transposición de esta Directiva, el 16 de marzo de 2007 se ha publicado en el Boletín Oficial del Congreso de los Diputados el **Proyecto de Ley de Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones**.

Respecto a su contenido, se señala como obligados a su cumplimiento a los operadores que presten servicios de comunicaciones electrónicas y a aquellos que exploten redes públicas de comunicaciones.

Las obligaciones más reseñables para estos operadores se resumen en la conservación de los datos necesarios para:

1. Rastrear e identificar el origen de una comunicación.
2. Identificar el destino de una comunicación.
3. Determinar la fecha, hora y duración de una comunicación.
4. Identificar el tipo de comunicación.
5. Identificar el equipo de comunicación de los usuarios.
6. Identificar la localización del equipo de comunicación móvil.
7. Conocer las llamadas infructuosas realizadas.

Es fundamental señalar que conforme al texto del Proyecto de Ley, no podrán conservarse en ningún caso los datos que revelen el contenido de la comunicación.

El periodo de conservación será en principio de doce meses (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE).

Por otra parte, el Proyecto de Ley incorpora en sus disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido del nuevo texto. Esta adaptación incluye, entre otras, la consideración de infracción grave del incumplimiento, por parte de los operadores, de las obligaciones expuestas.

Del estudio del Proyecto de Ley puede concluirse que se ha tratado de elaborar un texto respetuoso con el derecho al secreto de las comunicaciones (garantizado por la limitación de las obligaciones de conservación a los datos de tráfico y no al contenido de las comunicaciones)

No obstante, distintos sectores han puesto de manifiesto su preocupación por el respeto del derecho fundamental a la tutela de los datos de carácter personal que puede verse afectado.

En efecto, los datos de localización y tráfico, que deberán ser conservados, son datos de carácter personal.

Por ello, el hecho de que no se determinen expresamente los delitos que justifiquen la cesión de los datos conservados, tal y como indicaba la recomendación 3/2006 del Grupo de Protección de Datos ya comentada, puede generar una importante merma del derecho a la protección de datos de los titulares de dichos datos.

Se trata por tanto de una cuestión que deberá tenerse en cuenta una vez que Ley entre en vigor pues, como se pone de manifiesto en distintos puntos de este informe, la lucha contra el terrorismo y la garantía de la seguridad, no deben en suponer un límite al ejercicio de derechos.

Transmisión de datos de los pasajeros (PNR) a EEUU

Con fecha de 16 de octubre de 2006, el Consejo de la Unión Europea sancionó el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

Dicho Acuerdo, recogido en la Decisión 2006/729/PESC/JAI[10], es el resultado de la exigencia que Estados Unidos venía realizando desde 2003 a las compañías aéreas para que éstas facilitasen 34 datos personales de los viajeros con destino a aquel país. Entre estos datos se encuentran el nombre, la dirección, la forma de pago del billete o, incluso, la agencia de viajes donde se compró.

En el año 2004, ya se alcanzó un acuerdo entre la UE y los EEUU en esta materia, pero el mismo fue anulado por la Corte Europea de Justicia 30 de mayo de 2006 por un defecto de forma.

El tribunal europeo dio entonces un plazo que finalizaba el 30 de septiembre de 2006 para alcanzar otro acuerdo que pudiera aplicarse a esta materia.

Durante la negociación EEUU trató de ampliar el número de datos de los pasajeros que debían facilitársele, a lo cual se negó la UE que sin embargo accedió a que todas las agencias de seguridad estadounidenses implicadas en la lucha contra el terrorismo (y no solo el Servicio de Aduanas y Protección de Fronteras) pudieran acceder a estos datos.

El nuevo acuerdo especifica que los servicios aduaneros de EEUU no podrán acceder a datos calificados como "sensibles", tales como el origen racial o la religión. Tampoco se puede comunicar el estado de salud o la orientación sexual de los pasajeros. Las autoridades estadounidenses se comprometen a su vez a elaborar un sistema automático para borrar los datos sensibles que figuren en la lista de PNR.

Con fecha de 16 de octubre de 2006, el Consejo de la Unión Europea sancionó el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (DHS, por sus siglas en inglés).

Dicho Acuerdo, recogido en la Decisión 2006/729/PESC/JAI, es el resultado de la exigencia que EEUU venía realizando desde 2003 a las compañías aéreas para que estas facilitasen 34 datos personales de cada viajero con destino a aquel país. Entre estos datos se encuentran el nombre, la dirección, la forma de pago del billete o la agencia de viajes donde se compró.

[10] Publicado el 27 de octubre de 2006.

En el año 2004, ya se alcanzó un acuerdo entre la UE y los EEUU en esta materia, pero el mismo fue anulado por la Corte Europea de Justicia el 30 de mayo de 2006 por un defecto de forma. El tribunal europeo dio entonces un plazo que finalizaba el 30 de septiembre de 2006 para alcanzar otro Acuerdo que pudiera aplicarse a esta materia. Se firmó entonces un nuevo Acuerdo para el que se estableció el 31 de julio de 2007 como fecha de expiración.

En virtud de lo anterior, y con fecha de 23 de julio se ha producido la Decisión 2007/551/PESC/JAI, del Consejo, relativa a la firma en nombre de la UE, de un Acuerdo entre la UE y los EEUU sobre transferencia de PNR por las compañías áreas al DHA de los EEUU (el denominado "Acuerdo PNR 2007")

El Acuerdo entró en vigor provisionalmente desde la fecha de su firma e incluye un sistema de transmisión por el que son las Compañías Aéreas que operan vuelos entre la UE y los EEUU quienes transmitirán los datos PNR al DHS.

Asimismo, el Acuerdo permite la utilización de los datos durante siete años desde su transmisión. Cumplido dicho plazo, se conservarán inactivos durante ocho años más. En el caso de que los datos de PNR incluyan datos sensibles, el DHS se compromete a filtrar dichos datos y a no utilizarlos excepto en casos excepcionales (en los que se le permite el acceso controlado a los mismos durante treinta días).

Dictamen del Supervisor Europeo de Protección de Datos (SEPD) sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento 1073/1999 relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF)

La Propuesta de Reglamento por el que se modifica el Reglamento (CE) 1073/1999 del Parlamento Europeo y del Consejo, de 25 de mayo de 1999, relativo a las investigaciones efectuadas por la OLAF, contiene revisiones de la mayoría de los artículos de dicho Reglamento que establece las normas operativas que deben seguir los implicados en las investigaciones de la OLAF y, como tal, constituye el fundamento jurídico para las actividades operativas de la OLAF.

La Propuesta fue enviada por la Comisión al SEPD el 15 de septiembre de 2006.

Las modificaciones propuestas al Reglamento aspiran a mejorar la eficacia y eficiencia de las investigaciones de la OLAF, por ejemplo asegurando que los poderes de investigación de la OLAF cubran a los operadores económicos de los Estados miembros que reciben fondos comunitarios. Con este fin se proponen también facilitar el intercambio de información sobre presuntas infracciones entre la OLAF y las diversas instituciones interesadas, tanto a escala de la UE como al nivel nacional. Es destacable el propósito de garantizar los derechos de las personas implicadas en una investigación, incluyendo su derecho a la protección de datos y a la intimidad.

Pese a lo anterior, el SEPD hace constar que la Propuesta puede implicar que el nuevo Reglamento se considere como una "*lex specialis*" para la regulación de los tratamientos de datos personales recogidos en el ámbito de las investigaciones de la OLAF, que estaría por encima de la aplicación del marco general de protección de datos contenido en el Reglamento 45/2001. Ello resulta particularmente preocupante si se considera que las normas de protección de datos contenidas en la Propuesta son

menos exigentes que las contenidas en el Reglamento (CE) no 45/2001, y ello sin ninguna justificación aparente.[11]

Por ello, el Dictamen analiza la Propuesta, y detecta las siguientes deficiencias a subsanar:

- Deficiencias relativas al derecho a la información en el contexto de las investigaciones de la OLAF
- Deficiencias relativas al derecho de acceso en el contexto de las investigaciones de la OLAF
- Deficiencias relativas al derecho de rectificación en el contexto de las investigaciones de la OLAF

Proyecto de Decisión Marco sobre protección de datos en la cooperación policial y judicial

La propuesta, presentada por la Comisión, de una Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, fue objeto de un amplio debate en el Grupo Multidisciplinar "Delincuencia Organizada" (GMD), donde ya pudieron aclararse en gran medida varias cuestiones. El Proyecto pretende que la Decisión Marco constituya un instrumento jurídico encaminado a facilitar este intercambio de información.

No obstante, tanto los Estados miembros como otros organismos, como es el caso especialmente del SEPD, aún siguen manteniendo un buen número de reservas al respecto.

En efecto, los textos que el Consejo está debatiendo en la actualidad suscitan dudas en cuanto a la idoneidad del resultado final, que debe garantizar al ciudadano una protección eficaz. En la situación actual, el objetivo de rapidez en la cooperación podría dar lugar a que algunas disposiciones de corte garantista queden suprimidas o rebajadas.

En este sentido, el SEPD se ha pronunciado en distintas ocasiones destacando la necesidad de un marco jurídico sólido que garantice el respeto de los derechos fundamentales del ciudadano.

Así, el 19 de diciembre de 2005, el SEPD ya formuló un dictamen sobre la propuesta de Decisión marco del Consejo que había presentado la Comisión. En dicho dictamen, se destacaba la importancia de la propuesta que debía constituir un instrumento eficaz para la protección de los datos personales en el ámbito regulado por el Título VI del Tratado de la UE.

En opinión del SEPD este instrumento no sólo debe respetar los principios de la protección de datos establecidos en el Convenio 108 del Consejo de Europa y, más concretamente, de la Directiva 95/46/CE, sino proporcionar además un cuerpo adicional de normas que tengan en cuenta la especificidad del ámbito policial y judicial.

En este primer dictamen, el SEPD consideraba esencial que la Decisión marco abarque todos los aspectos del tratamiento de datos policiales y judiciales, incluso los que no hayan sido transmitidos o facilitados por las autoridades competentes de otros Estados miembros. La coherencia de la protección de los datos personales es esencial a su juicio, con independencia del lugar de su tratamiento, del ente que lo realice o de la finalidad para la cual se traten los datos.

[11] Fuente: Web Supervisor Europeo de Protección de Datos (http://www.edps.europa.eu)

Por su parte, el 27 de septiembre de 2006, el Parlamento Europeo adoptó una resolución legislativa sobre la propuesta de la Comisión que, en términos generales, iba en el mismo sentido que el dictamen del SEPD, a saber: apoyo global a la propuesta e introducción de enmiendas encaminadas a mejorar el grado de protección ofrecido.

Ante la evolución de las negociaciones, en noviembre de 2006, el SEPD volvía a pronunciarse sobre este asunto expresando su preocupación por la forma en el que se están llevando a cabo las negociaciones, que en muchos casos no incorporan las enmiendas propuestas por el Parlamento Europeo ni los dictámenes del SEPD y de la Conferencia de las autoridades europeas de protección de datos. En cambio, en un buen número de casos, se han suprimido o debilitado considerablemente disposiciones de la propuesta de la Comisión que ofrecían garantías a los ciudadanos. Por ello expresaba su preocupación en estos términos: "Como consecuencia de ello, existe un riesgo importante de que el nivel de protección resultante de esta propuesta sea inferior al garantizado por la Directiva 95/46/CE, e incluso por el Convenio 108 del Consejo de Europa, cuya formulación es aún más general y que es vinculante para los Estados miembros".

Ante esta perspectiva, el SEPD recomendaba que el Consejo prolongue las negociaciones para alcanzar un resultado que garantice una protección suficiente.

La propuesta de la Comisión está siendo debatida en la actualidad por el Consejo que, al parecer, está progresando en sus trabajos y modificando elementos esenciales del texto de la propuesta[12]. (Ver pagina 37: Sanciones penales para garantizar el respeto a la protección de datos personales)

Instrucción de la AEPD 1/2006, de 12 de diciembre sobre Videovigilancia y Protección de Datos Personales

El 12 de diciembre de 2006 se publicó en el BOE la Instrucción de la AEPD 1/2006 sobre Videovigilancia y Protección de Datos Personales.

La Instrucción se entendía necesaria ante el notable incremento del número de sistemas de cámaras y videocámaras instaladas con fines de vigilancia. A este incremento ha contribuido sustancialmente el desarrollo de sistemas digitales de grabación y el abaratamiento de las comunicaciones, que han permitido que este tipo de soluciones sean muy accesibles.

Por otro lado, hay que tener en cuenta que esta materia afecta directamente a derechos fundamentales y no ha sido completamente desarrollada conforme establecía la Disposición Adicional Novena de la Ley Orgánica 4/1997[13], que establecía el plazo de un año para que el Gobierno elaborara la normativa que adaptara los principios establecidos en la Ley al ámbito de la Seguridad Privada. Esta materia implica también a otras áreas del ordenamiento jurídico como es el caso del derecho laboral en lo que respecta a la colocación de cámaras de vigilancia en los puestos de trabajo[14].

[12] Fuente: Web Supervisor Europeo de Protección de Datos (http://www.edps.europa.eu)

[13] Ley Orgánica 4/1997, de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en los lugares públicos.

[14] De hecho, la AEPD ya de había pronunciado en parte sobre el tema en el año 2001, cuando emitió el informe "Videovigilancia en el lugar de trabajo".

Por todo ello, la Instrucción resultaba necesaria de cara a clarificar conceptos y garantizar el correcto tratamiento de los datos personales. De hecho, la Instrucción viene a satisfacer la necesidad de una regulación que ya se había planteado en foros internacionales. Así, en la Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los días 1 a 3 de Noviembre de 2006, se discutió sobre la necesidad de adecuar la video vigilancia a las exigencias del derecho fundamental a la protección de datos.

Naturaleza del tratamiento

Para el análisis de esta materia hay que establecer, en primer lugar, que las imágenes de personas captadas a través de los sistemas de videovigilancia son datos personales. A esta conclusión llegamos en aplicación del artículo 3 de la LOPD y del artículo 1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

Es cierto, por otra parte, que la captación de imágenes mediante sistemas de videovigilancia posee notas que la singularizan respecto a otros tratamientos de datos personales.

En primer lugar, se trata de tratamientos que a menudo se llevan a cabo sin el conocimiento del interesado. Además, la evolución de la tecnología en este campo está alumbrando nuevas formas de tratamiento y explotación de estos datos que pueden plantear problemas desde la perspectiva de la protección de datos de carácter personal y de la protección de la intimidad de las personas.

Ámbito de aplicación

El ámbito de aplicación de la Instrucción 1/2006 es definido en su artículo 1 en el que se especifica que la será aplicable a los tratamientos "de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras".

Los tratamientos sometidos a la Instrucción serán aquellos que comprendan "la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas".

Por último el artículo 1 excluye de su regulación los tratamientos de imágenes "en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar"

Proporcionalidad

Debido a las características ya comentadas de los sistemas de videovigilancia, la Instrucción coloca como presupuesto fundamental para llevar a cabo este tipo de tratamientos, el principio de proporcionalidad.

En efecto, ya desde la Exposición de Motivos la Instrucción dispone que "el uso de cámaras debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo".

Si bien la proporcionalidad es un concepto jurídico indeterminado, la Instrucción cita la Sentencia del Tribunal Constitucional 207/1996 que ha utilizado como una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad.

Conforme a la doctrina del TC, para comprobar si una medida restrictiva de un derecho fundamental supera este criterio de la proporcionalidad, será necesario constatar si cumple los tres siguientes requisitos o condiciones:

> "Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la

> consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

Por lo tanto, con el objeto de evitar situaciones abusivas, la proporcionalidad será el elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia y así, el artículo 4 de la Instrucción 1/2006 dispone lo siguiente:

> "2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.
>
> 3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida".

Resumimos a continuación el régimen de responsabilidades establecido por la Instrucción 1/2006 que incluye las siguientes obligaciones a cumplir del responsable del tratamiento.

1. Notificación de ficheros.

   Como obligación previa al inicio del tratamiento, la persona o entidad que instale sistemas de este tipo, debe notificarlo a la AEPD, para su inscripción en el Registro General de la misma (art. 7.1 Inst. AEPD, 1/2006).

   Se excluye explícitamente de este deber de notificación aquellos tratamientos consistentes únicamente en la captación y reproducción de imágenes en tiempo real sin que dichas imágenes sean almacenadas.

2. Calidad tratamiento.

   Junto con los comentarios realizados al respecto de la exigencia de proporcionalidad, y de cara a cumplir con el principio de calidad de los datos establecido por el artículo 4 LOPD, estos tratamientos deberán tener en cuenta la selección de los lugares de instalación de las cámaras.

   Se trata por tanto de una de las particularidades de estos tratamientos de datos personales, y al respecto, la Instrucción dispone las siguientes limitaciones:

   - Las cámaras se instalarán exclusivamente en espacios privados y no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de las características de los espacios privados a controlar.
   - De acuerdo con la finalidad expresada y al consentimiento que en este sentido se solicitará, las cámaras deberán colocarse de forma que abarquen los espacios privados a controlar, los accesos a edificios o, en su caso, los puestos de trabajo. Se evitará la grabación de imágenes de zonas públicas o zonas comunes no afectadas por la finalidad descrita.

3. Información.

   Otra de las características consustanciales a los tratamientos de imágenes captadas por sistemas de videovigilancia es el hecho de que la persona pueda no ser consciente de que la grabación se está

realizando. La AEPD ha tenido este hecho en cuenta, estableciendo en el artículo 3 de la Instrucción 1/2006 las siguiente pautas para garantizar la correcta información de los interesados.

- El responsable de tratamiento deberá colocar, en las zonas vigiladas, al menos un distintivo o cartel informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados. En este sentido, la AEPD publicó un modelo de cartel informativo que ha tenido una amplia aceptación.
- Deberá tener además, a disposición de los interesados, impresos en los que se detalle la información prevista en el artículo 5.1 LOPD.

4. Ejercicio de derechos.

   Respecto al ejercicio de derechos, la única aportación específica de la Instrucción a la regulación recogida en el LOPD es la de que el procedimiento establecido, para garantizar los derechos de los interesados, deberá incluir la exigencia de que la solicitud del particular incluya una imagen reciente del mismo, requisito que parece adecuado a la naturaleza del tratamiento.

   Por otra parte, y debido a esta naturaleza, existe el riesgo de que el ejercicio de derechos por parte de un titular afecte a los de otros cuyos datos pueden estar contenidos en el mismo soporte. A este respecto, la Instrucción se limita a establecer en el punto 2 del artículo 5 que:

   > "El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento".

5. Cancelación.

   Una de las limitaciones más importantes que la Instrucción contiene respecto a estos tratamientos es el periodo de cancelación.

   Hasta aquí el análisis de las principales novedades incluidas en la regulación contenida en la Instrucción 1/2006. Hay que señalar que las mismas dejan abiertos algunos puntos para el análisis que deberán plantearse ahora.

   Así, por ejemplo, será necesario delimitar los casos en los que estará autorizada la videovigilancia en la vía pública conforme al contenido comentado del artículo 4.3: "(…) salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas"[15]

   El plazo para la implantación de las medidas contenidas en la Instrucción 1/2006, finalizó el 13 de marzo de 2007.

Fuentes:

- Web AEPD

  "Videovigilancia y protección de datos personales. La Instrucción 1/2006, de 12 de diciembre de la Agencia Española de Protección de Datos". Ramón Martínez Martínez. Revista Aranzadi de Derecho y Nuevas Tecnologías. Año 2007-1. Nº 13.Pág. 73 y ss.

[15] Artículo que habrá que interpretar a la luz del artículo 4 LOPD y del artículo 7.5 de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil de Derecho al Honor, a la intimidad personal y a la propia imagen: "Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el art. 2 de esta ley: (…)5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el art. 8.2"

Reglamento 1987/2006 del Parlamento Europeo y del Consejo

Con fecha de 20 de diciembre de 2006, se aprobó el Reglamento 1987/2006 del Parlamento Europeo y del Consejo relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II)[16].

El Sistema de Información de Schengen («SIS»), creado en 1990 en aplicación del Acuerdo de Schengen, de 14 de junio de 1985, y relativo a la supresión gradual de los controles en las fronteras comunes, es un instrumento esencial para la aplicación de las disposiciones de dicho Acuerdo.

El Reglamento regula las condiciones en las que el SIS II sustituirá al SIS, tal como fue creado en virtud del Convenio de Schengen.

Se trata de un sistema que tratará datos personales de los ciudadanos de la Unión Europea a efectos de denegación de entrada o de estancia y para dichos tratamientos se establecen en el Reglamento una serie de normas:

- El SIS II incluye un sistema central (SIS II Central) y aplicaciones nacionales. En este sentido se prevé la posibilidad de que los Estados miembros establezcan conexiones entre las descripciones del SIS II que no afectarán a los periodos de conservación de los datos personales ni a los derechos de acceso. Se prevé el control, en cada Estado, por parte de las Autoridades Nacionales de Protección de Datos.
- Excepto en algunos casos tasados (que se evalúan supuesto a supuesto), los datos personales gestionados por SIS II, se borrarán automáticamente transcurrido un período de tres años.
- El SIS II permite tratar datos biométricos para ayudar a una identificación fiable.
- El SIS II también debe permite el tratamiento de datos sobre personas cuya identidad haya sido usurpada, a fin de evitar las dificultades causadas por la identificación incorrecta, respetando las garantías adecuadas, en particular el consentimiento de la persona en cuestión y una limitación estricta de los fines legales para los que dichos datos podrán ser objeto de tratamiento.
- Los tratamientos de datos personales que los organismos comunitarios llevarán a cabo en la gestión del SIS II se someten expresamente al Reglamento 45/2001, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Informe AEPD sobre sistemas *whistleblowing*

En el mes de junio de 2007, y como contestación a una consulta planteada, el Gabinete Jurídico de la AEPD ha emitido un Informe[17] sobre la creación de sistemas internos de denuncias en algunas compañías (los denominados mecanismos de *whistleblowing*).

[16] Fuente: Diario Oficial de la Unión Europea 26/04/2007

Estos sistemas se están implantando en algunas empresas, sobre todo de entornos financieros, y consisten en la creación de un canal para la tramitación de acusaciones sobre el incumplimiento de normas internas por parte de empleados. Entre otras cuestiones, los sistemas de *whistleblowing* no prevén la información a los investigados.

Los sistemas de *whistleblowing* han sido objeto de profundo y reiterado análisis por parte de las autoridades europeas de protección de datos, principalmente en el marco del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, en particular en lo relacionado con la implantación de los sistemas impuesta por la Ley Sarbanes-Oxley.

Desde el punto de vista de la protección de los datos de carácter personal, la AEPD aísla en el Informe mencionado las siguientes características de estos sistemas en relación con su funcionamiento:

- El sistema permite la denuncia de "comportamientos, acciones o hechos que puedan constituir violaciones tanto de las normas internas de la compañía como de las leyes, normativas o códigos éticos" que rigen su actividad.
- Todos los empleados de la compañía pueden ser denunciantes o denunciados en el sistema.
- Los empleados son previamente informados de la existencia, finalidad y funcionamiento del sistema, así como de las garantías de confidencialidad que se ofrecen para sus datos (tanto si se trata del denunciante o denunciado).
- Sólo accederán, en principio, a los datos el responsable de la investigación (denominado *compliance counter*) y las personas imprescindibles en la investigación de los hechos denunciados.
- Se informará al denunciado en el plazo más breve posible de los hechos denunciados, los destinatarios de la información, el departamento responsable del sistema y sus derechos en materia de protección de datos. No se informará de la identificación del denunciante a menos que hubiera obrado con mala fe.
- Los datos son transmitidos a las oficinas competentes de la compañía (en el caso de la consulta, ubicadas en el Reino Unido y Japón). Para el caso de los datos que se transmiten a Japón, solicitará autorización del Director de la Agencia Española de Protección de Datos.

La AEPD realiza respecto a los sistemas de *whistleblowing* las siguientes consideraciones:

- Todas las personas cuyos datos pueden ser tratados como consecuencia del establecimiento de procedimientos de denuncia mantendrán con la sociedad un vínculo contractual de derecho laboral, civil o mercantil. De esta forma se garantiza el cumplimiento del requisito del consentimiento (artículos 6 y 11 LOPD) para el tratamiento, incorporando la existencia de estos procedimientos dentro de la relación contractual, y en el caso de que se consideren necesarios para el desarrollo y control adecuado de la relación contractual, lo que permitiría considerar el mismo amparado en la LOPD.

  No obstante, para que esto fuera posible, sería preciso que la finalidad que justifica el establecimiento de los sistemas de denuncia resultase ajustada al adecuado mantenimiento de las relaciones contractuales, de forma que los sistemas deben centrase en la denuncia de conductas que puedan efectivamente afectar al mantenimiento o desarrollo de la relación contractual que vincula al denunciado y a la consultante (principio de proporcionalidad del tratamiento a la finalidad).

[17] REF. 2007/128

- En lo que respecta a la confidencialidad la AEPD exige que se respete el tratamiento confidencial de las denuncias presentadas a través de los sistemas de *whistleblowing*, de forma que se evite la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información. La garantía de la confidencialidad debe incluir que la persona denunciada no pueda acceder a los datos identificativos de la persona denunciante.
- Otro aspecto que la implantación de estos sistemas deberá tener en cuenta son los plazos de conservación de la información. En relación con este punto, es imprescindible que se establezca un plazo máximo para la conservación de los datos relacionados con las denuncias, a fin de evitar el mantenimiento de los mismos por un período superior que perjudique los derechos del denunciado y del propio denunciante.

  Este plazo debería limitarse a la tramitación de las medidas de auditoría interna que resultasen necesarias y, como máximo, a la tramitación de los procedimientos judiciales que se derivasen de la investigación realizada (como, por ejemplo, los que se deriven de las medidas disciplinarias adoptadas o de la exigencia de responsabilidad contractual a los auditores).
- Los sistemas de *whistleblowing*, implican también ciertas particularidades respecto al acceso de los interesados a sus datos fruto, en este caso, de la investigación que se está llevando a cabo. En tal sentido, la AEPD indica que la demora en la información al afectado no debería en ningún caso sobrepasar el plazo de tres meses previsto en el artículo 5.4 de la LOPD, dado que nos encontramos ante un supuesto de tratamiento de datos no obtenidos del afectado.
- Por último, y respecto al nivel de las medidas de seguridad que deberán aplicarse a estos sistemas, se recomienda la implantación de medidas de nivel alto, ya que la naturaleza de estos sistemas no permite conocer a priori el contenido real del fichero que dependerá de los datos derivados de las investigaciones que pueden implicar la inclusión en el sistema de datos especialmente protegidos, regulados por el artículo 7 LOPD.

Sanciones penales para garantizar el respeto a la protección de datos personales

Con fecha 8 de junio de 2007 el Parlamento Europeo ha aprobado un **Informe de la Comisión de Libertades Civiles** en el que se propone aplicar sanciones penales a las infracciones sobre la protección de datos personales. [18]

Los diputados reclaman, mediante este documento que la Autoridad de Control común de Datos Personales agrupe a las autoridades nacionales y al Supervisor Europeo de la Protección de Datos.

El Parlamento cree necesario establecer normas comunes sobre confidencialidad y seguridad en el tratamiento de datos, así como sanciones por utilización ilícita de la información personal por parte de las autoridades competentes. Sin embargo, aclara que corresponderá a cada Estado miembro determinar las sanciones, "incluidas las penales", aplicables a las infracciones de las disposiciones nacionales sobre protección de datos (enmiendas 6 y 53).

El Informe introduce también una serie de enmiendas a la Decisión Marco del Consejo relativa a la protección de datos en el marco de la cooperación policial y judicial ya comentado (ver página 29 de este Informe). En este sentido, aunque las autoridades nacionales de protección de datos supervisarán el

[18] Fuente: Web del Parlamento Eurpeo (www.europarl.europa.eu)

procesado de la información, el Informe subraya que las normas establecidas en la Decisión Marco se aplicarán a todas las autoridades sin excepción.

Por último, el Informe añade quince principios que deben guiar la recogida de datos personales (Enmienda 60) para los tratamientos de datos personales realizados en el marco de la cooperación policial y judicial en materia penal:

Principio 1: Protección de los derechos y las libertades

1. El tratamiento de datos personales asegurará un elevado nivel de protección de la dignidad y de los derechos y libertades fundamentales de los interesados, incluido el derecho a la protección de los datos personales.

Principio 2: Minimización

1. La utilización de datos personales se configurará minimizando su tratamiento cuando el fin perseguido pueda lograrse mediante el uso de información anónima o no identificada.

Principio 3: Transparencia

1. El tratamiento de datos personales será transparente de conformidad con el ordenamiento jurídico.

2. Deben especificarse y estar disponibles el tipo de datos y tratamientos, el período de conservación pertinente y la identidad del supervisor y del responsable, o responsables, del tratamiento.

Principio 4: Legitimidad del tratamiento

Sólo podrán tratarse los datos personales cuando así lo disponga una disposición legal que establezca que es necesario el tratamiento por las autoridades competentes.

Principio 5: Calidad de los datos

Principio 6: Categorías especiales de datos

1. Se prohibirá el tratamiento de datos personales sobre la mera base de que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical y de datos relativos a la salud o a la vida sexual. El tratamiento de dichos datos sólo podrá efectuarse en caso de que sea absolutamente necesario para una investigación determinada.

2. Se establecerán las salvaguardias pertinentes respecto de las operaciones de tratamiento de datos que puedan probablemente presentar riesgos para los derechos y las libertades de los interesados como, en especial, el tratamiento de perfiles de ADN, los datos biométricos, los datos de personas no sospechosas y la utilización de técnicas especiales de vigilancia o de nuevas tecnologías.

Principio 7: Información que debe recibir el interesado

1. El interesado será informado del hecho de que se están tratando datos que le conciernen, del tipo de datos implicados, de la identidad del supervisor o de su representante.

2. La información que debe recibir el interesado podrá aplazarse en la medida en que sea necesario para no poner en peligro el fin para el que se han recogido y tratado los datos.

Principio 8: Derecho de acceso a los datos y a su rectificación

1. El interesado tendrá derecho a obtener de la autoridad de control libremente, sin restricciones y con una periodicidad razonable y sin retrasos excesivos:

a) la confirmación de la existencia o inexistencia de tratamientos de datos que le conciernan.

b) la transmisión, en forma inteligible, de los datos objeto de tratamiento.

c) el conocimiento de la lógica implícita en todo tratamiento automático de datos que le concierna, al menos en el caso de las decisiones automáticas mencionadas en el principio 9.

2. El interesado tendrá derecho a:

a) la rectificación o, en su caso, la supresión de los datos.

b) la notificación a los terceros a quienes se hayan transmitido los datos de toda rectificación o supresión.

Principio 9: Decisiones individuales automatizadas

1. Toda persona tiene el derecho de no verse sometida a decisiones con efectos jurídicos sobre ella, o que le afecten de forma significativa, basadas únicamente en el tratamiento automático de datos destinados a evaluar determinados aspectos personales con ella relacionados.

2. Sin perjuicio de los otros principios, toda persona podrá verse sometida a una decisión del tipo mencionado cuando esta decisión esté autorizada por una ley.

Principio 10: Requisitos para la confidencialidad y seguridad del tratamiento

Principio 11: Requisitos para la transmisión de datos personales.

Principio 12: (Notificación y control previo)

1. Los Estados miembros identificarán las categorías de ficheros permanentes o *ad hoc* que presenten o puedan probablemente presentar unos riesgos específicos para los derechos y libertades de los interesados, que deben ser notificadas a la autoridad de control.

Principio 13: Responsabilidad del Supervisor respecto a los principios enunciados

Principio 14: Recursos judiciales y régimen de responsabilidad.

1. Toda persona podrá interponer un recurso judicial en caso de violación de los derechos garantizados por estos principios.

2. El interesado tendrá derecho a obtener compensación por todo daño sufrido a causa del tratamiento ilícito de los datos personales que le conciernan.

Principio 15: Supervisión

La observancia de los principios relativos a la protección de datos personales será controlada y garantizada por las autoridades públicas de control.

Otras novedades Normativas que afectan al tratamiento de datos personales

Proyecto de Ley de Medidas de Impulso de la Sociedad de la Información (LISI)

Durante el mes de abril de 2007 el Gobierno ha aprobado la remisión a las Cortes Generales del Proyecto de la Ley de Medidas de Impulso de la Sociedad de la Información, dentro del conjunto de medidas que integran el Plan 2006-2010 para el desarrollo de la Sociedad de la información y de convergencia con Europa y entre las Comunidades y Ciudades Autónomas.

Dentro de estas medidas, el Plan Avanza prevé la adopción de una serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y a garantizar los derechos de los ciudadanos en la Sociedad de la Información.

En esta línea, el Proyecto de Ley introduce innovaciones normativas que tienen el objetivo de impulsar la Sociedad de la Información en España y cubrir vacíos normativos existentes hasta ahora.

En concreto, se llevan a cabo una serie de modificaciones de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico y de la Ley de Firma Electrónica.

Desde la perspectiva de la protección de datos, el Proyecto implica una nueva obligación para determinado tipo de empresas.

En efecto, el proyecto impone a las grandes empresas (empresas con más de cien empleados o un volumen de operaciones superior a los seis millones de euros), que presten servicios al público considerados como de especial trascendencia económica (electricidad, agua y gas, telecomunicaciones), la obligación de facilitar un medio de interlocución telemática con sus clientes, que deberá estar basado en certificados reconocidos de firma electrónica (y especialmente en el DNI electrónico), y que permita a los clientes mantener relaciones de carácter contractual con la empresa, efectuar reclamaciones y ejercer sus derechos de acceso, rectificación, oposición y cancelación en materia de protección de datos.

Con el objeto de dar cobertura a la nueva obligación, se modifica la Ley de Ordenación del Comercio Minorista.

Modificación de la Ley Orgánica de Universidades

El 29 de marzo de 2007, el Congreso de los Diputados aprobó la modificación de la Ley Orgánica de Universidades. El proyecto fue aprobado en primera instancia por el Congreso el 14 de diciembre de 2006 y recibió el voto afirmativo de la Cámara Alta el 21 de marzo de 2007.

La modificación de la LOU pretende dotar de una mayor autonomía a las universidades españolas en su funcionamiento interno, en su administración y en el diseño de los títulos. La reforma incide también en el refuerzo de los mecanismos de rendición de cuentas ante la sociedad y de evaluación de la calidad.

Con el propósito de fomentar la modernización de las Universidades españolas, su especialización y su competitividad, la modificación de la LOU las dota de una mayor autonomía.

En lo que se refiere estrictamente al ámbito de la protección de datos personales, la Disposición Adicional Vigésimo Primera del texto se remite a la LOPD y habilita al Gobierno para que desarrolle los puntos pendientes previo informe de la AEPD:

> "1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.

> Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.
>
> 2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3[19].
>
> (…)
>
> 5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores"

Por otro lado, explícitamente se menciona el hecho de que no será necesario el consentimiento de los titulares de los datos para la publicación de las calificaciones obtenidas, clarificando así una cuestión que se ha planteado a las universidades en su condición de responsables de fichero:

> "3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.
>
> 4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación."

Fuente: www.Educaweb.com

Real Decreto 398/2007 de creación del Registro de Contratos de Seguro y Cobertura de Fallecimiento.

El Real Decreto, promulgado el 23 de marzo de 2007, desarrolla la Ley 20/2005, de 14 de noviembre, sobre la creación del Registro de contratos de seguro de cobertura de fallecimiento.

Crea el citado registro de naturaleza pública, dependiente del Ministerio de Justicia, y cuya gestión centralizada se llevará desde el Registro General de Actos de Última Voluntad de la Dirección General de los Registros y del Notariado.

La finalidad de este Registro es dar a conocer si una persona fallecida estaba asegurada con un seguro de cobertura de fallecimiento, ya que en muchas ocasiones por desconocimiento de los beneficiarios de estos seguros, se dejaban de percibir las cantidades correspondientes, y por lo tanto se veía frustrado el cobro de cantidades que legítimamente correspondían a determinadas personas. De ahí, por tanto, la importancia de la función social del Registro que se crea.

Desde el punto de vista de los datos personales, la norma regula detalladamente las características de los datos a comunicar por parte del Registro de Contratos de Seguros de cobertura de fallecimiento y ejercicio de derechos de acceso, rectificación, cancelación y oposición.

[19] Normas de acreditación para la pertenencia a comisiones de evaluación de acceso a los cuerpos de funcionarios docentes universitarios.

Agencia Española de Protección de Datos

Haremos por último una referencia a la actividad de la Agencia Española de Protección de Datos durante el periodo referido, resumiendo aquellos puntos que entendemos más relevantes:

- **La AEPD pone en funcionamiento el Sistema de Notificaciones Telemáticas a la Agencia, ´NOTA´**

  En el mes de septiembre de 2006, inició su funcionamiento el sistema NOTA para posibilitar las notificaciones telemáticas a la Agencia.

  El sistema, aprobado mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006 (BOE núm. 181 de 31 de julio de 2006), permite a los responsables de ficheros llevar a cabo las siguientes operaciones:

  - Cumplir con la obligación de notificación de creación y modificación de los ficheros a la AEPD de forma telemática mediante el uso de una herramienta que informa acerca de los requerimientos de la notificación y guía al usuario para su cumplimentación. En este sentido, el sistema incluye formularios previamente cumplimentados para los casos que generalmente son más utilizados por los responsables de ficheros.
  - Presentar las notificaciones a través de Internet mediante el uso de firma electrónica o utilizando otros soportes (digital o papel).
  - Conocer el estado de tramitación de las notificaciones remitidas a través de Internet, mediante certificado de firma electrónica o mediante el código de envío generado por el formulario electrónico.
  - Consultar el contenido completo de la inscripción de sus ficheros en la web de la AEPD.

  Además, se han incluido los formatos y especificaciones para aquellos responsables de ficheros y desarrolladores que trabajen con aplicaciones propias de gestión de datos y que de esta forma pueden ser integradas con el sistema NOTA.

- **El Consejo de Ministros nombró mediante Real Decreto a D. Artemi Rallo Lombarte**

  El 23 de febrero de 2007 el Consejo de Ministros aprobó el nombramiento de D. Artemi Rallo Lombarte como nuevo Director de la Agencia de Protección de Datos., sustituyendo en el cargo a D. José Luis Piñar Mañas, quien ha ocupado hasta su nombramiento como Director el cargo de Director General del Centro de Estudios Jurídicos.

  La Comisión Constitucional del Congreso de los Diputados aprobó por unanimidad su candidatura tratándose de la primera vez que, en España, el director de la Agencia española de Protección de datos se somete a este trámite previo en el Congreso, en cumplimiento del artículo 2.3 de la Ley 5/2006, de 10 de abril, de Regulación de los conflictos de intereses de los miembros del Gobierno y de los Altos Cargos de la Administración General del Estado.

- **Actuaciones AEPD**

  Se destacan, por último, algunas de las actuaciones de la AEPD que han tenido repercusión en los medios de comunicación durante el periodo referido.

  - Sancionan a dos hospitales de la Generalidad de Cataluña por utilizar historiales clínico**s para comprobar el uso del catalán**

La AEPD sancionó[20] a dos hospitales catalanes a pagar 60.000 euros cada uno por no custodiar debidamente sus ficheros.

El incumplimiento se produjo a raíz de la puesta en marcha de un programa piloto de la Generalidad de Cataluña con el objeto de conocer el uso del catalán en la Sanidad Pública.

Para ello se cedieron historias clínicas a una empresa privada sin el consentimiento de los pacientes.

La AEPD ha sancionado a los centros sanitarios de San Rafael y a la Clínica Plató Fundación Privada por incumplimiento del artículo 10 LOPD al haber quedado acreditado que permitieron el acceso del Centro Informático de Estadísticas y Sondeos S.A. a los datos contenidos en los historiales clínicos que custodiaban (datos especialmente protegidos).

- Un trabajador de CC.OO. filtra datos de 20.000 personas al usar el eMule

La sanción[21] se produce como consecuencia de una denuncia que data de 03/05/2004. En esa fecha la Agencia tuvo conocimiento de los resultados obtenidos por la Comandancia de Orense de la Dirección General de la Guardia Civil, Unidad Orgánica de Policía Judicial, en los rastreos efectuados a través de Internet para la detección de hechos delictivos. En concreto se denuncia la localización de dos ficheros, localizados mediante el buscador "emule" que contienen datos de carácter personal relativos a funcionarios de distintas Administraciones Públicas que habían solicitado o participado en Cursos de Formación organizados por la Confederación Sindical de Comisiones Obreras (en lo sucesivo CCOO). Estos ficheros contenían datos de una gran cantidad de personas, con indicación de nombre, apellidos, domicilio, teléfono y lugar de trabajo, entre otros.

La AEPD ha sancionado con una infracción grave a la Federación de Servicios y Administraciones públicas de CCOO, de la que salieron los datos, por incumplir su deber de custodiarlos.

La falta de control sobre el software utilizado por los empleados de las organizaciones y los riesgos derivados de los mismos se producen con relativa frecuencia. De hecho, la AEPD tiene abiertas otras 16 investigaciones por hechos similares.

Agencias Autonómicas de Protección de Datos

A lo largo del periodo que abarca el Informe, por parte de las agencias autonómicas de protección de datos se han promulgado distintas normas y dictámenes entre los que citamos la siguiente instrucción de la Agencia de Protección de Datos de la Comunidad de Madrid:

- Instrucción 1/2007 de la Agencia de Protección de Datos de la Comunidad de Madrid sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones públicas de la Comunidad de Madrid. En este sentido, la Instrucción reconoce el precedente de la Instrucción 1/2006 AEPD, para la regulación de este aspecto que en muchos casos implicaba situaciones y obligaciones no definidas para el responsable del fichero y los titulares de los datos. En relación con la Instrucción AEPD 1/2006,

[20] RESOLUCIÓN AEPD: R/00010/2007
[21] RESOLUCIÓN AEPD: R/00060/2007

la Agencia de Protección de Datos de la Comunidad de Madrid destaca en la Exposición de Motivos de la Instrucción 1/2007, que la norma de la agencia estatal se aplica únicamente al tratamiento de las imágenes de personas físicas identificadas o identificables realizados con fines de vigilancia. La norma autonómica, recoge por su parte diferentes supuestos de legitimación, haciendo una mención más genérica a la posibilidad recogida para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades de la Comunidad de Madrid.

La Agencia Vasca de Protección de Datos, por su parte, ha emitido distintos dictámenes relevantes en el periodo analizado como las siguientes[22]:

- Dictamen CN 12/2006 de la Agencia Vasca de Protección de Datos. Cesión de datos de un ayuntamiento a una de sus juntas administrativas
- Dictamen CN 23/2006 de la Agencia Vasca de Protección de Datos. Medidas de garantía de confidencialidad de datos tributarios en la relación de un Departamento de Hacienda con el Tribunal Vasco de Cuentas
- Dictamen CN 18/2006 de la Agencia Vasca de Protección de Datos. Cesión de datos del fichero al que se refiere la disposición adicional 2ª de la ley 2/2004

Creación de nuevos organismos de control a nivel autonómico

Dentro de la labor de velar por el cumplimiento de la legislación de protección de datos y el respeto a los derechos fundamentales implicados, la AEPD encuentra, en aquellas comunidades autónomas donde han sido creadas agencias de protección de datos personales, un importante apoyo en lo que se refiere al control de los datos personales manejados por las Administraciones Públicas.

Actualmente, solo en las Comunidades Autónomas de Madrid, País Vasco y Cataluña se han creado Agencias de Protección de Datos autonómicas, pero durante el periodo de tiempo que abarca este informe, hemos asistido a los primeros pasos para su creación en otras comunidades españolas:

- **Aragón.** La Ley Orgánica 5/2007, de 20 de abril, de Reforma del Estaturo de Autonomía de Aragón, en su artículo 75 establece que en el ámbito de las competencias compartidas, la Comunidad Autónoma de Aragón ejercerá el desarrollo legislativo y la ejecución de la legislación básica desarrollando políticas propias en Protección de datos de carácter personal, que, en todo caso, incluye la regulación, inscripción y el tratamiento de los mismos, el control de los ficheros creados o gestionados por las instituciones públicas de Aragón y, en especial, la creación de una Agencia de protección de datos de Aragón
- **Navarra.** Ley para la implantación de la Administración Electrónica de Navarra.

  El 9 de mayo de 2007 se ha publicado la LEY FORAL 11/2007, de 4 de abril, para la Implantación de la Administración Electrónica en la Administración de la Comunidad Foral de Navarra.

  Esta Ley, además de fomentar la introducción de las Tecnologías de la Información, de forma que se garanticen los derechos de los ciudadanos, en su Disposición Adicional Segunda establece que la implantación de la Administración electrónica en ningún caso supondrá exención o debilitamiento de los deberes de la Administración de la Comunidad Foral de Navarra y de sus organismos públicos en orden a la protección de los datos personales de los

[22] Fuente: Web de la Agencia Vasca de Protección de Datos: www.avpd.euskadi.net

ciudadanos. En este sentido, se habilita al Gobierno de Navarra para promover mediante Decreto Foral la creación de la Agencia de Protección de Datos Personales de Navarra.

- **Otras iniciativas:** En una fase anterior se encuentran iniciativas en comunidades como Andalucía o Valencia, en las que durante este periodo han surgido voces cualificadas defendiendo la necesidad de Agencias autonómicas. En el caso de Valencia, actualmente dispone de un modelo de gestión delegada, la actual Unidad administrativa de registro de ficheros (UARFI), embrión de la que previsiblemente será Agencia Valenciana de Protección de Datos.

autelsi

C/. Lagasca, 36 - 2º G • 28001 Madrid • Teléfono 91 432 32 20 • Fax 91 432 32 21
autelsi@autelsi.es