AGENCIA DE PROTECCIÓN DE DATOS

MEMORIA 1999

MEMORIA DE 1999 - PRESENTACIÓN

Un año más la Agencia de Protección de Datos, a través de su Memoria, rinde cuentas ante los ciudadanos de la labor desarrollada durante el ejercicio anterior, en el presente caso la llevada a cabo en el año 1999.

Como es habitual, la presente Memoria se adecua en cuanto a su estructura, a la marcada por el art. 2 del Real Decreto 428/1993, de 26 de marzo que aprobó el Estatuto de la APD, complementándose con otros datos y documentos que se consideran de interés para un mejor conocimiento de la actividad de la Agencia y de las tendencias legales y doctrinales desarrolladas en nuestro país, en el resto de los miembros de la Unión Europea y a nivel de la propia Comunidad.

El año 1999 cierra a mi juicio una etapa en la protección del derecho a la intimidad de los ciudadanos en cuanto al tratamiento de sus datos, por cuanto que a finales del mismo, se ha publicado una nueva Ley Orgánica de Protección de Datos Personales que derogando la LORTAD prevé su entrada en vigor el día 14 de enero de 2000. También en este año comienza a exigirse el cumplimiento de las medidas de seguridad para los ficheros ya creados conforme a las previsiones contenidas en el Real Decreto 994/1999, de 11 de junio, que aprobó el Reglamento de Medidas de Seguridad.

Si bien para incorporar en su totalidad la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, a nuestro derecho interno, era suficiente una reforma parcial de la Ley Orgánica 5/1992, de 29 de octubre, y en tal sentido el Gobierno remitió al Congreso de los Diputados para su tramitación un Proyecto de Ley de reforma parcial de la LORTAD, los diversos grupos parlamentarios decidieron acometer la tarea de redactar una nueva Ley que estuviera por encima del nivel de protección que diseña la Directiva comunitaria. Así es aprobada definitivamente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal por el Congreso de los Diputados en segunda lectura con fecha 25 de noviembre de 1999, incorporando diversas enmiendas introducidas durante la tramitación en el Senado. Esta Ley es la que corresponde aplicar a partir del 14 de enero de 2000.

En 1999 ha sido, una vez mas, tarea prioritaria de la APD dar a conocer mejor la Ley y sus exigencias de forma que se facilite así su cumplimiento, siguiendo la línea que me marqué al tomar posesión del cargo de Director de la Agencia. En este orden de preferencia se ha seguido con los planes de inspecciones sectoriales de oficio.

Durante 1999 se han iniciado y terminado las inspecciones de oficio a la Agencia Estatal de Administración Tributaria, a la Dirección General de Tráfico, al Sector de Investigación Privada, y a los Hospitales, Psiquiátrico de Foncalent y Militar Gómez Ulla; Igualmente se ha iniciado en este año un plan de inspección de oficio específico en el Sector de las Telecomunicaciones.

De todos ellos cabe destacar este último por cuanto que, las inspecciones ya realizadas al sector respecto del cumplimiento de la LORTAD, se ven ampliadas ahora en relación con el cumplimiento de la nueva normativa de protección de la intimidad en el sector de las telecomunicaciones, (art. 50 de la Ley General de Telecomunicaciones y el Reglamento por el que se desarrolla el Título III de esta Ley que traspone a nuestro derecho interno la Directiva 97/66/CE, del Parlamento Europeo y del Consejo).

Como complemento de estas actuaciones y para mejor difundir el conocimiento de la Ley, la APD ha organizado diversos actos entre los que merecen destacarse las Jornadas sobre "Contratación Electrónica, Privacidad e Internet", que se desarrollaron en Mérida, los días 1 y 2 de julio, en colaboración con el Centro de la Universidad de Educación a Distancia de Mérida. A la hora de elegir esta sede para la celebración de las referidas jornadas se tuvo en cuenta tanto el alto nivel académico del Centro coorganizador como la conveniencia de presencia de la Agencia en las diversas Comunidades Autónomas. Al propio tiempo se organizan otros actos con la misma finalidad de aproximación de la APD a los ciudadanos y a los titulares de ficheros de datos, como es el caso de la presentación de la anterior Memoria que se llevó a cabo en el Consejo Superior de Cámaras de Comercio, Industria y Navegación, así como la presentación del libro editado por la Agencia conteniendo todas las ponencias de la XX Conferencia de Autoridades de Protección de Datos, que se llevó a cabo en el Colegio de Abogados de Madrid. Con igual fin, como Director de la APD, participé como conferenciante en casi una treintena de seminarios, jornadas y cursos sobre diversos aspectos de la protección de datos que organizaron distintas entidades tanto públicas como privadas.

Como en anteriores ocasiones he comparecido ante la Comisión Constitucional del Congreso de los Diputados, a petición propia, para informar sobre la Memoria del anterior ejercicio así como para dar respuesta a las peticiones de los Grupos Parlamentarios. También he tenido ocasión de comparecer ante la Comisión Especial sobre Redes Informáticas del Senado. Este tipo de comparecencias del Director de la APD ante los representantes de los ciudadanos son, a mi juicio, de suma utilidad ya que por un lado posibilitan a estos un mejor conocimiento de la labor desarrollada por la APD y les permiten formular sugerencias para un mejor funcionamiento de la Agencia. De otro lado se establece así el control parlamentario directo de la APD, lo que supone una garantía adicional a la establecida por la Ley de la independencia que debe guiar todas las actuaciones del Director de la misma.

El interés de los ciudadanos por preservar su intimidad ha ido a mi juicio en aumento durante 1999. Así lo acreditan el alrededor de quince mil consultas formuladas a la Agencia durante este periodo, en nivel similar con el año anterior, pero que el presente se ve aumentado con las más de quinientas mil consultas a la página web en internet de la APD.

Ha sido asimismo mayor el número de denuncias, de inspecciones realizadas en ficheros públicos y privados, y de procedimientos de tutela de derechos y sancionadores tramitados. También se ha visto incrementado el montante total de multas impuesto que han alcanzado la cifra de 1.571 millones de pesetas. De todo lo anterior, a mi juicio resulta más

significativo el aumento experimentado por las denuncias y procedimientos seguidos contra las Administraciones Públicas, claro exponente de la concienciación de los ciudadanos de que también aquellas deben respetar su derecho a la intimidad. De igual forma puede constatarse en la presente Memoria, la mayor complejidad que va adquiriendo la protección de la intimidad debido al desarrollo de nuevas tecnologías que permiten la obtención de perfiles personales, lo cual supone una mayor intromisión en facetas mas íntimas del individuo.

Un hecho significativo que merece la pena mencionar, es el efecto producido por el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio. El Reglamento prevé una exigencia escalonada de los tres niveles de medidas de seguridad que establece, disponiendo que las medidas de nivel básico, es decir aquellas exigibles a todo fichero de datos, entraran en exigencia el 26 de diciembre de 1999 (luego prorrogado al 26-3-2000). Ello ha supuesto un auténtico colapso de la APD en el último mes del año, debiendo recurrir a medidas extraordinarias, contratando servicios externos aunque prestados en la propia sede de la Agencia, para dar respuesta al imprevisible aumento en la declaración de ficheros. A pesar de que el Reglamento de Medidas de Seguridad no exige ninguna declaración inmediata complementaria de la que ya se hubiese realizado, de lo que informó la Agencia entre otros medios a través de su página web en internet, la exigencia de implantación de medidas de seguridad ha tenido el efecto beneficioso indirecto de que se conociera la obligación derivada de la Ley, de declaración de los ficheros ante la Agencia.

En el ámbito internacional la actividad desarrollada durante el año 1999 ha sido muy importante y ha marcado una clara tendencia creciente. Cabe destacar las reuniones de trabajo llevadas a cabo con delegaciones de protección de datos de Japón y de la República Checa en nuestra sede, exponente del prestigio que la legislación española y la actuación de la APD está adquiriendo a nivel internacional. También cabe señalar la reunión de trabajo mantenida con el Vicepresidente de la "Autorite Garante Italiana" al que recibimos en el mes de noviembre, dando lugar a un fructífero cambio de impresiones. De igual modo el Presidente de la Agencia Portuguesa, invitado por la APD estuvo presente en las Jornadas de Mérida, interviniendo en el acto de clausura de las mismas y posibilitando un mejor conocimiento mutuo de nuestras respectivas legislaciones e inicio de una colaboración mas estrecha.

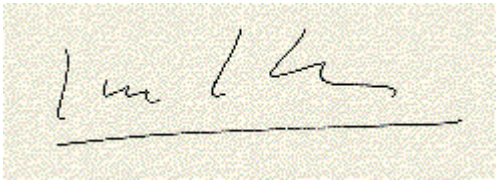
De las actividades habituales en el ámbito internacional cabe destacar la participación en las reuniones celebradas por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales establecido en el art. 29 de la Directiva 95/46/CE, integrado por las Autoridades de Control de todos los Países miembros de la Unión Europea. También la asistencia a las reuniones del Grupo de Proyectos sobre Protección de Datos (CJ-PD) del Consejo de Europa, a las de Autoridades Comunes de Control establecidas en los Convenios de Schengen y Europol, y a las del Grupo de Protección de Datos en Telecomunicaciones (Grupo de Berlín).

Asimismo, la Agencia estuvo presente en la Conferencia de Primavera de Comisionados Europeos de Protección de Datos celebrada en Helsinki en el mes de abril, presentando tres ponencias y en la Conferencia Internacional de Autoridades de Control de Protección de Datos celebrada en Hong Kong S.A.R. en el mes de septiembre, aunque personalmente no asistí a esta última por las razones que se exponen en el apartado correspondiente de esta Memoria.

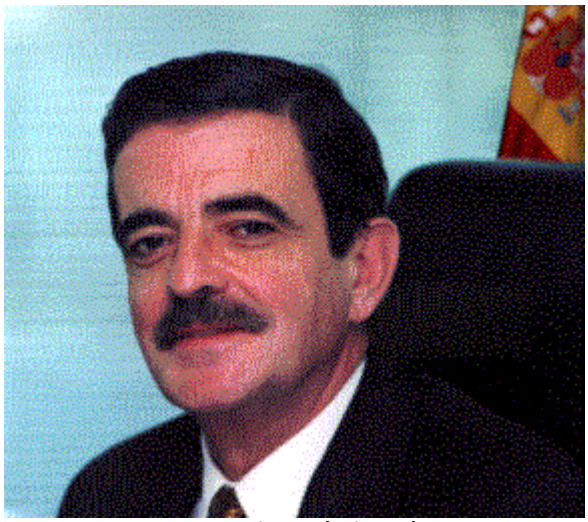
En definitiva deseo que pueda constatarse en esta Memoria, que invito a su lectura reposada, la creciente y entusiasta actividad que se ha podido realizar gracias a la entrega y profesionalidad de todos los que trabajan en la APD y que realizan gustosos, un constante esfuerzo por mejor servir a los intereses de los ciudadanos españoles.

Madrid, mayo de 2000

El Director de la Agencia de Protección de Datos.



Juan Manuel Fernández López.



Juan Manuel Fernández López.

MEMORIA DE 1999 - FUNCIONAMIENTO DE LA AGENCIA

I. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

De conformidad con lo establecido en el artículo 36 h) de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD) corresponde a la Agencia de Protección de Datos informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica, por su parte, el artículo 5 en sus apartados a) y b), concreta este precepto estableciendo que la Agencia informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica así como cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica.

A lo largo de 1999 se han sometido al parecer de la Agencia de protección de Datos, para su informe preceptivo, un total de 35 disposiciones, lo que supone un muy sensible incremento del 59 % respecto de los remitidos en 1998 (un total de 22).

Este incremento se debe, en gran medida al hecho de que durante el año 1999, y en línea con la voluntad manifestada por el Director de la Agencia en su comparecencia ante la Comisión Constitucional del Congreso de los Diputados de 27 de mayo de 1997, se ha incrementado el número de normas sectoriales de desarrollo de la Ley Orgánica, siendo especialmente de reseñar que han sido informadas por la Agencia de Protección de Datos la totalidad de las disposiciones de creación o modificación de ficheros promovidas por la Administración General del Estado durante el año 1999.

Entre las disposiciones informadas por esta Agencia de Protección de Datos, debe destacarse por su especial relevancia las siguientes:

- El informe sobre el anteproyecto de Ley sobre medidas de control de sustancias químicas susceptibles de desvío para la fabricación de armas químicas en aplicación de la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas, hecha en París el 13 de enero 1993.

- El informe sobre la propuesta de norma con rango de Ley para la actualización de la regulación de la Central de Información de Riesgos del Banco de España (CIRBE).

- El informe al anteproyecto de la Ley de Creación de la Agencia Catalana de Protección de Datos.

- El informe sobre el Anteproyecto de Ley sobre firma electrónica, aprobado posteriormente por el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

- Informe referente al Anteproyecto de Ley de Medidas Fiscales, Administrativas y del Orden Social, de acompañamiento a la Ley de Presupuestos de 2000.

- Los informes solicitados en cumplimiento de lo dispuesto en el artículo 69.3, párrafo tercero, del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

II. CONSEJO CONSULTIVO

- El Consejo Consultivo, previsto en el artículo 37 de la LO 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, y en los artículos 18 a 22 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos, se configura como órgano colegiado de asesoramiento del Director del Ente Público, cuyos cometidos se centran en emitir informe en todas las cuestiones que le someta el Director de la Agencia y formular propuestas en temas relacionados con las materias de competencia de ésta.

* Su composición, está integrada por los siguientes miembros:

* Presidente:

* D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos.

* Vocales:

* D. Carlos Navarrete Merino, Diputado propuesto por el Congreso de los Diputados

* Dª. Rosa Vindel López, Senadora propuesta por el Senado

* D. Álvaro de la Cruz Gil, Vocal de la Administración Local propuesto por la Federación Española de Municipios y

Provincias.

* D. Eloy Benito Ruano, Vocal propuesto por la Real Academia de Historia

* D. Antonio Pérez Prados, Vocal propuesto por el Consejo de Universidades.

* D. Alberto Perales Albert, Vocal propuesto por el Consejo de Consumidores y Usuarios.

* Dª. Elena Gómez del Pozuelo, Vocal del sector de ficheros privados propuesta por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.

* Secretaria:

* Dª. Sofía Perea Muñoz, Secretaria General de la Agencia de Protección de Datos.

* El estricto cumplimiento de los artículos antes referenciados exigiría la designación del Vocal representante de las Comunidades Autónomas, propuesto mediante acuerdo adoptado por mayoría simple de éstas.

* Entre los temas objeto de estudio y análisis por el Consejo Consultivo pueden destacarse los siguientes:

* Análisis de situación del proyecto de Ley Orgánica para la transposición de la Directiva 95/46 CE .

* Trabajos llevados a cabo por la Comisión designada por el Ministerio de Justicia para la regulación de las bases de datos de ADN

* Transferencias Internacionales, con especial referencia al caso Reader's Digest.

* Convocatoria de la tercera edición del Premio Protección de Datos Personales, así como fallo del mismo.

* Análisis de la situación del proyecto de Reglamento de Medidas de Seguridad. Medidas a adoptar por la Agencia de Protección de Datos para su mejor conocimiento e implantación.

* Recomendaciones de la Agencia de Protección de Datos para una mejor adecuación a la ley de los ficheros de las policías locales.

* Situación de las declaraciones de ficheros de los Ayuntamientos. Medidas a adoptar para su mejor cumplimiento.

* Memoria de la Agencia de Protección de Datos del ejercicio 1998.

* Responsabilidad del anunciante que alquila una base de datos asignándose por contrato que ésta proviene de fuentes accesibles al público.

* Informe de la Vocal propuesta por el Consejo Superior de Cámaras de Comercio, Industria y Navegación de los problemas que se plantean ante la entrada en vigor de la Directiva 95/46 CE para las empresas dedicadas a Seguros, registros de Morosos y Hospitales Privados.

* Reuniones llevadas a cabo por el Director de la Agencia con gerentes de las Universidades de Cataluña y criterios a seguir para asegurar el cumplimiento de la LO 5/92.

* Actuaciones llevadas a cabo para una mayor publicidad y conocimiento de la ley y concienciación de la obligación de cumplirla.

* Problemática de la aplicación de la nueva Ley Orgánica de Protección de datos personales.

* Balance del año 1999.

III. REGISTRO GENERAL DE PROTECCIÓN DE DATOS

1. **INTRODUCCIÓN**

El Registro General de Protección de Datos, en cumplimiento del artículo 13 de la LORTAD, es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con la finalidad de que los ciudadanos tengan la posibilidad de ejercitar los derechos de información, acceso, rectificación y cancelación de sus datos, pudiendo conocer a tal fin la siguiente información:

- la existencia de ficheros automatizados
- la finalidad de sus tratamientos
- la identidad del responsable del fichero

La Ley ha desechado el establecimiento de la autorización previa a la inscripción constitutiva en un registro con la pretensión de evitar una perniciosa burocratización, por lo tanto, la inscripción en el Registro General de Protección de Datos es declarativa. Por otra parte, la consulta es pública y gratuita y serán objeto de inscripción en el mismo, tanto los ficheros automatizados de los que sean titulares las Administraciones Públicas, como los ficheros automatizados de titularidad privada. También serán objeto de inscripción las autorizaciones de transferencias internacionales de datos a países que no proporcionen un nivel de protección equiparable al que presta la ley, y los códigos tipo.

En el Registro quedan inscritas todas las versiones por las que ha pasado la inscripción de un fichero, con la posibilidad de consulta automatizada al histórico.

Los principios de la inscripción de ficheros se pueden resumir en los siguientes puntos:

- El responsable del fichero deberá efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos.

- La inscripción de un fichero de datos no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la Ley.

- La notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.

- La notificación de los ficheros al Registro supone, una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quienes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, rectificación y cancelación.

2. **LÍNEAS DE ACTUACIÓN**

A lo largo del año 1999 las solicitudes recibidas en el Registro General, se han visto incrementadas en más de un 50% respecto de las del año anterior. Asimismo, los expedientes tramitados de Autorización de Transferencia Internacional han tenido un incremento superior al 25**%**. No obstante, la gestión de todo tipo de movimientos referentes a la inscripción de ficheros ha seguido siendo significativamente fluida, ya que el tiempo medio de respuesta desde que una notificación tiene entrada en la Agencia hasta que se emite la correspondiente resolución de inscripción al responsable del fichero no ha superado los siete días de media.

Dentro de las actividades propias del Registro se ha tramitado, a instancia de los responsables de ficheros, la inscripción de 5.201 nuevos ficheros, se han modificado 2.753 inscripciones y se han suprimido 1.479, lo que supone un total de 9.433 operaciones.

Las actuaciones más destacables del Registro durante el año 1999, son las siguientes:

2.1. **ENTRADA EN VIGOR DE LA NUEVA LEY 15/1999 Y LA NOTIFICACIÓN DE INSCRIPCIÓN**

La entrada en vigor de la nueva Ley 15/1999, no va a suponer cambios sustanciales a los efectos de lo previsto en sus artículos 20, 25 y 26, que ahora regulan la creación de ficheros y la obligación de notificarlos.

En los artículos 20 y 26 se establece para los ficheros de titularidad privada y pública respectivamente, la información que, como mínimo, debe figurar en la notificación. La única novedad respecto de las previsiones que contemplaba la LORTAD, es la relativa a las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

El artículo 39 de la nueva Ley contempla al Registro General de Protección de Datos, como órgano integrado en la Agencia de Protección de Datos. El artículo 37, al igual que el artículo 38 de la LORTAD, atribuye entre otros, el principio de publicidad de los ficheros, a cuyo efecto exige que se publique la relación de los mismos. Por lo tanto, y en el escenario de la declaración de ficheros, a los efectos de publicidad de los mismos, se puede considerar que el concepto al que se refiere la Directiva en su artículo 21 de *Publicidad de los tratamientos,* es equiparable al concepto utilizado por la nueva Ley española en su artículo 37.j) *Velar por la publicidad de la existencia de los ficheros automatizados.* Este contenido también coincide plenamente con lo dispuesto en la LORTAD en su artículo 36.j).

No obstante, sería interesante hacer algunas consideraciones en relación con los conceptos de *tratamiento* y *fichero* utilizados por la nueva Ley.

Tanto en la nueva Ley como en la Directiva existen definiciones de los dos conceptos en idénticos términos. A efectos prácticos se puede considerar que:

- La creación de un fichero exige, con carácter previo, la realización de diferentes tratamientos de datos personales: grabación, depuración, etc.
- Un tratamiento de datos supone la realización de cualquier operación o conjunto de operaciones sobre datos que deben encontrarse estructurados, ser accesibles y estar almacenados en ficheros.

Idéntica similitud de conceptos puede encontrarse en los modelos que al efecto se publicaron en la Resolución de 22

de junio de 1994 (B.O.E. nº 149 de 23 de junio de 1994). Así, se puede observar que la denominación del cuestionario aparece como "MODELO DE NOTIFICACIÓN DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL" *Creación, Modificación y Supresión de ficheros.*

En el mismo sentido, en las Instrucciones para cumplimentar el modelo en el apartado de *"Glosario de Términos*" se define a efectos de comprensión y cumplimentación del mismo:

Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de UN TRATAMIENTO AUTOMATIZADO, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

De lo anteriormente expuesto, se desprende que el término "tratamiento de datos" contenido en la nueva Ley no difiere a los efectos de inscripción, sustancialmente, del término "fichero" de la LORTAD, siendo el segundo más comprensible y de más larga tradición en nuestro idioma.

Con la finalidad de adecuar el Registro General de Protección de Datos a las nuevas previsiones legales, a lo largo de este año, se ha realizado el estudio y desarrollo de los sistemas de información necesarios para implantar aquéllas, con la previsión que estén operativos en el primer semestre del año 2000.

Asimismo, se ha desarrollado el proyecto que permitirá instrumentalizar la notificación de ficheros para su inscripción en el Registro General a través de Internet.

Como resultado de estas actividades se han definido nuevos modelos de notificación de ficheros lo que ha implicado el desarrollo de nuevas aplicaciones informáticas así como la adecuación de las actuales a las nuevas necesidades funcionales y legales. Estos cambios legales supondrán la modificación del contenido de la notificación, en los siguientes aspectos formales:

* Aparece un nuevo apartado de Encargado del Tratamiento.
* Se modifica el apartado de Medidas de Seguridad.
* En el apartado de Origen de los Datos, se incorpora el subapartado *Fuentes accesibles al público,* con los siguientes tipos:
- Censo promocional.
- Guías de servicios de telecomunicaciones.
- Listas de personas pertenecientes a grupos profesionales.
- Diarios y boletines oficiales.
- Medios de comunicación.
* Se actualiza el apartado *datos sensibles,* ampliando la tipificación de pertenencia a sindicatos y adecuándolo a los nuevos supuestos previstos en el artículo 7.
* Se incluyen, en el apartado de Transferencias Internacionales, los nuevos supuestos de excepciones a la norma general previstos en el artículo 34 de la Ley 15/1999.

Por otro lado, como la Agencia dispone de una página Web en Internet, que entre otra información incluye los modelos de formularios de declaración de ficheros, es frecuente que los responsables de los mismos que consultan estas pági - nas, soliciten la declaración de ficheros a través de Internet. Esta cirunstancia ha puesto de manifiesto la necesidad de permitir la notificación de ficheros a través de la Red.

Todo ello ha supuesto, a lo largo de este año, realizar los trabajos precisos que permitan cumplir los principios de calidad y eficiencia en los procedimientos de inscripción, lo que ha supuesto la realización de las siguientes tareas:

- Modificar los modelos de declaración de ficheros.
- Facilitar la declaración segura de ficheros vía Internet.
- Modificar la estructura de la base de datos del Registro y de las aplicaciones de forma que permita la adaptación a la nueva Ley y a los cambios que de ella han surgido.

2.2. **INSCRIPCIONES SECTORIALES**

El Director de la Agencia ha seguido manteniendo diversas reuniones con responsables de ficheros para el análisis de su situación específica en relación con la declaración de ficheros y la protección de datos personales, con el objeto de concienciarles sobre las obligaciones y responsabilidades en esta materia, así como de la conveniencia de realizar códigos tipo. Entre ellas, se pueden resaltar por su interés:

- Declaraciones de ficheros en el marco de la Ley de Prevención de Riesgos Laborales.

- Declaraciones de ficheros en el ámbito de Internet.

- Declaraciones de ficheros en relación con la entrada en vigor del Reglamento de Seguridad.

- Declaración de ficheros relacionados con empresas matriz y las filiales del grupo.

- Las transferencias internacionales y la tramitación de las correspondientes autorizaciones.

2.3. **INSCRIPCIONES DE FICHEROS PÚBLICOS**

Con el objetivo de concienciar a los responsables de ficheros de las Administraciones Públicas, a lo largo del año se han mantenido diversas reuniones y se han realizado requerimientos a los siguientes órganos:
- Administración General del Estado: Reuniones con representantes de las Secretarías Generales Técnicas y unidades informáticas.
- Administración Autonómica: Reuniones con representantes de las unidades informáticas responsables de ficheros.
- Administración Local: Reuniones con Federaciones de Municipios, Diputaciones, unidades de coordinación de entes locales del Ministerio de Administraciones Públicas.

Los aspectos que se han tratado, en líneas generales, son los siguientes:

- Revisión de la inscripción actual, en relación con las medidas de seguridad,
- Determinación de sistemas informáticos con datos personales que no han sido inscritos,
- Inscripción de ficheros que suponen tratamientos de datos por más de un responsable.
- Propuesta de elaboración y distribución de normas y recomendaciones para los usuarios y responsables de sistemas que utilicen ficheros con datos personales.

3. **NOTIFICACIÓN DE FICHEROS: DERECHO NACIONAL APLICABLE**

Con la entrada en vigor de la Directiva, se han producido una serie de consultas y dudas de los responsables de ficheros en relación con la territorialidad de los mismos y su declaración a efectos de inscripción.

El avance de las tecnologías implica, en estos momentos, la posibilidad de realizar tratamiento de datos1, sin que sea determinante la ubicación de los soportes informáticos (ficheros); por lo tanto, podrían quedar sin contenido los derechos de los ciudadanos ante un uso indebido en el tratamiento de sus datos cuando el lugar de ubicación de los ficheros residiera fuera del territorio español.

La informática permite almacenar datos en ficheros, pero aún es más importante la facilidad con la que posibilita el acceder a ellos en apenas segundos y tratar la información en tiempo real, por distante que sea el lugar de la ubicación de los ficheros. Estas facilidades tecnológicas no deben menoscabar los derechos de los ciudadanos ante el tratamiento de sus datos.

La aproximación de las legislaciones nacionales relativas al tratamiento de datos personales, no debe conducir a una disminución de la protección que garantizan.

Los principios de protección de datos deben aplicarse a todos los tratamientos de datos personales y para evitar que una persona sea excluida de la protección, es necesario que todo tratamiento de datos efectuado en la Unión Europea, sea sometido a la aplicación de la legislación de algún Estado.

El establecimiento, en territorio español, de una actividad que conlleve un tratamiento de datos, deberá cumplir las obligaciones impuestas por el Derecho español2.

Los procedimientos de notificación tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características siendo una de las funciones más importantes de la Autoridad de Control la de contribuir a la transparencia de los tratamientos de datos efectuados en un Estado Miembro.

La Ley 15/1999, en transposición de los artículos 4 y 18 de la Directiva ha previsto, en el ámbito de aplicación, establecido en su artículo 2, que se regirá por dicha Ley todo tratamiento de datos de carácter personal:

- Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

- Cuando el responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

- Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español salvo que tales medios se utilicen únicamente con fines de tránsito.

Se considera necesaria la notificación a efectos de inscripción, en el Registro General de Protección de Datos, de los tratamientos de datos que se efectúen en un establecimiento en España que implique el ejercicio efectivo y real de una actividad, con la finalidad de conseguir los siguientes objetivos:

- Transparencia de los tratamientos de datos.

- Identificación del responsable o representante, en su caso.

- Facilitar a los ciudadanos una dirección en España para poder ejercitar sus derechos.

- Garantizar al máximo los derechos de los ciudadanos ante un tratamiento de datos, que se verían seriamente

mermados si tiene que ejercer sus derechos ante el responsable del fichero en otro país.

Será indiferente donde se encuentren ubicados los ficheros en los que se almacenan los datos. A efectos de inscripción, tendrán que declarar, las transferencias internacionales que efectúen, así como la ubicación del fichero, en un territorio diferente del español.

Las entidades domiciliadas en terceros países3 que pretendan tratar datos en España, en virtud del artículo 5.1.e) de la Ley 15/1999, vendrán obligadas a designar, con carácter previo al comienzo de su actividad de tratamiento de datos personales en territorio español, un representante en España.

Por lo tanto, en el nuevo modelo de declaración, se deberá consignar el nombre del país donde resida el responsable del fichero, en caso de que este no sea España. Si se trata de un país que no pertenezca a la Unión Europea se deberán cumplimentar obligatoriamente los datos de su representante en España en el apartado de *Servicio o Unidad de Acceso*, ya que los derechos de oposición, acceso, rectificación y cancelación serán facilitados por aquél, para lo que deberá notificar, a efectos de inscripción, la dirección del establecimiento en España4, con la finalidad de que el Registro General de Protección de Datos pueda proporcionar dicha dirección a los afectados cuando éstos la soliciten.

En caso de que los ficheros se vayan a ubicar o se vaya a realizar tratamientos de datos en un tercer país, además de cumplir con las notificaciones correspondientes a efectos de inscripción, deberán solicitar la autorización de transferencia internacional o declarar en su caso dicha transferencia si no fuera necesaria la autorización preceptiva.

En el caso de que se utilicen medios para el tratamiento de datos personales solamente con fines de tránsito por el territorio español, no será de aplicación lo expuesto en los párrafos anteriores.

4. **PUBLICACIÓN DEL CATÁLOGO DE FICHEROS Y DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS**

La Ley 15/1999 dispone en su artículo 14 el Derecho de consulta al Registro General de Protección de Datos:

"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita."

Entre las funciones de la Agencia se encuentra la de velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

El Registro General de Protección de Datos, según dispone el artículo 26 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, debe publicar la relación de los ficheros inscritos en el mismo.

El objetivo de este catálogo es dar publicidad de la existencia de los ficheros, siendo fundamental conocer la dirección ante la que el ciudadano puede ejercitar los derechos de acceso, rectificación y cancelación de sus datos personales que la Ley le reconoce.

La primera publicación, en el año 1995, se editó en soporte papel, resultando excesivamente voluminosa y, por tanto, poco manejable.

Debido a ello, en la publicación de los siguientes catálogos, se optó por un soporte óptico, en el que se podía incluir un software de búsqueda ágil, que permitiese localizar la información en él incluida a través de cualquiera de los conceptos publicados por cada fichero inscrito en el Registro.

Teniendo en cuenta las experiencias precedentes, para la publicación del catálogo correspondiente a 1998-1999 se optó por continuar utilizando el soporte en CD-ROM y la publicación del mismo en la página Web de la Agencia. No obstante, el ciudadano también puede pedir la información en soporte papel o a través de consulta telefónica.

Los datos publicados para cada uno de los ficheros inscritos en el Registro han sido:

- Nombre del responsable del fichero.

- Dirección en la que se pueden ejercer los derechos de acceso.

- Nombre del fichero y su descripción

- Tipo, número y fecha del Boletín en el que se ha publicado la disposición de creación del fichero, para aquellos ficheros de titularidad pública.

- Finalidad y usos del fichero.

Para cumplir con el precepto de dar publicidad a la existencia de ficheros se ha mantenido, con una actualización mensual, el catálogo de ficheros en la Web de la Agencia, lo que permite completar las publicaciones que se vienen realizando en papel y en CD-ROM, de forma que los ciudadanos puedan por este medio conocer la situación de los ficheros con una actualización mensual.

La publicación en Internet se incluye como una opción mas dentro de la Web institucional de la Agencia, donde se puede encontrar en primer lugar, información con carácter general. También se facilitan las instrucciones necesarias para inscribir nuevos ficheros en el Registro, pudiendo obtenerse el modelo normalizado de inscripción tanto de ficheros de titularidad pública como de titularidad privada y el catálogo de ficheros propiamente dicho. También se puede utilizar este medio para solicitar la información prevista en el artículo 13 de la LORTAD o para efectuar la previsión de Derecho de Consulta previsto en el artículo 14 de la Ley 15/1999, así como para obtener cualquier información a través de la aplicación por correo electrónico.

La consulta de ficheros en Internet puede realizarse a través de un formulario que presenta todos los campos publicados por cada fichero, introduciendo en uno o varios de ellos el texto por el que se desea efectuar la búsqueda. Opcionalmente, indicando un texto libre, es posible localizar todos los ficheros que contengan dicho texto en cualquiera de los campos del formulario de búsqueda.

Además, para los ficheros de titularidad pública, se ha establecido una consulta que reproduce la estructura orgánica de los diferentes tipos de Administración, permitiendo navegar y desplegar sus ramas (Organismos, Centros Directivos y Unidades), hasta localizar el responsable buscado.

Con cualquiera de las opciones de búsqueda se obtiene la relación de ficheros que cumplen los criterios establecidos.

Por otra parte, dada la capacidad de almacenamiento del CD-ROM, se ha incluido la siguiente información publicada por la Agencia, que puede resultar de interés para aquellas personas que deseen consultar el Catálogo de ficheros, y que es:

* Las memorias publicadas hasta el momento, correspondientes a los años 1994, 1995, 1996, 1997 y 1998.

* Manual de Protección de Datos, incluyendo los modelos que pueden utilizar los ciudadanos en el ejercicio de los derechos que la Ley, les reconoce.

* Legislación sobre protección de datos.

* Ponencias de las jornadas organizadas por este Organismo en 1995 y 1996, relativos a Seguridad y Derecho Español sobre protección de datos, respectivamente.

* XX Conferencia Internacional.

* Estadísticas de la actividad del Registro General de Protección de Datos.

* Premios de Protección de Datos.

* Recomendaciones para usuarios de Internet.

5. **FICHEROS DE TITULARIDAD PRIVADA**

5.1. **EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN**

Corresponde al Registro General de Protección de Datos instruir los expedientes de inscripción de los ficheros automatizados de datos de carácter personal. Asimismo, le corresponde instruir los expedientes de modificación y cancelación del contenido de los asientos y rectificar de oficio los errores materiales de los mismos.

Los trabajos referentes a los movimientos en los asientos registrales constituyen el núcleo de la actividad diaria del Registro. Pueden distinguirse tres grandes apartados, los movimientos de inscripción de ficheros, los de modificación de la inscripción y los de supresión.

5.1.1. **Inscripción de ficheros**

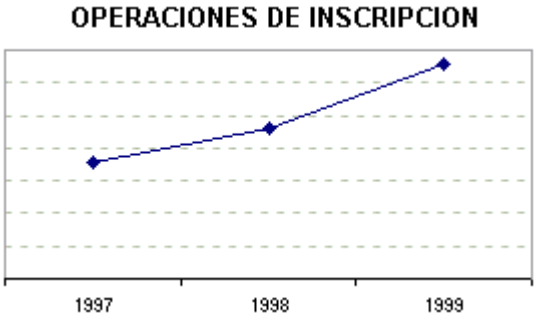
** Cifras generales.*

A lo largo de 1999 se han tramitado y realizado 3.289 solicitudes de alta de inscripción de ficheros de titularidad privada. Si contrastamos la cifra de operaciones de alta de ficheros privados de 1999 con las de los dos últimos años (2.296 altas en 1998 y 1.789 altas en 1997) se observa un gran incremento en el número de solicitudes, lo que ha supuesto un aumento del 43% en relación con las altas de 1998 y un 84% con las de 1997.

Este aumento tan significativo respecto de los últimos años, se ha originado, en parte, por el cada vez mayor conocimiento de la Ley que tienen los responsables de ficheros debido a las campañas de información que la propia Agencia de Protección de Datos y otras entidades privadas realizan y, en parte, debido a la publicación 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. La publicación de este Reglamento originó que los responsables de los ficheros revisasen las notificaciones realizadas al Registro General de Protección de Datos con la finalidad de adaptarlos a la nueva normativa, lo que ha dado lugar a una cantidad considerable de nuevas inscripciones y modificaciones de los ficheros ya inscritos.

El gráfico que se presenta a continuación muestra la evolución del número de operaciones de inscripción a lo largo de los tres últimos años.

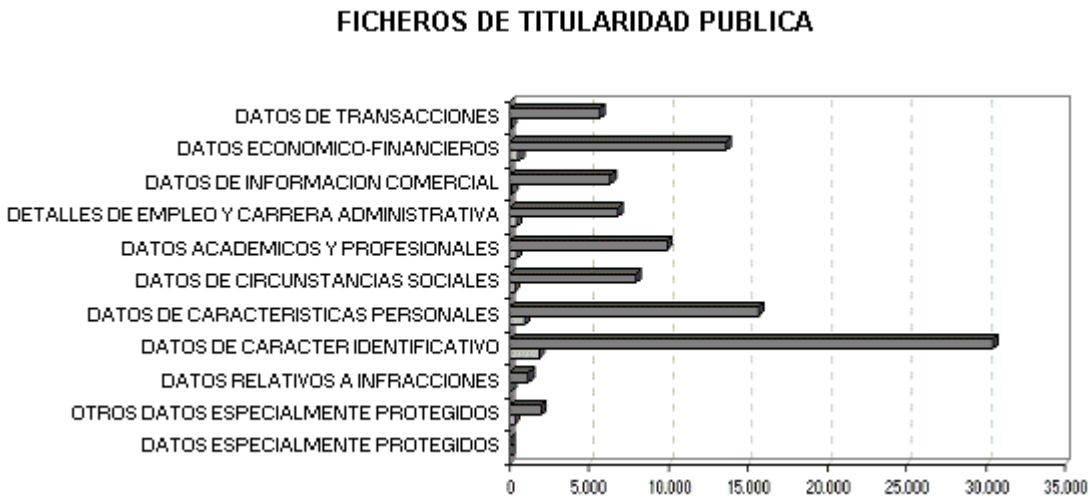


** Tipos de datos.*

En cuanto a la tipología de datos declarados en los ficheros privados inscritos en el ejercicio de 1999, aparte de los datos de carácter identificativo que aparecen lógicamente en el 100% de la inscripción, predominan los datos de características personales (54,3% de la inscripción), los económico-financieros (47,1% de la inscripción) y los datos de detalles de empleo (43,3%). En un segundo plano se sitúan los datos de transacciones (25,8%), los académicos y profesionales (21,1%), los de circunstancias sociales (20,2%) y los de información comercial (16,6%). En una escala inferior (4,7%) se encuentran las declaraciones de ficheros que contienen datos de salud, vida sexual y origen racial, encuadrados bajo la denominación de "otros datos especialmente protegidos". Por último, los ficheros inscritos que declaran "datos especialmente protegidos" de ideología, creencias y religión suponen un porcentaje insignificante en relación con la inscripción de altas del ejercicio.

Estos porcentajes son muy similares a los del ejercicio anterior y también se mantienen en línea con la tipología de datos reflejada en la inscripción total del Registro. Se observa que los tipos de datos dominantes están en consonancia con la elevada inscripción de ficheros cuya finalidad está relacionada con la gestión de personal, clientes, proveedores y gestión económica, dado que es norma generalizada la gestión automatizada de estas actividades en las empresas españolas.

En la gráfica siguiente se presenta una comparativa de los datos sobre tipología en la inscripción de ficheros relativos a los dos últimos años. Es notoria la evolución paralela de todos los tipos de datos, evolución que presumiblemente pueda consolidarse a lo largo del tiempo.



** Finalidades y usos*

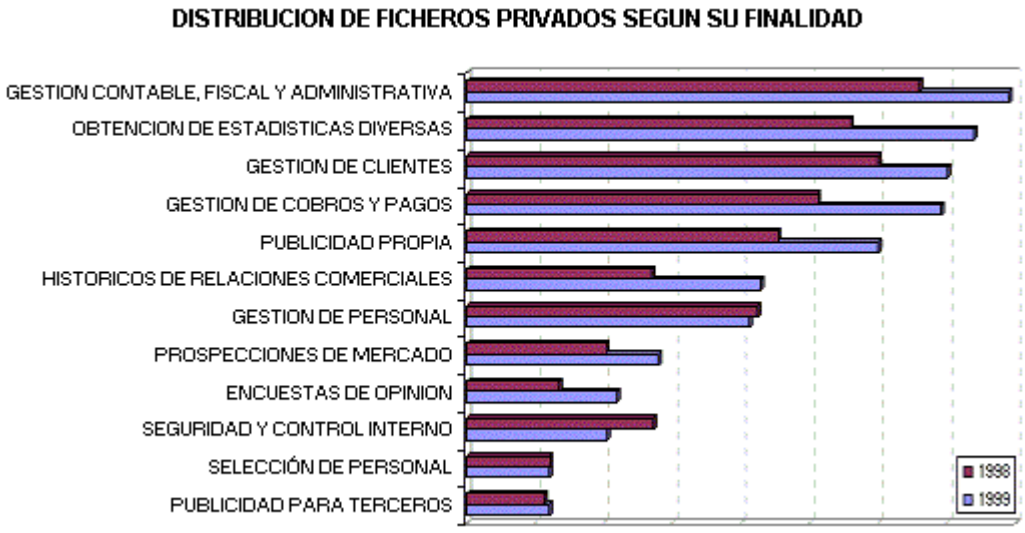
En cuanto a los usos declarados en los ficheros inscritos en 1999 destacan aquellos que declaran como finalidad del tratamiento *la gestión contable, fiscal y administrativa* (39,5%), *obtención de estadísticas diversas* (37%), *la gestión de clientes* (35%), *gestión de cobros y pagos* (34,6%), *publicidad propia* (30%), *históricos de relaciones comerciales* (21, 4%), *gestión de personal* (20,6%), *prospecciones de mercado* (14%), *encuestas de opinión* (11%), *seguridad y control interno* (10,3) *selección de personal, publicidad para terceros* y *seguros de vida y salud* (6%).

Estas cifras están en consonancia con la elevada inscripción de ficheros de personal, clientes, proveedores y gestión económica por parte de las empresas, y ponen de manifiesto el aumento continuado de creación de ficheros cuya finalidad declarada es la contabilidad, gestión de cobros y pagos, gestión de clientes, fiscalidad, gestión de personal y nóminas.

En líneas generales, las cifras de inscripción de ficheros por finalidades en el año 1999 no se alejan de las del año anterior, ni de las mismas cifras referidas a la inscripción total de ficheros. Quizá sea reseñable en la inscripción de los dos últimos años un aumento significativo en la finalidad de selección de personal, debido, en su mayor parte, a las declaraciones de inscripción de ficheros por parte de empresas de nueva creación, a la proliferación de las empresas de trabajo temporal y a la fuerte irrupción de Internet como nuevo medio en la selección de personal.

También merece especial mención el aumento que presentan en los dos últimos años las declaraciones de inscripción de ficheros con finalidades de encuestas de opinión, prospección de mercado, publicidad propia y publicidad para terceros. Este aumento puede estar basado en el desarrollo de nuevas técnicas en el ámbito del tratamiento de la información como, almacenes de datos (*datawarehouse)*, minería de datos (*data mining)*, sistemas de ayuda a la decisión *(DSS)*, etc., que pretenden ofrecer soluciones en los procesos de negocio para la toma de decisiones en general y en el ámbito del marketing en particular. Estas técnicas que surgen por la necesidad de hacer más operativa la enorme cantidad de información almacenada en distintas bases de datos, facilitan la elaboración de perfiles personales, debiendo ser utilizadas con una especial sensibilidad respecto del cumplimiento de la normativa de protección de datos.

A continuación se presenta una gráfica comparativa con los ficheros declarados en los dos últimos años según su finalidad. Se observa una evolución paralela de las distintas finalidades, siendo notoria la presencia de cifras superiores para las finalidades que más incidencia tienen en la gestión administrativa de las entidades. Las finalidades con cifras levemente inferiores en 1999 respecto del año anterior son las relativas a seguridad y control interno y, en menor cuantía, la gestión y selección de personal. Ello puede ser debido, a que en el ejercicio anterior, hubo un incremento de declaración de ficheros cuyas finalidades estaban relacionadas con las nuevas empresas cuya actividad suponía la gestión de empleo temporal y la seguridad y control interno. No obstante, la evolución paralela de la inscripción por finalidades en los últimos ejercicios puede indicar que estas cifras sean extrapolables a ejercicios venideros.



* *Origen y procedencia de los datos*

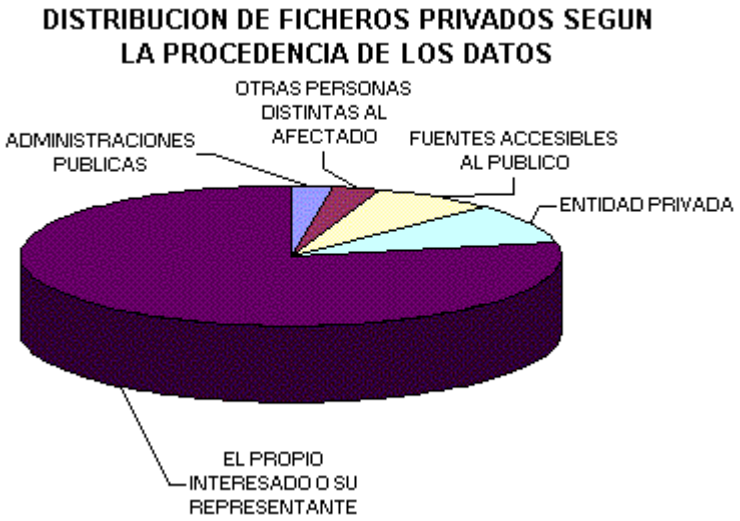
En cuanto a la procedencia de los datos declarados en los ficheros inscritos en 1999, destacan aquellos que declaran que los datos provienen del propio interesado o su representante legal (93,8% de los ficheros declarados), seguido de aquellos que declaran el origen a través de entidades privadas (10,8%), fuentes accesibles al público (9%), otras personas distintas del afectado o su representante legal (3,5%) y administraciones públicas (3%).

En la mayoría de los casos es el propio interesado el que suministra los datos al responsable, lo cual concuerda con la elevada cifra de ficheros inscritos cuya finalidad estaría relacionada con la existencia de una relación contractual que implica necesariamente que el dato lo aporte el propio interesado; tal sería el caso de la gestión de la contabilidad, fiscalidad, gestión de personal y nóminas constatados en el apartado anterior.

Por otra parte, la cifra referente a la procedencia de los datos de las *Administraciones Públicas* puede no resultar demasiado fiable, debido a la dificultad de interpretación de este concepto por parte de los declarantes, produciéndose confusión con orígenes relacionados con fuentes accesibles al público. No obstante, en este último año se ha producido un descenso considerable en la inscripción de ficheros que declaran como origen de los datos las administraciones públicas debido, por una parte, a que el Registro ha procedido a solicitar aclaración para subsanar la declaración, y por otra parte al aumento de la calidad de la inscripción por parte de los responsables.

Si comparamos el origen o procedencia de los datos de los ficheros inscritos en 1999 con el mismo apartado de la inscripción para el total de ficheros inscritos, se observa en este año un aumento significativo de los ficheros que declaran como origen de sus datos *otras personas distintas del afectado*, originado posiblemente por la utilización creciente de las bases de datos disponibles en Internet. Así mismo, se puede observar, que para el resto de apartados de procedencia de los datos, las cifras que se recogen del año 1999 son bastante coincidentes con las cifras de las inscripciones que configuran el Registro.

El gráfico siguiente presenta las cifras de inscripción en el Registro en relación con la procedencia de los datos relativas al año 1999.



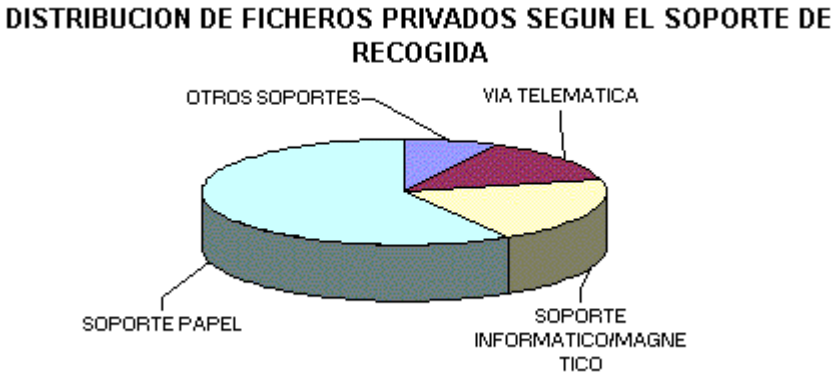
** Soporte utilizado en la recogida de los datos*

El 84% de los ficheros que se han notificado al Registro durante el año 1999, declaran que el soporte utilizado en la recogida de los datos ha sido a través de cuestionarios y métodos convencionales.

Los datos que se han recogido directamente en soportes tecnológicos (directamente desde el teclado del ordenador o a través de medios telemáticos) alcanzan la cifra del 28,5% los primeros y el 20% los segundos.

Si analizamos los datos de todos los ficheros que constan inscritos y comparamos con las cifras de los inscritos durante este año, destaca el aumento en 1999 de las declaraciones que consignan técnicas relacionadas con las nuevas tecnologías en la recogida de los datos, aumento que también se había reflejado ya en los años anteriores. Esto es debido sobre todo a la fuerte incidencia de nuevos medios de acceso a la información, como es el caso de la red Internet, lo que también está en consonancia con los datos reflejados en el apartado anterior.

El gráfico siguiente presenta las cifras de inscripción según el soporte de recogida de los datos relativas al año 1999.



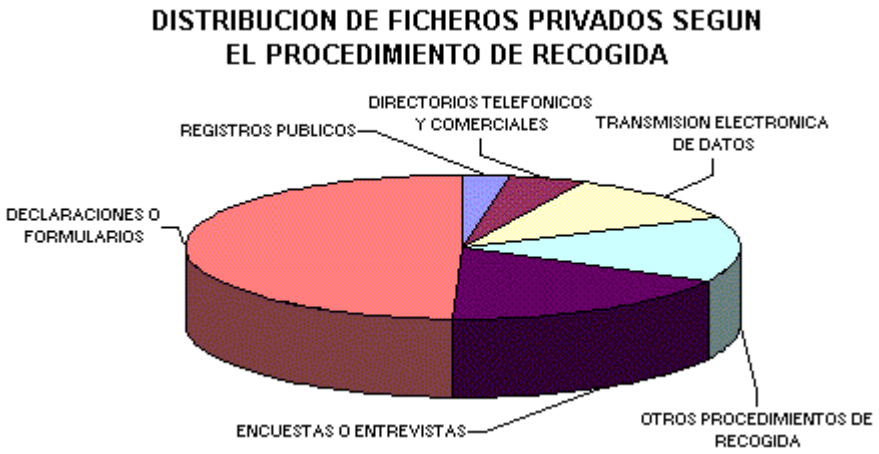
** Procedimiento de recogida.*

En cuanto al procedimiento de recogida de los datos de los ficheros inscritos en 1999 predominan aquellos que consignan como medio de recogida las *declaraciones o formularios* (68,3%) seguido de *encuestas o entrevistas* (24, 6%), *transmisión electrónica de datos* (15,1%), *directorios telefónicos y comerciales* (6,3%) y *registros públicos* (3,8%) y *otros procedimientos de recogida* (20%). Estas cifras están en consonancia con las cifras sobre soporte de recogida de la información, con las cifras de inscripción por finalidades, y con las cifras declaradas en relación al origen de los datos cuando se consigna *el propio interesado*, ya que los datos de los ficheros de contabilidad, fiscalidad, gestión de personal y nóminas, que son los predominantes, suelen recogerse inicialmente en formularios en papel o mediante entrevista directa con el afectado. En relación a la comparación con los datos totales del Registro se puede resaltar

también en este caso, el aumento de los procedimientos que implican el uso de vías telemáticas y soportes informáticos.

El apartado *"otros procedimientos de recogida"* engloba distintos procedimientos de obtención de información que no están normalizados en el modelo de notificación de ficheros. En este apartado se contemplan distintas formas de obtención de datos, en la mayoría de los casos facilitados por el propio interesado, pero a través de nuevos medios de captación de la información, como los cupones respuesta y testigos de compra, catálogos y cuestionarios, campañas publicitarias, "buzoneo", recogida de currículos, encuestas telefónicas, fax y sitios Web en la red.

El gráfico siguiente presenta las cifras de inscripción según el procedimiento de recogida de los datos relativas al año 1999.



** Cesiones de datos.*

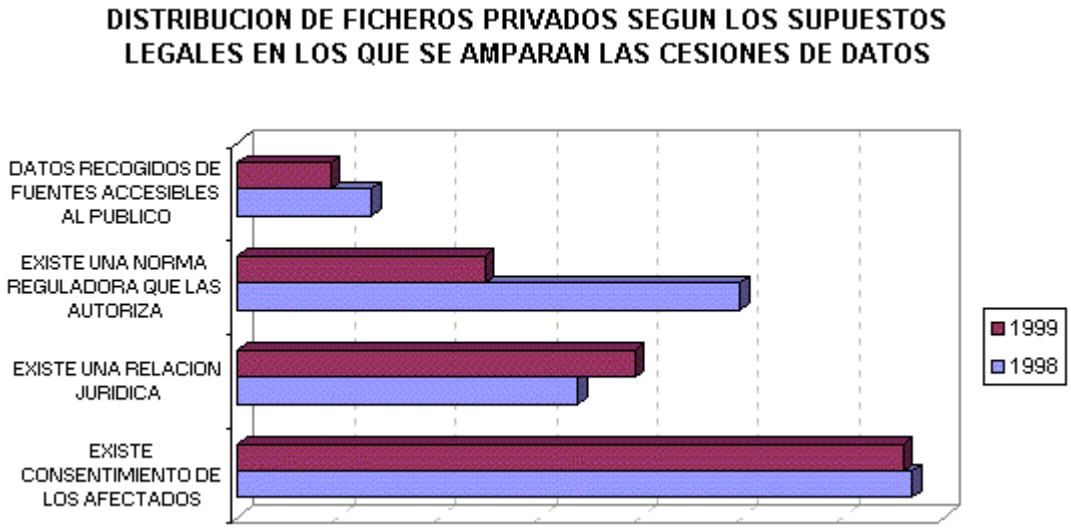
En cuanto a las cesiones de datos, en 1999 se han inscrito 1.063 ficheros que declaran este apartado, lo que supone un 32,3% en relación con el total de ficheros inscritos durante el ejercicio. El mayor porcentaje de cesiones lo justifican por la existencia del consentimiento de los afectados (66% del total de ficheros declarados con cesiones en el ejercicio), seguido por la existencia de una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros (39,4%), la existencia de una norma reguladora que las autoriza (28,5%), y los que realizan la cesión amparándose en que los datos cedidos fueron recogidos de fuentes accesibles al público (9, 2%).

El consentimiento de los afectados como justificación de la cesión se refleja en ficheros de gestión de clientes, históri - cos de relaciones comerciales y publicidad a los propios clientes. La inscripción de ficheros que justifican las cesiones por la existencia de una relación jurídica está en consonancia con la inscripción de ficheros que declaran como finali - dad pagos de nóminas, transferencias bancarias, domiciliación de recibos, gestión de tarjetas de crédito, correduría de seguros y todo tipo de relaciones de intermediación. A su vez, la cifra de cesiones basadas en la existencia de una norma que las autoriza es acorde con la existencia de ficheros de nóminas y gestión contable, fiscal y administrativa, que son cedidos a la Agencia Tributaria y a la Tesorería de la Seguridad Social en virtud de Ley.

Los ficheros que justifican las cesiones amparándose en la procedencia de los datos de fuentes accesibles al público son aquellos cuya finalidad se corresponde con el uso para servicios de marketing, envíos de publicidad, prospección de mercados y fines relacionados con este sector de actividad.

En el gráfico siguiente se presentan las cifras relativas a ficheros privados inscritos durante 1999 según los supuestos legales en los que se ampara la cesión.

El gráfico siguiente compara los datos de cesiones declaradas en los ficheros inscritos en 1999 con las cesiones declaradas durante el año 1998, distribuyendo los ficheros entre los supuestos legales en los que se amparan. En este gráfico se observa el paralelismo existente entre las cifras de los dos últimos años, salvo en la rúbrica de cesiones justificadas por la existencia de una norma reguladora que las autoriza, que sufre un fuerte descenso, que se podría justificar por el mayor conocimiento y cumplimiento de la Ley por parte de los responsables en lo referente a cesiones de datos.

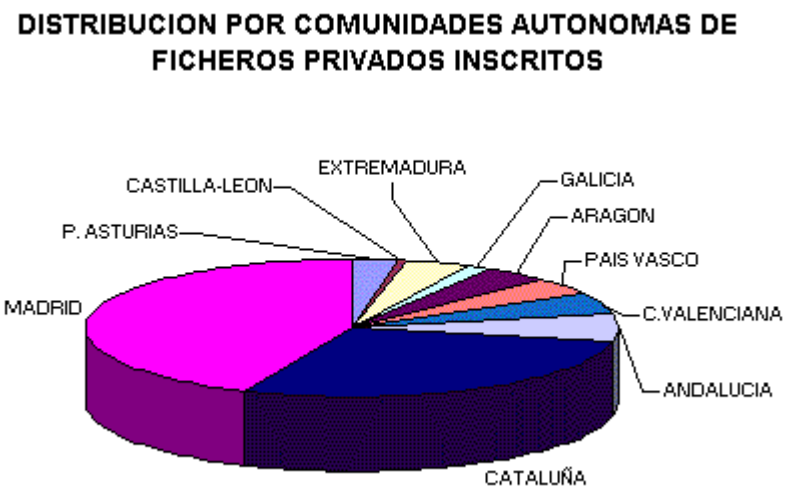


** Inscripción de ficheros privados por ámbito geográfico.*

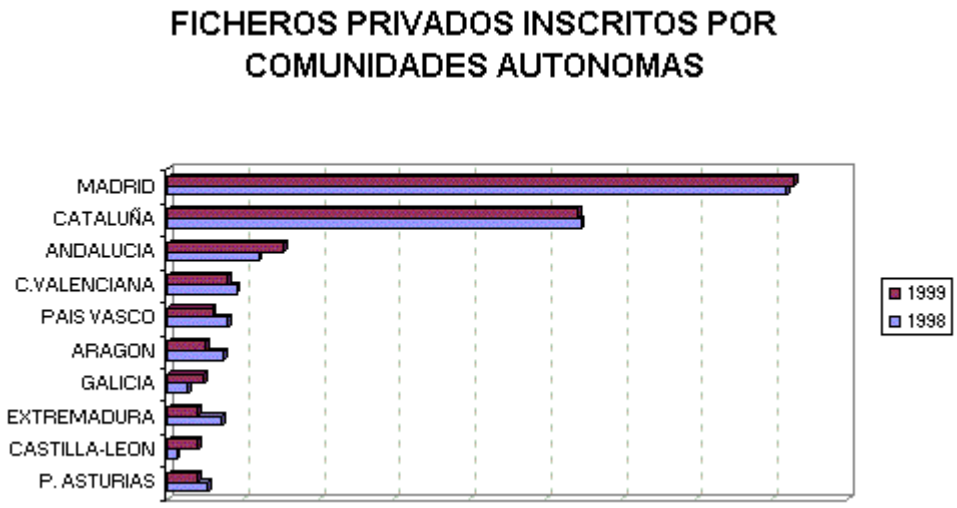
En cuanto a la distribución geográfica de las cifras de inscripción de ficheros más representativas durante el año 1999 por Comunidades Autónomas, se observa que los responsables establecidos en la Comunidad de Madrid ha notificado el 41,4% del total de ficheros del ejercicio, seguidos de los de Cataluña con una inscripción del 27,1% del total, Andalucía el 7,7%, Comunidad Valenciana el 4%, País Vasco el 3%, Aragón el 2,5%, Galicia el 2,4% y Extremadura, Castilla-León y el Principado de Asturias con el 2%.

Es de destacar la estabilización de las altas cifras de inscripción de Madrid y Cataluña, ya que son los grandes núcleos industriales y de servicios. Las cifras de estas dos comunidades son muy semejantes en los dos últimos años e indican una posible evolución paralela en el tiempo. Pero no sólo se estabilizan las cifras de inscripción en Madrid y Cataluña, sino que en el resto de las comunidades, se observan unas cifras de inscripción muy similares en los dos últimos años

El gráfico siguiente muestra las cifras de inscripción de ficheros durante el año 1999 por Comunidades Autónomas.

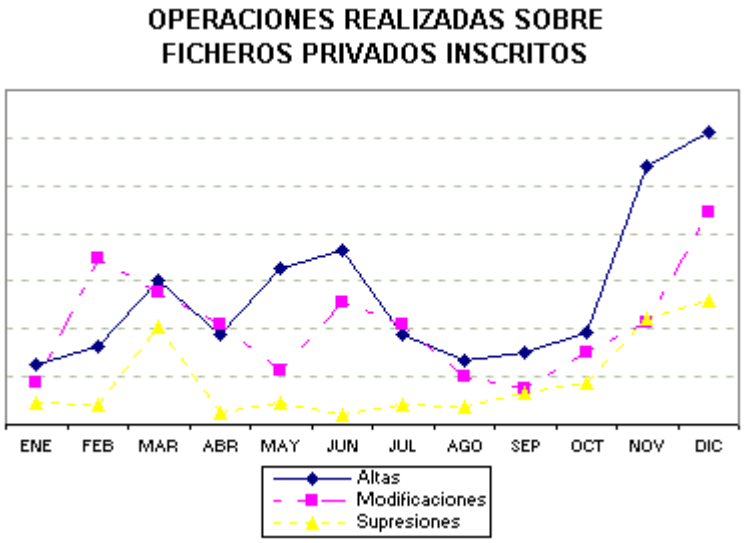


En el gráfico siguiente se comparan las cifras de inscripción para las comunidades autónomas más representativas en los dos últimos años.



** Distribución temporal de la inscripción*

En cuanto a la distribución temporal de la inscripción en 1999, se observa una tendencia creciente a lo largo del año, tendencia que solo se trunca en época de vacaciones y que se acentúa en la parte final del año, tal y como se muestra en la figura siguiente:

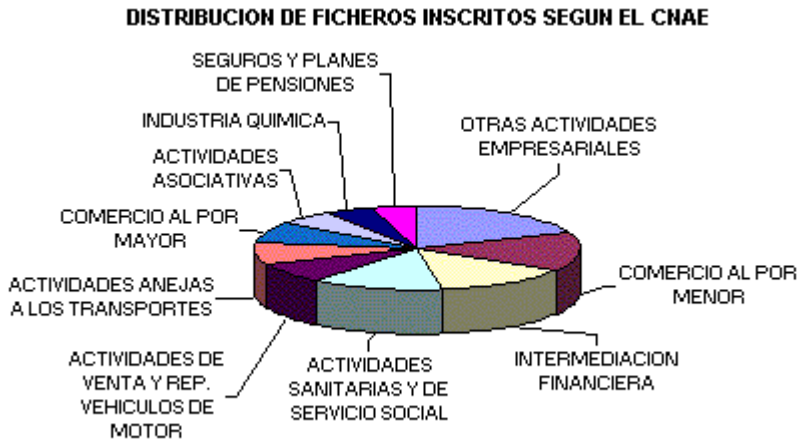


Si comparamos la evolución temporal de las cifras totales de operaciones realizadas sobre ficheros de titularidad privada a instancias de los responsables durante los dos últimos años en el Registro General de Protección de Datos se observan cifras superiores en 1999 para la mayoría de los meses del año. Esta tendencia de crecimiento se acentúa a medida que el año avanza, y es mucho más acusada a final de año.

** Inscripción por Sectores Económicos.*

En cuanto a la inscripción de ficheros en el año 1999 por sectores económicos de actividad, predomina el sector de *otras actividades empresariales* (que es muy amplio, y que incluye, entre otras, las actividades jurídicas, de contabilidad, auditoría, asesoría fiscal, estudios de mercado, encuestas de opinión y asesoramiento sobre dirección y gestión empresarial) con un 12,8%. Le siguen el sector del *comercio al por menor* con un 10% del total de ficheros inscritos en el ejercicio, el sector de la *intermediación financiera* con un 9,5%, las *actividades sanitarias y de servicio social* con un 8, 8%, las *actividades de venta, reparación* y *mantenimiento de vehículos de motor* con un 5,7%, las *actividades anejas a los transportes y agencias de viajes* con un 5,6%, las *actividades de comercio al por mayor e intermediarios del comercio* con un 5,4%, las *actividades asociativas* con un 3,6%, la *industria química* con un 3,5% y las actividades de *seguros y planes de pensiones* , con un 3%.

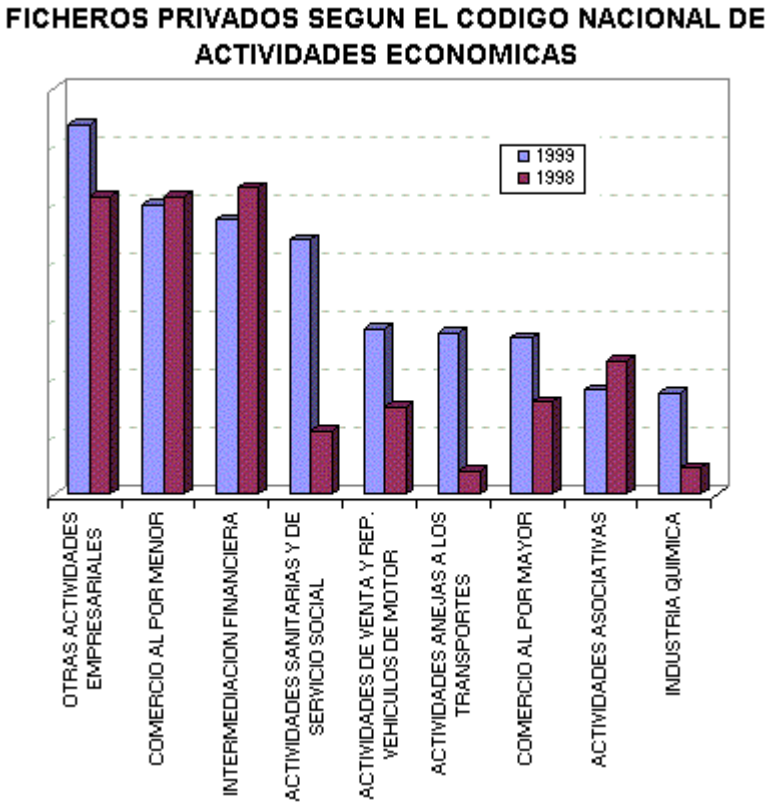
Estos datos se resumen en el gráfico siguiente:



Si comparamos la inscripción de ficheros por sectores económicos de actividad en el año 1999 respecto del año anterior, se observa una cierta semejanza en las cifras relativas a los sectores más importantes, sectores que coinciden con los más representativos del mercado en cuanto a actividad general. En algunos sectores puntuales se observan ciertas

diferencias en cuanto a cifras en los dos años, pero los 10 primeros sectores son los mismos en ambos años, aunque con diferencias en su orden de importancia.

La gráfica siguiente compara la inscripción según sectores de actividad en los dos últimos ejercicios.



5.1.2. **Modificación de inscripción de ficheros**

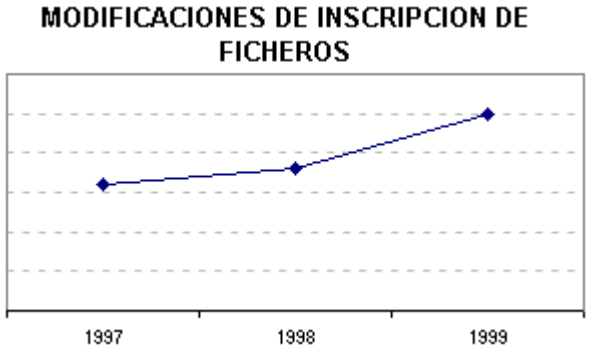
Se han modificado, a solicitud del responsable, mediante recepción de notificación en tal sentido (en soporte papel o en disquete), un total de 2.485 inscripciones de ficheros, cifra muy cercana a la relativa a la inscripción de nuevos ficheros.

Estas cifras de modificaciones son superiores a las de los dos últimos años, hecho que está en línea con el ya citado aumento de las notificaciones de altas que se han producido en este ejercicio. Por otra parte, también ha intervenido en el aumento de las modificaciones la publicación, en el mes de junio, del Reglamento sobre medidas de seguridad de los ficheros automatizados de datos de carácter personal, lo que ha supuesto que los responsables de los ficheros solicitaran actualizar el apartado de medidas de seguridad, para adaptarlo a las exigencias de dicho Reglamento, con el fin de hacer constar que disponían de un plan de seguridad debidamente documentado, toda vez que hasta ese momento no estaba reglamentado y se podía declarar la posibilidad de que no existiera dicho plan .

Especial importancia, en la cifra de modificaciones de ficheros, puede haber tenido las revisiones que se han realizado durante el año 1999 a los sistemas de información para prevenir el Efecto 2000. A su vez, estas nuevas aplicaciones han supuesto la necesidad de revisar el contenido de la inscripción y su modificación para adecuarlo a los nuevos sistemas de información.

También influye en el aumento de las modificaciones los cambios que se producen en las empresas ya sean tecnológicos en sus sistemas de información como en su forma de constitución social. Durante el ejercicio de 1999 han aumentado considerablemente las peticiones de información sobre el estado de la inscripción de los ficheros por parte de los propios responsables, con la finalidad de proceder a regularizar, a los efectos de inscripción, las modificaciones que se habían producido en los ficheros desde su inscripción inicial.

El siguiente gráfico refleja la evolución del número de operaciones solicitadas por los responsables para modificar la inscripción de sus ficheros. Se observa que esta evolución es muy similar a la relativa a inscripción de nuevos ficheros.



Una parte importante de las solicitudes de modificaciones están relacionadas con el apartado de *responsable del fichero* y se han originado por cambio de titular, absorción por otra empresa, fusiones de empresas o cambios en la denominación de la razón social. En estos casos, además de la información preceptiva que debe contener la notificación y su comunicación, a efectos de inscripción, se requiere al responsable del fichero para que aporte garantías suficientes que justifiquen la situación jurídica que alegan y, de esta forma, informarles de las exigencias legales que en estos casos debe cumplir el responsable del fichero, en particular, sobre la comunicación de la identidad del nuevo responsable a los afectados.

El apartado de responsable también ha generado confusión en la declaración de los ficheros, debido a que desde la perspectiva de los propios declarantes, han existido interpretaciones erróneas derivadas de situaciones como la falta de delimitación clara entre las figuras de responsable y encargado del tratamiento, la confusión entre el domicilio de la entidad donde se ubica físicamente el fichero y el del responsable del mismo, las incorrecciones en el código de identificación fiscal y el desconocimiento del código nacional de actividad económica.

Se hace especial referencia, en las dudas que produce la interpretación de la figura del Responsable del fichero de una sociedad matriz, cuando en esa sociedad se centraliza la Dirección Informática del Grupo, y los ficheros y sistemas de información pueden ser utilizados por las Sociedades Filiales, sobre todo en el caso que además estén participadas por la matriz al 100%.

En este caso, si la empresa matriz se limita a prestar un servicio de gestión informática unificada por cuenta de sus filiales, deberá considerarse como encargada del tratamiento, manteniéndose las filiales como responsables del fichero debiendo constar en la inscripción esta doble condición.

En todo caso, no hay que olvidar lo ya manifestado explícitamente en el apartado de introducción, en el que, claramente se ha puesto de relieve el carácter meramente declarativo de la inscripción de los ficheros, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

Sin perjuicio, de que en su caso, comportará por su propia naturaleza, el que puedan ser sancionadas conductas contrarias a los principios que la misma tiene en la protección de la intimidad de los ciudadanos.

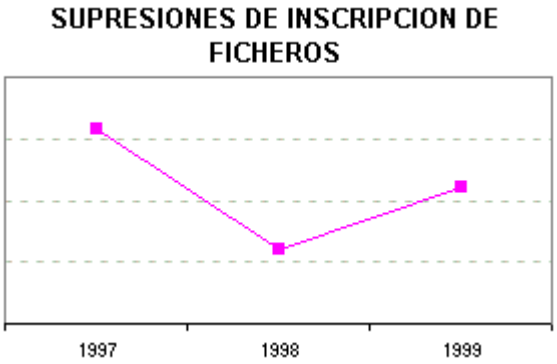
Otro apartado de la inscripción que también ha sido objeto de modificaciones frecuentes es el *apartado de cesiones*, bien como consecuencia de errores producidos en la notificación de ficheros derivados de la dificultad que supone la interpretación de los supuestos legales que amparan las cesiones de datos a terceros, o bien por la aparición de nuevos destinatarios de las mismas derivada de la actividad de la empresa. Las dificultades que en la práctica supone justificar legalmente las cesiones también provoca errores en la notificación de ficheros. Le sigue en importancia el apartado de *procedencia de los datos*, motivado bien por errores en la interpretación de los tres subapartados de los que consta el modelo de los formularios, o bien por la dificultad de plasmar en la notificación la procedencia real de los datos que originan los ficheros automatizados.

5.1.3. **Supresión de ficheros**

El artículo 24 apartado 3 de la Ley y el artículo 8 apartado 2 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley en relación a la cancelación de la inscripción de ficheros, dispone que se deberá comunicar la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

Durante el año 1999 se han realizado 1.113 operaciones de supresión de inscripción de ficheros de titularidad privada a petición de sus responsables, lo que supone aproximadamente un tercio del número de altas del ejercicio y la mitad del número de modificaciones. Esta cifra de supresiones es superior a la del año anterior, hecho que está en línea con el ya citado aumento de todo tipo de notificaciones al Registro que se ha producido en este ejercicio.

El siguiente gráfico refleja la evolución de las operaciones de supresión a efectos de cancelación a lo largo de los años.



El apartado de supresiones presenta una casuística determinada, que ha supuesto las diferentes situaciones que se exponen a continuación:

- En primer lugar, se producen casos de bajas, disoluciones o ceses de actividad de las empresas, que conllevan una destrucción física de los ficheros con datos personales. En estos casos, se solicita al responsable que se asegure la destrucción de los ficheros. Además, se anota, a efectos informativos, en su caso, la existencia de copias de seguridad, para el cumplimiento de las obligaciones determinadas por la Ley.

- En segundo lugar, se plantean situaciones en las que se solicita la supresión de una inscripción de un fichero porque sus datos se han incluido con un colectivo que forma parte de otro fichero o sistema de información del mismo responsable, bien por una modificación considerable de los sistemas de información de la empresa, o bien por la implantación de un nuevo sistema de información. En estos casos se reflejan en los asientos de supresión los códigos de inscripción de los nuevos ficheros resultantes.

- En tercer lugar, existen casos en los que no se produce la destrucción física de los ficheros, sino que sus datos se integran en nuevos ficheros con la misma estructura, pero de un responsable o titular de los mismos diferente. Esta situación suele ser causada por la absorción por otra empresa, fusión de empresas, cambio de titular o desafectación de un servicio público. En estos casos no se tramitan las supresiones hasta que se garantice que no hay una cesión enmascarada, para lo cual han de aportarse las suficientes garantías que justifiquen el cumplimiento de los preceptos de la Ley. Además, en el caso de la absorción, se comprueba la inscripción anterior de la empresa absorbente y en los asientos de supresión se reflejan los códigos de inscripción de los nuevos ficheros que van a contener la información de los suprimidos. En el caso de la fusión de empresas, es necesario que conste en el Registro la solicitud de nueva inscripción de los nuevos ficheros de la empresa resultante, anotando de oficio sus códigos en los asientos de los ficheros suprimidos, así como la razón social y código de identificación fiscal de la nueva sociedad.

- En cuarto lugar, se solicitan supresiones por subsanar un error cometido en la inscripción inicial, suelen consistir en la existencia de más de una inscripción de un mismo fichero, o en la declaración de apartados que no concuerdan con la realidad en la inscripción, o en la inscripción de ficheros con titularidad errónea (públicos como privados o privados como públicos), o en la inscripción indebida de ficheros por interpretación incorrecta de la ley o simplemente en la inscripción de ficheros que no poseen datos de carácter personal. En estos casos se anota de oficio en los asientos de inscripción de los ficheros suprimidos las causas que han originado la supresión. Además si se trata de la supresión de la inscripción de un fichero duplicado, se refleja en el asiento de supresión el código de inscripción del fichero con el que estaba duplicado. En el caso de la supresión de un fichero por titularidad errónea se refleja en el asiento de supresión el nuevo código de inscripción que le sustituye.

Mención aparte merece la situación que ha dado lugar a supresiones de inscripción con el fin de subsanar un error en la interpretación de la norma, en relación con el encargo a terceros de la gestión de los servicios de tratamiento informático. En este caso, surge la figura definida en la Directiva 95/46/CE, como "encargado del tratamiento" transpuesta en la Ley 15/1999 en su artículo 12 (relacionado con el artículo 27 de la Ley 5/1992) como "prestación de servicios de tratamiento automatizado de datos de carácter personal, por cuenta de terceros". Este servicio, a efectos de inscripción, no supone la creación de nuevos ficheros, por lo tanto, no hay que realizar nuevas notificaciones de inscripción. Únicamente podría suponer una declaración de modificación con el objeto de actualizar los apartados de ubicación de los ficheros y sistemas de tratamiento.

Como ya se ha indicado en páginas anteriores, uno de los nuevos apartados que contendrá el nuevo modelo de notificación será el de *Encargado de tratamiento* , lo que supondrá que este tipo de errores no se produzcan en un futuro.

5.1.4. **Resumen de operaciones realizadas durante 1999 a solicitud del responsable del fichero de titularidad privada**

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Altas	126	164	302	189	325	366	190	133	152	193	539	610	3.289
Modificaciones	86	346	277	210	115	254	211	101	74	150	215	446	2.485
Supresiones	45	44	204	26	48	23	44	39	67	90	223	260	1.113
TOTAL	257	554	783	425	488	643	445	273	293	433	977	1.316	6.887

Como se puede observar en la tabla el crecimiento en el último año también es aplicable a cada tipo de operación, es decir, tanto altas como modificaciones y como supresiones han experimentado una subida general, acentuada sobre todo a final de año.

Las escasas cifras que son superiores en determinados meses del año 1998 se deben como norma general a notifica - ciones masivas puntuales enviadas por los responsables en respuesta a requerimientos específicos realizados por el Registro.

Ciñéndose ya a cifras totales, vemos que estos aumentos mensuales del total de operaciones provocan un aumento acumulado en la cifra del total de operaciones de 1999 de un 46% respecto del total de operaciones de 1998. En cuanto a las cifras totales relativas a altas de ficheros se observa un aumento del 43% en este último año. En lo relativo a las cifras totales de modificaciones el aumento es de un 37%, y en lo atinente a supresiones el aumento es de un 85, 5%.

Refiriéndose a cifras totales mensuales desde junio en adelante, que es la época en que empieza a ser notorio el aumento (salvo en el mes de septiembre), tenemos los siguientes datos: Las operaciones totales del mes de junio de 1999 superan en un 92% a las operaciones del mismo mes en 1998, las operaciones del mes de julio son superiores en un 33%, las de agosto son superiores en un 3%, las de octubre son superiores en un 30%, las de noviembre son superiores en un 221% y las operaciones de diciembre de 1999 son superiores a las de 1998 en un 143%. Se percibe que las tasas de crecimiento de las operaciones realizadas en 1999 respecto de las de 1998 sufren su mayor variación en los tres últimos meses del año.

Existen factores puntuales que pueden haber provocado la subida general de la inscripción durante el año 1999, como puede haber sido la publicación del Reglamento de medidas de seguridad de los ficheros automatizados de datos de carácter personal o en su momento la inminencia de la transposición de la Directiva comunitaria de protección de datos. Hay otros factores aleatorios en el tiempo que también inciden sobre la evolución temporal de la inscripción, como pueden ser el mayor conocimiento de la Ley, la publicidad institucional en los medios de comunicación, los artículos en prensa relativos a la intimidad y protección de datos, los requerimientos que realiza la propia Agencia demandando información a determinados sectores, las campañas realizadas por determinadas entidades privadas directamente relacionadas con las tecnologías de la información y la protección de datos, el gran aumento en el uso de las nuevas tecnologías producido en todos los ámbitos de la sociedad.

La evolución en el aumento de solicitudes de inscripción, es presumible que tienda a consolidarse en estas cifras o aumentaran aún mas a medio plazo, debido por un lado, a que las declaraciones iniciales que se realizaron con la entrada en vigor de la LORTAD, han sufrido modificaciones, a lo largo del tiempo, lo que podría suponer una segunda etapa de inscripción masiva para actualizar y adecuar las declaraciones que constan inscritas a la situación real de los sistemas informáticos.

Por otro lado, hay que tener en consideración la entrada en vigor de la nueva Ley, lo que también es previsible que incida en el aumento en la declaración de ficheros y tratamientos a los efectos de su inscripción el Registro General de Protección de Datos.

5.2. **OPERACIONES DE OFICIO**

El Artículo 26 del Estatuto de la Agencia de Protección de Datos, faculta al Registro General para rectificar de oficio los errores materiales reflejados en los expedientes de inscripción, modificación y cancelación de ficheros.

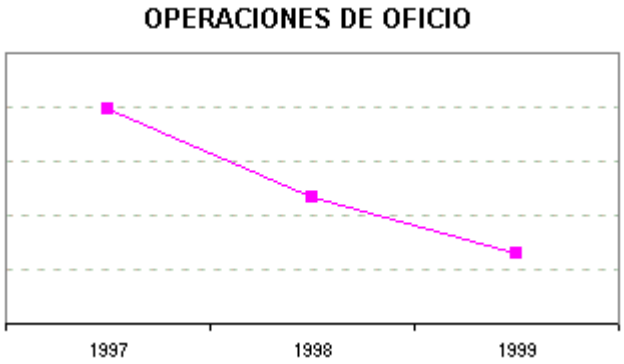
En el ejercicio 1999 se han realizado 1.308 operaciones de oficio en las inscripciones de ficheros de titularidad privada. El 83,6% de las operaciones de oficio corresponden a subsanaciones de errores materiales de los asientos y un 16, 36% a cancelaciones o supresiones de inscripciones debidas a la depuración de inscripciones duplicadas.

El número de operaciones de oficio tiende a disminuir debido a las siguientes consideraciones:

- Los responsables de ficheros conocen mejor la legislación vigente y por lo tanto, los modelos se cumplimentan con menos errores.

- La implantación en el Registro General de nuevos procedimientos de depuración a priori, lo que supone, que en vez de subsanar de oficio muchos errores que se consignan en las declaraciones, antes de proceder a la inscripción, se requiera al declarante de los ficheros para que procedan a subsanar los datos consignados erróneamente.

La evolución temporal de las operaciones de oficio se presenta en el siguiente gráfico



5.2.1. **Depuración de inscripciones duplicadas**

Como consecuencia de la tendencia de los responsables de ficheros a notificar una nueva inscripción, cuando realmente desean modificar la inscripción de un fichero ya existente, se producen duplicidades difíciles de detectar, sobre todo en el caso de la inscripción en soporte magnético. Para subsanar esta anomalía y antes de realizar cada año la publicación del catálogo de ficheros inscritos, se procede a depurar de oficio la base de datos con el fin de suprimir todas aquellas inscripciones duplicadas que correspondan a un mismo fichero.

El procedimiento establecido para realizar esta depuración ha consistido en seleccionar las inscripciones de ficheros del mismo responsable cuyo nombre y finalidad constaba inscrita más de una vez en la base de datos, agrupándolos por responsables. Se detectó la existencia de ficheros que se encontraban inscritos dos veces, e incluso más de dos veces. A partir de aquí, se definió un proceso de depuración con la finalidad de eliminar duplicidades, haciendo grupos según el número de veces que se repetían los ficheros. Dando como resultado la supresión de 214 inscripciones de ficheros duplicados durante el año 1999.

5.2.2. **Ficheros con el mismo nombre y responsable, pero no duplicados**

Existen responsables de ficheros que debido a la distribución geográfica de su actividad, tienen distintas delegaciones en el territorio nacional y en cada una de ellas tienen ubicados ficheros, que en lo único que se diferencian, es en el colectivo de personas que se almacenan en los mismos. Tal es el caso de las grandes superficies, las empresas de grandes dimensiones y en general las empresas con numerosas sucursales en distintas provincias de España. En estos casos, el responsable de los ficheros es único y la dirección de acceso, rectificación y cancelación también suele ser única y centralizada. Sin embargo un mismo fichero presenta distintas ubicaciones físicas, en general tantas como sucursales o centros de actividad distintos posea el responsable. Debido a estas circunstancias, existen inscripciones de ficheros del mismo responsable y con el mismo nombre, pero con ubicación física distinta, que inicialmente pueden confundirse con ficheros duplicados. En estos casos, se ha subsanado de oficio y de forma normalizada la denominación del nombre y descripción de los ficheros incluyendo, adicionalmente a la denominación, el nombre de la localidad o bien el nombre de la sucursal o delegación donde se ubican. Este proceso de subsanación se ha realizado en 211 inscripciones de ficheros.

5.2.3. **Depuración de denominaciones de responsables**

Existe una variada casuística de problemas que pueden provocar la inscripción de ficheros de un responsable con denominaciones distintas del mismo, lo que puede desembocar en el error de la presencia de inscripciones de distinto titular pero con el mismo NIF/CIF, hecho que dificulta la identificación de responsables y distorsiona los análisis, estadísticas y publicaciones relativas a la inscripción en el Registro General de Protección de Datos. Las fuentes más comunes de estos problemas son las siguientes:

- Errores tipográficos en la declaración del nombre del responsable.
- Personas físicas responsables de ficheros que unas veces declaran el nombre delante de los apellidos y otras detrás.
- Denominaciones de responsables declaradas de forma totalmente distinta debido a que unas veces notifican su identidad como personas físicas y otras como personas jurídicas haciendo constar el mismo NIF/CIF.
- Confusión entre la denominación del nombre de marca o de logotipo con la denominación de la razón social.
- Errores en la declaración de las siglas que acompañan al tipo de sociedad.
- Declaración del nombre del mismo responsable unas veces con abreviaturas y otras no, o con distintos espaciados entre sus caracteres.
- Modificaciones del nombre del responsable derivadas de procesos de fusiones, absorciones y otras figuras mercantiles que no son comunicadas en tiempo y forma al Registro General de Protección de Datos.

Este tipo de circunstancias origina un proceso minucioso y continuo de control de las notificaciones de ficheros, que implica la consulta de toda la inscripción previa de un responsable cada vez que se recibe una notificación que, en su caso, conlleva modificaciones de oficio. El problema se agrava cuando el responsable notifica sus ficheros en soporte magnético y cuando ha cambiado su denominación social y no se ha comunicado al Registro a efectos de inscripción.

5.2.4. **Cesiones de datos**

En la declaración del apartado de cesiones, se debe consignar la opción por la que se justifica la cesión de datos. Cuando la cesión se ampara en la existencia de una norma reguladora que las autoriza, es necesario especificar el número de la norma y el año, así como el nombre de la disposición reguladora. Del estudio de las normas legales declaradas, como supuesto en el que se amparan las cesiones de datos de ficheros de titularidad privada, se han observado distintos tipos de fuentes de error entre los que destacan los siguientes:

- Se citan normas inexistentes, tanto en lo referido al número y al año, así como a la propia denominación de la norma.
- Se citan normas que no tienen el rango suficiente para justificar una cesión de datos.
- Se cita, de forma incorrecta, la propia Ley Orgánica 5/1992 como norma reguladora que autoriza la cesión.
- En determinado tipo de ficheros, que son objeto de cesión a Organismos Públicos porque un norma así lo obliga (declaración de IRPF, declaración de cotizaciones a la Seguridad Social, etc.), no se citan las normas y en muchos casos ni siquiera se especifican las propias cesiones.
- Una misma norma se consigna de forma distinta en diferentes ficheros.

Ante esta problemática, es necesario normalizar la información que se inscribe en este apartado. Para ello, se han elaborado instrucciones de depuración y normalización con la finalidad de mantener uniforme la inscripción en cuanto al nombre de las disposiciones legales que justifican las cesiones, su número y fecha, y sus destinatarios.

5.3. **OTRO TIPO DE ACTIVIDADES**

5.3.1. **Análisis de la inscripción privada por sectores de actividad.**

Entre las actividades del Registro General de Protección de Datos, se encuentra la de realizar análisis de la inscripción por sectores de actividad cuando lo requiere una situación concreta, como puede ser una petición de la Dirección, una petición de la Inspección, el control del propio sector u otra causa similar. Dentro de este tipo de actividades destacan, durante el año 1999, las siguientes:

** Notarías*

En la Memoria del año 1998, ya se puso de manifiesto la necesidad de establecer procedimientos para la correcta inscripción de los ficheros de los que son responsables los notarios.

Por ello, el Director de la Agencia mantuvo diferentes reuniones con el Consejo General del Notariado con la finalidad de concienciar e informar en lo relativo a la protección de los datos de carácter personal. Se procedió a informar de una forma organizada, uniforme y coordinada, objetivo que pudo conseguirse a través del Consejo General del Notariado, y fruto de ello, en el ejercicio actual se ha observado un aumento de la declaración de los ficheros automatizados de este sector, tal y como se había previsto el año pasado.

Los ficheros inscritos declaran tipologías relativas a los clientes de las notarías relativos a escrituras autorizadas otorgadas, documentos públicos en general, confección del libro de registro, datos exigidos por la legislación notarial para los índices mensuales y alfabéticos, datos de declaraciones de herederos y testadores, datos de la gestión integral de las notarías, datos de facturación emitida por las notarías, datos de los propios trabajadores, etc.

Entre las finalidades declaradas en este tipo de ficheros destacan la gestión del protocolo, gestión fiscal, confección de índices colegiales, listados y estadísticas para las administraciones tributarias y organismos públicos, contabilidad propia, facturación y gestión estadística.

Este tipo de ficheros presenta cesiones amparadas en la mayoría de los casos en la existencia de una norma reguladora que las autoriza. Se realizan cesiones a la Dirección General de Registro y Notariado, al Colegio Notarial Provincial y al Registro General de Actos de Última Voluntad del Ministerio de Justicia en virtud del Reglamento Notarial. Se ceden datos a las Delegaciones Provinciales de la Agencia Tributaria y a los Servicios Fiscales de las Juntas Autonómicas en virtud de diversa legislación fiscal. También se ceden datos a los Ayuntamientos para el impuesto de plusvalía en virtud de la Ley Reguladora de las Haciendas Locales.

** Ficheros con fines de publicidad y marketing*

Dentro de la rúbrica de análisis de inscripciones sectoriales adquiere relevancia la inscripción de los ficheros con fines de publicidad, marketing y prospecciones de mercados. El desarrollo de las nuevas tecnologías de la información, aplicadas al marketing, están introduciéndose en nuestro país, lo que exigirá analizar su incidencia en la intimidad. Los riesgos que pueden presentar los datos de los ciudadanos, tomados parcialmente, revelan aspectos parciales de éstos. Pero cuando se fusionan, se mezclan, puede llegar a dar un perfil concreto del individuo.

El desarrollo tecnológico actual permite el acceso masivo a una cantidad de información elevada proporcionada por las propias empresas y relativa a los productos o servicios que ofrecen. El objetivo final de la tarea de marketing realizada

por las compañías es el propio usuario, usuario sobre el que necesitan información las citadas compañías para evaluarlo con fines de aumento de ventas con coste controlado. La posible respuesta de los clientes se almacena con la finalidad de ser utilizada en el futuro. Por tanto, las nuevas tendencias del marketing van encaminadas a conseguir nuevos clientes y fidelizar los actuales.

Las compañías disponen de personal, técnicas y herramientas encaminadas a analizar la información pormenorizadamente con la finalidad de conocer el perfil de los clientes y poder así realizar su oferta de modo más preciso y con más posibilidades de éxito. De este forma se pueden utilizar las preferencias de los clientes para realizar segmentaciones y redirigir las promociones de productos según los patrones de los diferentes clientes. Las nuevas técnicas de investigación de mercados están aflorando a medida que los recursos tecnológicos y los tratamientos automatizados se perfeccionan. Estas técnicas se basan en el análisis de los datos personales con el fin de realizar una selección personalizada y dirigida a su perfil, gustos y preferencias. El desarrollo de las nuevas tecnologías de la información, aplicadas al tratamientos de datos personales, implica nuevos riesgos en el tratamiento de datos personales.

En los párrafos siguientes se hace una referencia breve a algunas de las técnicas en las que se basan estos tratamientos automatizados, como es el caso del almacenamiento de datos (*datawarehouse*), minería de datos *(data mining)* y los sistemas de apoyo a la decisión *(DSS).*

Actualmente, lo común es disponer de una cantidad ingente de información, inicialmente desordenada, y que ha de ser explotada de forma eficiente para obtener de ella el máximo beneficio. Se conoce como *datawarehouse* la técnica que aglutina una serie de diseños de bases de datos que tienen en común el ser una agrupación de un gran volumen de información optimizada para su explotación. Estos datos provienen de diversas áreas funcionales de la empresa y pueden guardar datos históricos y/o acumulados para facilitar una determinada consulta. Estos diseños de datos convierten la información de la empresa en un gran almacén de datos organizado de forma óptima para su posterior consulta a medida. El almacenamiento de datos organizado combina todas las fuentes de información relevantes para una organización en una única estructura de base de datos susceptible de apoyar el proceso estratégico de la información.

Una vez almacenados los datos de forma óptima mediante técnicas de *datawarehouse*, su análisis efectivo se realizará mediante técnicas de *data mining*, que están basadas en el uso adecuado de los algoritmos estadísticos de análisis multivariante para descubrir sutiles relaciones, o relaciones ocultas entre elementos que constituyen la información de las bases datos, así como la generación de modelos predictivos derivados de ellos. En lo relativo al marketing, las técnicas de *data mining* desembocan en un marketing inteligente aplicado al cliente individual que tiene como finalidad esencial el adquirir una visión integral del mismo en todas sus facetas (económica, de relación con la entidad, perfil socioeconómico, historia detallada, entorno, etc.) y desde un gran número de perspectivas.

En particular, la técnica de *redes neuronales*, puede identificar los patrones de comportamiento de los clientes a partir de complejas interacciones entre variables de cuya información se dispone en las bases de datos, permitiendo extraer la información de las mismas de forma dirigida, construir muestras y analizarlas, y finalizado el proceso, extender los resultados a toda la base de datos en tiempos muy cortos. Una vez identificados perfiles y patrones de comportamiento, se puede realizar publicidad dirigida y marketing inteligente en general. Las redes neuronales ofrecen una poderosa herramienta de predicción basada en la detección de determinados comportamientos inicialmente ocultos en los datos. Existen otras técnicas de *data mining* como son las *técnicas de clasificación* de individuos en grupos según sus características (*análisis discriminante, análisis cluster, análisis logístico*, etc.) y las *técnicas de reducción de la dimensión* que permiten resumir de forma óptima un gran conjunto de información en los mínimos factores esenciales contenidos en ella con la mínima pérdida en exactitud (*análisis factorial, análisis en componentes principales, análisis de correspondencias* , etc.)

Por otra parte, se utilizan sistemas DSS (*Decision Support Solutions o Sistema de Apoyo a la Decisión*) término general que describe aplicaciones para el análisis de grandes cantidades de datos y la realización de gran variedad de cálculo y proyecciones. La extracción y el almacenamiento de datos son elementos complementarios en la mejora del acceso a los datos para la toma de decisiones. El almacenamiento de los datos es el mecanismo que facilita el Sistema de apoyo a la Decisión (DSS), almacenando los datos de la organización de una forma integrada.

El avance de las técnicas citadas tiene su reflejo en la finalidad de los ficheros inscritos en el Registro General de Protección de Datos. Así, el 30% de los ficheros inscritos en 1999 presenta finalidad de publicidad propia, el 14% presenta finalidad de prospecciones de mercado, el 11% presenta finalidad de encuestas de opinión y el 6% presenta finalidad de publicidad para terceros. Al comparar estas cifras con las relativas a ejercicios anteriores se observa una evolución creciente de las mismas, provocada en parte por el crecimiento de las nuevas técnicas emergentes de tratamiento de la información analizadas en los párrafos anteriores. Asimismo, también se encuentran inscritos ficheros que contemplan directamente finalidades como prospección, marketing, estudios de mercado y segmentación, entre otras.

Contemplado todo ello a la luz de la Ley 15/1999, que entrará en vigor en el año 2000, es de señalar las mayores exigencias que tanto en la información en el momento de la recogida del datos como en la prestación del consentimiento se contempla en la misma.

** Ficheros relacionados con Internet*

El desarrollo de las telecomunicaciones y su incidencia en las nuevas formas de comercio ha hecho que medios como Internet se hayan adueñado de una cuota de mercado considerable. Las empresas utilizan Internet, intranets y extra-

nets en sus relaciones con los clientes para ofrecer sus productos minimizando costes, optimizar su posición respecto de las empresas de la competencia y captar y fidelizar clientes. Internet permite la relación on-line con los clientes sin límites geográficos ni temporales. Esta relación adquiere su más alto grado de eficiencia al tratarse de una relación bidireccional e interactiva, con lo que su utilización en marketing y en investigación de mercados produce resultados muy provechosos y cuyos límites están todavía por descubrir.

La interactividad cliente-empresa citada en el apartado anterior califica a Internet como un medio de altas prestaciones en el mundo del marketing. El entorno de Internet se ha convertido en un nuevo canal de marketing de altas prestaciones debido a la interactividad que ofrece. Por otra parte, el fuerte desarrollo multimedia que ha tenido lugar en este medio hace que la relación con el cliente sea, además de eficiente, atractiva y con un entorno que hace aumentar las posibilidades de visitas repetidas a las páginas Web de las empresas. Estas visitas repetidas permiten personalizar la información que proviene de los distintos clientes permitiendo así acciones de perfilado, detección de patrones y fidelización de clientes, que son los objetivos más codiciados en al marketing moderno. Por otra parte, las empresas a través de Internet también difunden su oferta, su marca, su atención al cliente, y en definitiva explotan cualquier factor que pueda incidir en sus posición en el mercado y en sus ventas.

El avance de Internet también tiene su reflejo en la inscripción de los ficheros en el Registro General de Protección de Datos. Así, existen ficheros inscritos con datos personales de clientes resultantes de la promoción de productos del responsable a través de su página Web en Internet, ficheros de clientes de centros comerciales virtuales de distintas actividades (librerías, servicios financieros, directorios de empresas, etc.), ficheros de servicios bancarios a través de la Red, ficheros de usuarios de proveedores de servicios de Internet, ficheros de actividades de I+D de las universidades, directorios de servicios de arte español, fichero relativos a clubes y foros a través de Internet, ficheros de profesionales y empresas, ficheros de reclutamiento de personal para su posterior selección como trabajadores de empresas a través del currículum, ficheros con cupones para participaciones en sorteos, ficheros con datos de solicitantes de información de productos y servicios a través de la Red, bases de datos con fines publicitarios y promocionales, bases de datos de impagados y morosos y ficheros de marketing en general.

Paralelamente a lo que ocurre con los ficheros de publicidad y marketing en general, al comparar las cifras de ficheros inscritos en los últimos años con contenido y finalidad relacionado con Internet se observa una evolución creciente de las mismas, provocada por el rápido crecimiento del uso de la Red Internet en todas las facetas de la actividad y por el atractivo y la rentabilidad de este nuevo medio. No olvidemos que hoy en día es fácil, accesible y bastante económico utilizar la Red como medio para realizar actividades de cualquier sector económico, siendo posible situar de forma muy sencilla cualquier negocio en Internet, incluso de forma gratuita. El crecimiento de la inscripción de ficheros relacionados con Internet se ha acentuado en los dos últimos años, paralelamente al desarrollo intensivo de esta nueva tecnología de comunicación y negocio.

** Ficheros con transferencias internacionales autorizadas según el sector de actividad*

Salvo los países que proporcionan un nivel de protección equiparable al que presta la Ley española, para transferir datos a terceros países es necesario solicitar la preceptiva autorización de transferencia internacional según se detalla posteriormente.

Dada la relevancia que han adquirido los movimientos internacionales de datos por diversos motivos, como puede ser la centralización de recursos de las empresas para su tratamiento de forma globalizada, los nuevos sistemas de información y de la comunicación, las nuevas formas de mercado, los nuevos sistemas de gestión integrada de las compañías y otros factores similares, se hace necesario realizar un análisis por sectores de actividad de la inscripción en el Registro General de Protección de Datos de los ficheros privados que declaran transferencias internacionales de datos.

Las empresas del sector de las actividades informáticas ocupan un lugar importante en la inscripción de ficheros con transferencias internacionales de datos, generalmente con destino a Estados Unidos donde suele residir la empresa matriz. Los ficheros afectados suelen ser los que contienen datos personales y laborales de los empleados de la compañía, la gestión de recursos humanos en general, ficheros con datos de candidatos para reclutamiento y selección, ficheros de distribuidores independientes de productos comercializados por las compañías y otros ficheros de la actividad informática.

El sector bancario también suele notificar transferencias internacionales de datos en sus ficheros, generalmente en los referidos a operaciones de sus clientes, medios de pago y también recursos humanos.

Las entidades de seguros privados, por la naturaleza de su actividad también notifican transferencias internacionales de datos, afectando a ficheros de clientes y tomadores de seguros, a ficheros con datos de contratos de pólizas de automóviles referidos a sus conductores, ficheros con datos para gestión de los siniestros declarados con información de beneficiarios y perjudicados, ficheros con datos para la gestión del reaseguro y también ficheros de la propia gestión de personal y recursos humanos.

Las sociedades mediadoras en el mercado de dinero, del sector de actividades auxiliares a la intermediación financiera y de actividades bursátiles notifican ficheros con transferencias relativos a registros de ordenes de compraventa dadas por los clientes, relativos a datos personales y laborales de sus empleados, relativos a la compra de divisas en las oficinas internacionales y relativos a solicitudes de tarjetas como medio de pago y crédito.

Determinadas empresas del sector de estudios de mercado y encuestas de opinión declaran transferencias internacionales en sus ficheros por la necesidad de efectuar tratamientos masivos de datos en otros países por motivos

presupuestarios.

También son típicas las transferencias internacionales de datos en las empresas del sector de la consultoría y otras actividades de asesoría. Los ficheros afectados suelen ser como norma general los relativos a la gestión de recursos humanos.

El sector de actividad de las agencias de viajes, mayoristas y minoristas del turismo y otras actividades de apoyo turístico declaran transferencias en ficheros relativos a emisión de billetes y reservas de viajes de los pasajeros.

El sector del transporte aéreo transfiere datos internacionalmente con la finalidad de gestionar las relaciones contractuales asumidas con sus clientes a bases de datos del sistema de reservas y formas de pago.

El sector del alquiler de automóviles notifica ficheros que presentan transferencias internacionales de datos relativos a sus clientes y proveedores referidos a las reservas de automóviles, a las tarjetas de crédito, a la facturación y a la gestión del negocio.

El sector de la edición de libros y revistas transfiere datos internacionalmente relativos a ficheros de clientes y clientes potenciales necesarios para la relación negocial.

6. **FICHEROS DE TITULARIDAD PÚBLICA**

6.1. **EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS**

Al Registro General de Protección de Datos le corresponde la inscripción de las operaciones de creación, modificación o supresión de ficheros de las diferentes Administraciones Públicas. En este área, sobre ficheros de titularidad pública, en el transcurso del año 1999 se han reflejado en el Registro un total de 2.937 operaciones. De estos movimientos, a instancia de parte se han practicado 1.912 inscripciones de creación de ficheros, 268 modificaciones y 366 cancelaciones de inscripción. Asimismo, se realizaron 391 rectificaciones de oficio, de subsanación de errores, debido a la necesidad de normalización y adecuación de los datos consignados en la notificación de ficheros, en relación con las disposiciones de regulación de los mismos que se publican en los boletines oficiales.

Al finalizar el ejercicio, el número de ficheros de titularidad pública que constaban inscritos en el Registro es de 1.882. De ellos, el porcentaje más alto, con 1.385 ficheros, equivalente al 73% aproximadamente, corresponde a ficheros de la Administración Autonómica.

Por otra parte, la Administración Local en este año, ha solicitado la inscripción de 353 nuevos ficheros, lo que representa un 20% del total de ficheros inscritos en 1999, aunque tan sólo supone un aumento de un 1% respecto al total de municipios que ya constan inscritos en el Registro General de Protección de Datos. La distribución de los nuevos ficheros inscritos de Administración Local se reparte uniformemente por todo el territorio español, alcanzando una concentración mayor en Cataluña, concretamente en la provincia de Barcelona, donde los municipios pequeños han continuado encomendando a la Diputación de Barcelona la gestión informatizada del Padrón de Habitantes.

La inscripción de ficheros automatizados de datos personales de la Administración General del Estado, aunque estabilizada por haber declarado prácticamente todos sus ficheros en años anteriores, se ha incrementado en un 4% respecto a las cifras finales de 1998, lo que ha supuesto la inscripción de 124 nuevos ficheros. Destaca en este sector de la Administración la regularización de ficheros realizada por el Ministerio de Fomento mediante la publicación de una Orden Ministerial que recoge la relación actual de todos los ficheros existentes en el Departamento.

En el apartado de "Otras Personas Jurídico Públicas" el resultado de inscripciones nuevas ha sido prácticamente el mismo del año anterior con un incremento de 20 ficheros, correspondientes a Universidades de nueva creación, a las que se ha ido requiriendo según se ha tenido conocimiento de su puesta en marcha.

Analizando la inscripción de ficheros de titularidad pública, en función de la finalidad y los usos previstos en su creación, se puede apreciar que los porcentajes más elevados se corresponden con los ficheros destinados a la gestión de procedimientos administrativos (28%), gestión de estadísticas internas (27%), gestión tributaria y de recaudación (22%), gestión económica con terceros (19,5%), seguidos de la gestión de la función estadística pública (17,3%), gestión del padrón (14,4%) y gestión de personal (14,4%). Comparando este análisis con el realizado al finalizar el ejercicio anterior se puede apreciar que los resultados son prácticamente idénticos**,** indicando que la mayor parte de ficheros declarados por la Administración Pública y Organismos de titularidad pública corresponden a la gestión administrativa. Por otra parte, si se observan las tipificaciones de finalidades de los ficheros inscritos en este año llama la atención el fuerte incremento experimentado en ficheros de historiales clínicos (14,1%) y de gestión y control sanitario (12,6%), explicando estas cifras la notificación realizada por la Consejería de Sanidad de Canarias, que en 1999 ha regularizado la inscripción de los centros hospitalarios dependientes de dicha Comunidad Autónoma.

Respecto al tipo de datos registrados en los ficheros inscritos en el año 1999, es de resaltar, por tratarse de datos especialmente protegidos, de acuerdo al artículo 7 de la Ley Orgánica, la inscripción de 5 nuevos ficheros conteniendo datos especialmente protegidos, referidos a ideología, religión o creencias, correspondientes a ficheros de adopciones y tutelas, asistencia social y representaciones sindicales, contemplando todos ellos la recogida de este tipo de datos en sus disposiciones de creación.

Por otra parte, se ha producido un aumento significativo de inscripciones de ficheros conteniendo *otros datos especialmente protegidos* de salud, origen racial o vida sexual, ascendiendo en 1999 a 382 los ficheros declarados con esta tipología, correspondientes a las instituciones sanitarias dependientes de las Consejerías de Salud de las Comunidades Autónomas de Andalucía, Canarias, Castilla y León y Madrid, y a nuevos ficheros correspondientes con el Sistema de Información sobre los Usuarios de Servicios Sociales (SIUSS), también denominado "Ficha Social", aplicación informática desarrollada por el Ministerio de Trabajo y Asuntos Sociales, que se continúa implantando en las Corporaciones Locales del ámbito territorial de las Comunidades Autónomas que han suscrito el oportuno convenio con el Ministerio.

Mediante este sistema de información se recogen en soporte informático los datos de los usuarios de los servicios sociales generales que demandan asistencia o sobre los que se realiza algún proceso de intervención social a través de las Corporaciones Locales, poniendo el Ministerio, a disposición de las Comunidades Autónomas que lo convengan, un programa informático que da soporte a esta aplicación por éstas y por las Corporaciones Locales de su territorio.

Anualmente, las Comunidades Autónomas colaboradoras remiten los datos de las Corporaciones Locales correspondientes, excluidos los de identificación personal de los usuarios, al Ministerio de Trabajo y Asuntos Sociales, con el fin de que éste pueda planificar y realizar análisis de demanda, siempre tratando de mejorar la adecuación de los recursos existentes a las necesidades y demandas planteadas por los ciudadanos.

Desde la creación del Registro se aproxima a 300 el número de ficheros inscritos en el mismo para dar soporte a este sistema de información.

También en la categoría de ficheros con datos especialmente protegidos amparados en el artículo 7 de la Ley, se encuentran aquellos que contienen información sobre infracciones penales y/o administrativas. En el año 1999, se ha llevado a cabo la inscripción de 86 ficheros, pertenecientes a Policía Local y Protección Ciudadana de los Ayuntamientos de Madrid y Marbella, en la Administración Local. En las Comunidades Autónomas ha habido un fuerte incremento en ficheros con este tipo de datos proveniente de la Comunidad de Madrid, concretamente de la Agencia Antidroga, de la Agencia Madrileña de Tutela de Adultos y de diversos Centros Ocupacionales dependientes de esta Comunidad. En todos los casos, y como en los apartados anteriores, estos ficheros contemplan en sus disposiciones de creación la recogida de este tipo de datos.

6.2. **OPERACIONES DE OFICIO**

Durante 1999, las operaciones de rectificaciones de oficio con el objeto de subsanar errores de las notificaciones han ascendido a 391. Si se compara este dato con el correspondiente a 1998 en el que prácticamente se alcanzaban las 1.697 subsanaciones de oficio, y a 1997 y años anteriores, en los que se llegó a superar la cifra de 5.000 rectificaciones anuales, se constata una disminución considerable en este tipo de operaciones, de lo que podemos deducir que ha mejorado ostensiblemente la calidad en las declaraciones de los responsables.

Por otra parte, la distribución de estos movimientos a lo largo del año es uniforme, y corresponde, como ya se ha reseñado en memorias de años anteriores, a la necesidad que se ha tenido de establecer un procedimiento normalizado para inscribir el encuadramiento de los órganos responsables de los ficheros de titularidad pública, con el objetivo y finalidad de homogeneizar las inscripciones para facilitar su consulta, tanto en el propio Registro, como en los diferentes soportes en los que posteriormente se publican los ficheros declarados.

Se puede observar un aumento de este tipo de operaciones en el mes de abril, debido al proceso de depuración y subsanación que se realiza como consecuencia de la publicación del Catálogo de Ficheros del año 1998/1999, cuya edición se cerró el 31 de mayo de 1999.

6.2.1. **Actuaciones relacionadas con la Administración General del Estado**

Los ficheros de datos de carácter personal, de titularidad pública, han de ser notificados a la Agencia de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto ha elaborado la Agencia, de una copia de la disposición de creación del fichero.

Las disposiciones generales de creación o modificación de los ficheros automatizados de datos de carácter personal de la Administración General del Estado se publican en el Boletín Oficial del Estado, permitiendo realizar un seguimiento de su inscripción. Durante 1999 se han publicado en el Boletín, las siguientes disposiciones de carácter general que regulan nuevos ficheros o modifican alguno de los existentes en la Administración General del Estado y/o sus Organismos Autónomos:

- Orden de 11 de noviembre de 1999, del Ministerio de Sanidad y Consumo, por la que se amplía la Orden de 21 de julio de 1994, que regula los ficheros con datos de carácter personal gestionados por el Ministerio (BOE nº 290, de 4 de diciembre de 1999)

- Orden de 30 de septiembre de 1999, del Ministerio de Justicia, por la que se amplía el anexo de la Orden del Ministerio de Justicia e Interior del 26 de julio de 1994, incorporando los ficheros automatizados gestionados por el Centro de Estudios Jurídicos de la Administración de Justicia (CEJAJ) (BOE nº 270, de 11 de noviembre de 1999)

- Orden de 4 de octubre de 1999, del Ministerio de Fomento, por la que se actualiza la relación de ficheros automati-

zados de datos de carácter personal (BOE nº 252, de 21 de octubre de 1999)

- Orden de 6 de octubre de 1999, del Ministerio de Agricultura, Pesca y Alimentación, por la que se modifica la Orden de 26 de julio de 1994, que regula los ficheros de datos de carácter personal del Ministerio (BOE nº 246, de 14 de octubre de 1999)

- Orden de 30 de julio de 1999, del Ministerio de Defensa, por la que se modifica la Orden de 26 de julio de 1994, que regula los ficheros de tratamiento automatizado de datos de carácter personal existentes en el Ministerio (BOE nº 191, de 11 de agosto de 1999)

- Resolución de 28 de mayo de 1999, de la Comisión del Mercado de las Telecomunicaciones, por la que se crean los ficheros automatizados de datos de carácter personal (BOE nº 188, de 7 de agosto de 1999)

- Orden de 26 de julio de 1999, del Ministerio de Economía y Hacienda, por la que se regulan las bases de datos y ficheros automatizados de carácter personal existentes en la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda (BOE nº 186, de 5 de agosto de 1999)

- Orden de 1 de julio de 1999, del Ministerio del Interior, por la que se amplía la de 26 de julio de 1994, creando y regulando el fichero automatizado *sobre comunicaciones de vacaciones* (BOE nº 161, de 7 de julio de 1999)

- Orden de 24 de junio de 1999, del Ministerio del Interior, por la que se amplía la de 26 de julio de 1994, crando y regulando el fichero automatizado Locupol, sobre análisis de voz (BOE nº 155, de 30 de junio de 1999)

- Orden de 20 de mayo de 1999, del Ministerio de Industria y Energía, por la que se actualizan los anexos publicados mediante Orden de 26 de julio de 1994, modificados por Orden de 30 de septiembre de 1997, reguladora de los ficheros de tratamiento automatizado de datos de carácter personal del Ministerio (BOE nº 131, de 2 de junio de 1999)

- Orden de 15 de abril de 1999, del Ministerio de Sanidad y Consumo, por la que se modifica la Orden de 21 de julio de 1994, reguladora de los ficheros con datos de carácter personal gestionados por el Ministerio (BOE nº 100, de 27 de abril de 1999)

- Orden de 26 de marzo de 1999, del Ministerio de Trabajo y Asuntos Sociales, por la que se crean y modifican ficheros automatizados de datos de carácter personal (BOE nº 84, de 8 de abril de 1999)

- Orden de 19 de enero de 1999, del Ministerio de Sanidad y Consumo, por la que se amplía la Orden de 21 de julio de 1994, que regula los ficheros con datos de carácter personal gestionados por el Ministerio (BOE nº 25, de 29 de enero de 1999)

- Orden de 21 de diciembre de 1998, del Ministerio de Defensa, por la que se modifica la Orden 75/1994, de 26 de julio, por la que se regulan los ficheros de tratamiento automatizado de datos de carácter personal existentes en el Ministerio (BOE nº 8, de 9 de enero de 1999).

De estas disposiciones cabe destacar la Orden del Ministerio de Fomento. Los ficheros de este Ministerio se encontraban regulados en la Orden de 21 de julio de 1994 del Ministerio de Obras Públicas, Transportes y Medio Ambiente. Con la nueva estructura por la que se crean los Ministerios de Fomento y Medio Ambiente, habían quedado desactualizados los ficheros del Departamento. Esta disposición ha venido a recopilar todos los ficheros existentes en este Ministerio, tanto los que habían pertenecido al anterior Ministerio de Obras Públicas, Transportes y Medio Ambiente y por reparto de competencias se transferían a Fomento, como algunos otros de nueva creación.

La Comisión del Mercado de las Telecomunicaciones, procedió a publicar una disposición de creación de ficheros, a requerimiento de la Agencia toda vez que no constaba inscripción de ficheros en el Registro General de Protección de Datos. Así también, ha ocurrido con los correspondientes a la gestión de certificaciones electrónicas de la Fábrica Nacional de Moneda y Timbre.

Las Ordenes del Ministerio de Sanidad y Consumo de 19 de enero y 15 de abril de 1999, corresponden a sendas modificaciones realizadas en el fichero denominado GESTIÓN DE PRESTACIÓN FARMACEÚTICA, creado mediante la Orden de 21 de julio de 1994 (BOE 178, de 27 de julio), cuyo responsable es el Instituto Nacional de la Salud.

En la primera Orden de 19 de enero, ya se contemplaba la existencia de datos sanitarios, sin embargo, en el apartado *de Personas o Colectivos sobre los que se obtienen datos* no se había incluido el colectivo de usuarios del INSALUD, por lo que fue precisa la publicación de la siguiente Orden de 15 de abril de 1999.

Una vez publicadas las modificaciones oportunas se procedió por parte el INSALUD a la notificación al Registro, quedando inscrito un fichero correspondiente al sistema de centralización de información del INSALUD, así como uno por cada una de las Delegaciones Provinciales del INSALUD, en los que se realiza la captura en el ámbito provincial, de la información sobre las recetas emitidas por el INSALUD, el facultativo que las emite y las oficinas farmacéuticas que las dispensan.

6.2.2. **Actuaciones relacionadas con la Administración Autonómica.**

Como se indicaba en la memoria del año anterior, desde la inscripción inicial de los ficheros de Comunidades Autónomas, a raíz de la creación de la Agencia se habían producido reestructuraciones orgánicas en esta Administración que no habían tenido reflejo en el Registro General de Protección de Datos.

Por este motivo, una de las funciones más importantes encomendadas al Registro, como es la de velar por la publicidad de los ficheros en él inscritos, facilitando al ciudadano las direcciones de los responsable de ficheros, no se estaba cumpliendo convenientemente, lo que motivó que el Director de la Agencia se dirigiese al Consejero encargado de la coordinación entre Departamentos de cada Comunidad Autónoma, informándole de los siguientes puntos:

* La obligación de cada responsable de ficheros automatizados de inscribir y mantener actualizada la inscripción en el Registro de estos ficheros.

* La importancia de la revisión de la actual inscripción, debido al impulso del uso de las nuevas tecnologías en la Administración y la posibilidad de haberse creado nuevos ficheros automatizados.

* Necesidad del análisis de las normas legales que establecen la creación de Registros Nacionales, con objeto de mantener la eficiencia y coordinación de medios estatales, que a su vez, se actualizan a partir de ficheros de las Comunidades Autónomas.

A finales de 1998, ya se habían recibido contestaciones de algunas Comunidades Autónomas, indicando que estaban procediendo a realizar los trámites administrativos oportunos, para adecuar la inscripción de ficheros a las situaciones reales de los mismos. Concretamente, en 1998 se inscribieron 179 nuevos ficheros.

Durante el año 1999, se ha recibido la contestación, o se ha completado la enviada en 1998, de las Comunidades de Andalucía, Aragón, Asturias, Canarias, Cantabria, Castilla La Mancha, Castilla y León, Cataluña, Galicia, Madrid, Navarra, La Rioja, País Vasco, y Valencia, inscribiéndose 1.385 nuevos ficheros. Este aumento es bastante elevado si se compara con otros años, y se ha debido por una parte a la inscripción de los ficheros de gestión hospitalaria de la Comunidad Autónoma de Canarias, que estaba pendiente de normalizar, y de las Comunidades de Andalucía y Castilla León, que también tenían pendientes de inscripción algunos sectores de su administración, y por otra parte, se ha visto significativamente incrementado por la inscripción de la Comunidad de Madrid.

A continuación se relacionan las disposiciones de carácter general de creación, modificación o supresión de ficheros de la Administración de las Comunidades Autónomas publicadas en los respectivos Diarios Oficiales durante 1999, que han dado lugar a la notificación de ficheros en el Registro General de Protección de Datos:

- Orden de 22 de septiembre de 1999, que actualiza los ficheros automatizados con datos personales de la Consejería de Medio Ambiente de la Junta de Andalucía (BOJA nº 119, de 14 de octubre de 1999)

- Orden de 30 de julio de 1999, reguladora de los ficheros automatizados con datos personales de las Delegaciones Provinciales de la Consejería de Salud de la Junta de Andalucía (BOJA nº 97, de 21 de agosto de 1999)

- Orden de 11 de enero de 1999 por la que se crean ficheros de tratamiento automatizado con datos de carácter personal de la Consejería de Salud de la Junta de Andalucía (BOJA nº 14, de 2 de febrero de 1999)

- Orden de 15 de junio de 1999, por la que se crean ficheros automatizados con datos personales por la Empresa Pública Hospital de Poniente de Almería (BOJA nº 76, de 3 de julio de 1999)

- Orden de 8 de junio de 1999, regulando el fichero automatizado con datos de carácter personal de Bastanteos del Departamento de Presidencia y Relaciones Institucionales de la Diputación de Aragón (DOA nº 75, de 16 de junio de 1999)

- Orden de 11 de junio de 1999, de Vicepresidencia del Gobierno de Canarias, por la que se crean y regulan los ficheros automatizados del Servicio de Atención de Urgencias y Emergencias 112 (BOC nº 100, de 28 de julio de 1999)

- Orden de 19 de agosto de 1998, reguladora de los ficheros automatizados con datos personales del Servicio Canario de Salud (BOC nº 130, de 14 de octubre de 1999)

- Decreto 119 de 13 de octubre de 1999, regulador del Registro de Títulos Académicos y Profesionales de la Comunidad Autónoma de Cantabria (BOC nº 207, de 10 de octubre de 1999)

- Decreto 189 de 13 de julio de 1999, que modifica el Decreto 359 de 29 de noviembre de 1994, regulador de los ficheros automatizados del Departamento de Bienestar Social de la Generalidad de Cataluña (DOGC nº 2940, de 28 de julio de 1999)

- Decreto 274/1999, de 13 de octubre de 1999, de creación del fichero automatizado de datos de carácter personal del Centro de Emergencias 112 de la Generalidad de Cataluña (DOGC nº 2741, de 25 de octubre de 1999)

- Orden de 22 de noviembre de 1999, del Departamento de Presidencia y Relaciones Institucionales, regulador del fichero automatizado con datos personales relativo a parejas estables no casadas (DOGC nº 157, de 10 de diciembre de 1999)

- Decreto 288/1999, de 26 de octubre, del Departamento de Sanidad y Seguridad Social, por el que se regula el uso de la Tarjeta Sanitaria Individual a efectos del acceso a la prestación farmacéutica y se modifica el fichero con datos de carácter personal denominado Farmacias (DOGC nº 3013, de 11 de noviembre de 1999)

- Orden de 31 de mayo de 1999, por la que se regulan los ficheros automatizados con datos personales de la Conseje - ría de Justicia, Interior y Relaciones Laborales de la Junta de Galicia (DOGA nº 114, de 16 de junio de 1999)

- Modificación de la Orden de 31 de mayo de 1999, por la que se regulan los ficheros automatizados con datos perso - nales de la Consejería de Justicia, Interior y Relaciones Laborales de la Junta de Galicia (DOGA nº 148, de 3 de agosto de 1999)

- Orden 35/99 de 7 de mayo, de la Consejería de Educación, Cultura, Juventud y Deportes de la Comunidad Autónoma de La Rioja, que regula ficheros automatizados con datos de carácter personal (BOR nº 63, de 22 de mayo de 1999)

- Orden de 7 de junio de 1999, de la Vicepresidencia del Gobierno Vasco, por la que se amplía en anexo II de la Orden de 17 de noviembre de 1997, reguladora de los ficheros automatizados del Departamento de Hacienda y Administra - ción Pública (BOPV nº 132, de 13 de julio de 1999)

- Orden de 25 de febrero de 1999, reguladora de ficheros automatizados con datos personales del Departamento de Sanidad del Gobierno Vasco (BOPV nº 47, de 9 de marzo de 1999)

- Resolución de 26 de abril de 1999, de la Consejería de Cultura, reguladora del fichero informatizado con datos personales de Gestión del Plan Formativo del Principado de Asturias (BOPA nº 107, de 11 de mayo de 1999)

- Resolución de 16 de diciembre de 1998, de la Consejería de Industria, Turismo y Empleo, por la que se suprimen los ficheros de carácter personal de la extinta Agencia Regional de Empleo del Principado de Asturias (BOPA nº 12, de 16 de enero de 1999)

- Resolución de 13 de octubre de 1999, de la Consejería de Salud y Servicios Sanitarios del Principado de Asturias, reguladora del fichero automatizado con datos personales de Enfermedades Laborales Centinela (BOPA n1 255, de 4 de noviembre de 1999)

- Resolución de 7 de enero de 1999, de la Consejería de Sanidad y Servicios Sociales del Principado de Asturias, que deja sin efecto la de 29 de diciembre de 1994 y regula nuevos ficheros automatizados con datos personales de la Consejería (BOPA nº 18, de 23 de enero de 1999)

- Decreto 40/1999, de 8 de marzo, regulador de ficheros automatizados con datos personales de la Comunidad Autó - noma de Castilla y León (BOCyL nº 47, de 10 de marzo de 1999)

- Orden de 26 de julio de 1999, reguladora de los ficheros automatizados con datos personales de la Consejería de Sanidad y Bienestar Social de la Comunidad Autónoma de Castilla y León (BOCyL nº 148, de 3 de agosto de 1999)

- Orden Foral 171/1999, del Consejero de Presidencia e Interior, por la que se crea el fichero informatizado Atención de Emergencias de la Comunidad Foral de Navarra (BON nº 110, de 3 de septiembre de 1999)

Por otra parte, el artículo 40 de la LORTAD, dispone que las funciones de la Agencia de Protección de Datos reguladas en su artículo 36, a excepción de las mencionadas en los apartados j), k), y l) y en los apartados f) y g) en lo que se refiere a transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas por los órganos correspondientes de cada Comunidad, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por la propia Comunidad Autónoma.

Hay que hacer mención especial al nuevo artículo 41 de la Ley 15/1999, en relación las competencias que transfiere a los Organos correspondientes de las Comunidades Autónomas, ya que amplía el ámbito de aplicación a los ficheros de datos de carácter personal creados o gestionados por la Administración Local de su ámbito territorial.

En el Registro General de Protección de Datos serán objeto de inscripción los ficheros automatizados que sean titulares las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros que se puedan crear de conformidad con el artículo 40.2 de la Ley.

A su vez, el apartado 2 del artículo 40 de la LORTAD habilita a las Comunidades Autónomas a crear y mantener sus propios registros de ficheros públicos, respecto de los archivos informatizados cuyos titulares sean los órganos de las respectivas Comunidades Autónomas.

La Agencia de Protección de Datos de la Comunidad de Madrid es la primera agencia autonómica creada por la Ley 13/1995, de 21 de abril, de Regulación del Uso de la Informática en el Tratamiento de Datos Personales por la Comu - nidad de Madrid, que desde julio de 1997, viene desarrollando sus competencias.

Durante 1999 se ha continuado manteniendo una estrecha relación entre la Agencia de Protección de Datos de la Comunidad de Madrid y este Registro, tal como se ha venido haciendo desde la creación de esta Agencia Autonómica.

También en este año, se ha materializado el compromiso de esta Agencia Autonómica, de hacer llegar al Registro General de Protección de Datos la notificación, para su inscripción, de todos los ficheros de la Comunidad Autónoma, con el fin de facilitar a los responsables de los ficheros la doble obligación de inscripción de los mismos en la Agencia de Protección de Datos y en la Agencia de Protección de Datos de la Comunidad de Madrid.

Tras realizarse por parte de la Agencia de Madrid, la adecuación de su sistema informático para ajustarse a los requerimientos establecidos por la Resolución de 23 de junio de 1994, de la Agencia de Protección de Datos, y las pruebas llevadas a cabo durante 1998, en los primeros meses de 1999, se realizó la actualización de la inscripción de la totalidad de los ficheros pertenecientes a los diferentes centros directivos de esta Comunidad, lo que ha supuesto la inscripción de 856 nuevos ficheros.

La operación registral realizada en el Registro General de Protección de Datos, ha consistido en suprimir la inscripción de 234 ficheros que constaban inscritos con anterioridad a la entrada en funcionamiento de la Agencia de Protección de Datos de la Comunidad de Madrid y el alta de los nuevos ficheros habilitados por el Decreto 133/1997, de creación de nuevos ficheros y la adaptación de la norma reguladora a las especificaciones de la Ley de Protección de Datos de la Comunidad de Madrid.

Con posterioridad, han sido publicados en el Boletín Oficial de la Comunidad de Madrid, las siguientes disposiciones de creación, modificación y supresión de ficheros de datos de carácter personal creados por la propia Comunidad Autónoma de Madrid:

* Decreto 7/98, de 15 de enero, de la Consejería de Hacienda, por el que se crean ficheros automatizados de datos de carácter personal de la Empresa Pública "Madrid 112, Sociedad Anónima" (BOCM 25 de 30 de enero de 1998)

* Decreto 15/98, de 5 de febrero, del Consejero de Gobierno por el que se crea el fichero de datos de carácter personal de residentes fallecidos en la Comunidad Autónoma de Madrid (BOCM 43 de 20 de febrero de 1998)

* Decreto 63 de la Consejería de Economía y Empleo de la Comunidad de Madrid, de 23 de abril de 1998, de creación de nuevos ficheros de datos de carácter personal, (BOCM nº 104, de 4 de mayo de 1998).

* Decreto 105 de 18 de junio de 1998 del Consejo de Gobierno por el que se crean y modifican ficheros automatizados de datos de carácter personal en la Consejería de Presidencia de la Comunidad Autónoma de Madrid (BOCM 154 de 1 de julio de 1998)

* Decreto 129 de 3 de julio de 1998, de la Consejería de Educación y Cultura de la Comunidad de Madrid, de creación del fichero MADRIMASD, de datos de carácter personal (BOCM 161 de 9 de julio de 1998)

* Decreto 127 de 2 de julio de 1998 por el que se crean los ficheros que contienen datos de carácter personal de la Agencia de Protección de Datos de la Comunidad de Madrid (BOCM 164 de 13 de julio de 1998)

* Decreto 225 de 30 de diciembre de 1998, del Consejo de Gobierno de la Comunidad de Madrid, por el que se crea un fichero automatizado de datos de carácter personal de la Agencia de Protección de Datos de la Comunidad de Madrid (BOCM 16 de 20 de enero de 1999)

- Decreto 2/1999, de 7 de enero, de la Consejería de Educación y Cultura, regulador de los ficheros automatizados con datos personales del organismo autónomo Instituto Madrileño del Deporte (BOCM nº 11 de 14 de enero de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal (BOCM nº 24, de 29 de enero de 1999)

- Decreto 23/1999 de 11 de febrero, de la Consejería de Hacienda, regulador de los ficheros automatizados con datos personales del Canal de Isabel II (BOCM nº 45, de 23 de febrero de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Presidencia (BOCM nº 62, de 15 de marzo de 1999)

- Decreto 38/1999 de 4 de marzo, de la Consejería de Medio Ambiente y Desarrollo Regional, regulador de los ficheros automatizados con datos personales de la Consejería (BOCM nº 71, de 25 de marzo de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Economía y Empleo (BOCM nº 76, de 31 de marzo de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Sanidad y Servicios Sociales (BOCM nº 83, de 9 de abril de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Economía y Empleo (BOCM nº 82, de 8 de abril de 1999)

- Decreto 49/1999 de 8 de abril, de la Consejería de Educación y Cultura, por el que se actualizan los ficheros de datos personales de la Consejería (BOCM nº 98, de 27 de abril de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Obras Públicas, Urbanismo y Transportes (BOCM nº 103, de 3 de mayo de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Economía y Empleo (BOCM nº 119, de 21 de mayo de 1999)

- Decreto 66/99, de 13 de mayo, de la Consejería de Economía y Empleo, regulador de los ficheros automatizados con datos personales del Instituto Madrileño para la Formación - IMAF (BOCM nº 119, de 21 de mayo de 1999)

- Decreto 68/1999 de 13 de mayo, de la Consejería de Sanidad y Servicios Sociales, sobre creación de ficheros de datos de carácter personal en el Servicio Regional de Bienestar Social (BOCM nº 125, de 28 de mayo de 1999)

- Decreto 75/1999 de 27 de mayo, de Consejería de Presidencia, por el que se modifican los ficheros automatizados con datos personales del Ente Público de Radio Televisión Madrid (BOCM nº 133 de 7 de junio de 1999)

- Decreto 77/99, de 27 de mayo, regulador de ficheros automatizados con datos personales de la Consejería de Economía y Empleo (BOCM nº 134, de 8 de junio de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal en la Consejería de Obras Públicas, Urbanismo y Transportes (BOCM nº 137, de 11 de junio de 1999)

- Decreto 82/1999 de 3 de junio, regulador ficheros automatizados con datos personales de la Consejería de Medio Ambiente y Desarrollo Regional (BOCM nº 137, de 11 de junio de 1999)

- Decreto de Consejo de Gobierno, de la Comunidad de Madrid, sobre creación de ficheros de datos de carácter personal (BOCM nº 143, de 18 de junio de 1999)

- Decreto 84/1999, de 10 de junio, de la Consejería de Economía y Empleo, regulador de los ficheros automatizados con datos personales de la Agencia para la Formación de la Comunidad de Madrid (BOCM nº 146, de 22 de junio de 1999)

- Decreto 87/1999 de 10 de junio, de la Consejería de Sanidad y Servicios Sociales, regulador de ficheros automatizados con datos personales de la Dirección General de la Mujer (BOCM nº 147, de 23 de junio de 1999)

- Decreto 88/1999 de 10 de junio, de la Consejería de Sanidad y Servicios Sociales, regulador de ficheros automatizados con datos personales del Servicio Regional de Salud (BOCM nº 147, de 23 de junio de 1999)

- Decreto 90/1999 de 10 de junio, de la Consejería de Sanidad y Servicios Sociales, regulador de ficheros automatizados con datos personales del Instituto Madrileño del Menor y la Familia (BOCM nº 146, de 22 de junio de 1999)

- Decreto 94/1999 de 17 de junio, de la Consejería de Hacienda, regulador de los ficheros automatizados con datos personales de la Consejería (BOCM nº 149, de 25 de junio de 1999)

Aunque la Comunidad Valenciana no tiene un órgano autonómico de los previstos en el artículo 40 de la LORTAD, ha creado mediante el Decreto 96/98, de 6 de julio, del Gobierno Valenciano el Registro de Ficheros Informatizados en el ámbito de la Administración de la Generalidad Valenciana.

Tras los encuentros mantenidos en el año anterior entre representantes de la Generalidad Valenciana y la Agencia de Protección de Datos con el fin de establecer los mecanismos de comunicación y coordinación entre ambos, en 1999 entra en funcionamiento el Registro de Ficheros Informatizados previsto en el Decreto 96/98 citado anteriormente.

El Registro de Ficheros Informatizados es un órgano integrado en la Generalidad Valenciana para coordinar las actuaciones previstas, en materias registrales, en la normativa de protección de datos personales. Sus funciones son las siguientes:

- Notificar al Registro General de Protección de Datos los expedientes de inscripción, modificación y cancelación de ficheros informatizados, de conformidad con el procedimiento previsto en la normativa de aplicación.

- Rectificar de oficio los errores materiales de los asientos inscritos en su Registro.

- Elaborar la relación anual de los ficheros informatizados con datos de carácter personal dependientes de la Administración de la Generalidad Valenciana, dando a la misma la oportuna publicidad.

En relación con la primera de estas funciones, durante 1999, se ha iniciado la recepción de notificaciones de la administración de la Comunidad Valenciana, a través del Registro de Ficheros Informatizados, según el procedimiento establecido en el Decreto 96/98, que se detalla a continuación:

Los órganos dependientes de la Administración de la Generalidad Valenciana que pretenden la creación de un fichero automatizado que contenga datos de carácter personal, lo notifican previamente al Registro de Ficheros Informatizados cumplimentando el modelo normalizado de la Agencia de Protección de Datos.

Una vez aprobada por la Consejería correspondiente, como órgano competente en la materia, la disposición general de creación del fichero informatizado, según lo dispuesto en el artículo 18 de la Ley Orgánica 5/92, el Registro de Ficheros Informatizados da traslado del modelo cumplimentado, junto con una copia de la norma de creación del fichero, a la Agencia de Protección de Datos a los efectos de su inscripción en el Registro General de Protección de Datos.

Inscrito el fichero en el Registro General de Protección de Datos, se procede a la inscripción de oficio en el Registro de la Administración de la Generalidad Valenciana.

Durante 1999, las disposiciones generales de creación, modificación o supresión de ficheros de la administración de la Generalidad Valenciana, publicadas en el Diario Oficial de la Generalidad Valenciana han sido las siguientes:

- Orden del 28 de abril de 1999, por la que se crean ficheros automatizados con datos personales en la Consejería de Empleo, Industria y Comercio de la Generalidad Valenciana (DOGV nº 3504, de 27 de mayo de 1999)

- Orden de 12 de julio de 1999, por la que se actualiza la relación de ficheros automatizados de la Consejería de Obras Públicas, Urbanismo y Transporte de la Generalidad Valencia (DOGV nº 3550, de 30 de julio de 1999)

- Decreto 126/1999, de 16 de agosto, del Gobierno Valenciano, por el que se crea el Sistema de Información Poblacional de la Consejería de Sanidad (DOGV nº 3566, de 23 de agosto de 1999)

- Orden de 20 de septiembre de 1999, del Consejero de Industria y Comercio, por la que se crea el fichero automatizado R.E.D.E.S. de la Generalidad Valenciana (DOGV nº 3605, de 15 de octubre de 1999)

- Orden de 23 de septiembre de 1999, del Consejero de Sanidad, por la que se crean ficheros informatizados (DOGV nº 3644, de 14 de diciembre de 1999)

- Orden de 24 de noviembre de 1999 reguladora del fichero automatizado con datos personales de las visitas de la Consejería de Justicia y Administraciones Públicas de la Generalidad Valenciana (DOGV nº 3649, de 21 de diciembre de 1999)

- Orden de 16 de noviembre de 1999, de la Consellería de Bienestar Social, por la que se actualizan los ficheros de tratamiento automatizado de datos de carácter personal de esta Consellería (DOGV nº 3649, de 21 de diciembre de 1999)

A través del Registro de Ficheros Informatizados de la Generalidad Valenciana se ha recibido notificación para su inscripción en el Registro General de Protección de Datos de todas ellas, excepto de las publicadas en el mes de diciembre, que se esperan recibir en el primer trimestre del año 2000.

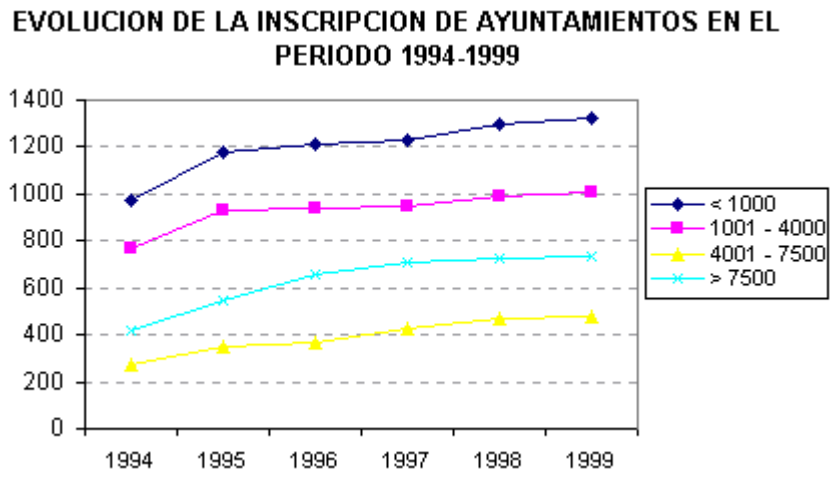
6.2.3. **Actuaciones relacionadas con Administración Local**

La inscripción de los ficheros automatizados pertenecientes a las Entidades de la Administración Local, que en años anteriores suponía el porcentaje más elevado de altas registrales de ficheros de titularidad pública, en 1999 apenas ha alcanzado el 20% de dichas altas. No obstante, en datos comparativos con el total de ficheros inscritos de titularidad pública, 23.320 ficheros, al finalizar 1999, se observa que la inscripción que corresponde a la Administración Local supone el 76,6% de la inscripción total.

La distribución de Entidades Locales que han formalizado la inscripción de sus ficheros en el Registro, y las que no han cumplido con esta obligación, se puede observar en la siguiente tabla, en función del número de habitantes de sus municipios.

HABITANTES	MUNICIPIOS	INSCRITOS	POR INSCRIBIR	% PENDIENTES
< 1000	4.898	1.327	3.571	72,9
1001 – 4000	1.885	1.005	880	46,7
4001 – 7500	540	478	62	11,5
> 7500	764	734	30	3,9
Total	8.087	3.544	4.543	56,1

En el siguiente gráfico, se puede apreciar la evolución de inscripciones de ficheros automatizados de Entidades Locales en los últimos ejercicios.



En el transcurso de los años precedentes al del ejercicio que se cierra con esta memoria, se han efectuado reiterados requerimientos a los responsables de los Ayuntamientos con una población superior a los 4.000 habitantes, recordándoles sus obligaciones en relación con la notificación e inscripción de los ficheros de datos de carácter personal existentes en cada Ayuntamiento. Como consecuencia de estos requerimientos a 31 de diciembre de 1998, eran 71 los Ayuntamientos con una población comprendida entre 4.000 y 7.500 habitantes, y 43 los de población superior a 7.500 habitantes, en total 134, los Ayuntamientos que no habían notificado sus ficheros a la Agencia.

Finalizando 1998, el Director de la Agencia, puso este hecho en conocimiento del Consejo Consultivo de la Agencia, del que forma parte un representante de la Federación Española de Municipios y Provincias, siendo en enero de 1999, cuando se produce la comunicación formal y reiterándose de nuevo, en julio de 1999, al representante de dicha Federación en el Consejo.

Como resultado se puede observar que durante el año 1999, únicamente han formalizado su inscripción 22 Ayuntamientos de los que figuraban como pendientes de inscribir.

Es de resaltar en esta memoria, el hecho de haberse producido en 1999 la inscripción de los ficheros del Ayuntamiento de Ourense, último Ayuntamiento de capital de provincia pendiente de inscripción de sus ficheros en el Registro General de Protección de Datos.

El incremento de Ayuntamientos inscritos en 1999 correspondientes a municipios con menos de 4.000 habitantes corresponde en su práctica totalidad a la provincia de Barcelona debido a la colaboración, ya iniciada el año anterior, de la Diputación de Barcelona.

- Participación de las Diputaciones en la gestión informatizada del padrón municipal.

La Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, y las normas que la desarrollan y modifican, dictan las instrucciones técnicas a los Ayuntamientos sobre la gestión y revisión del padrón municipal, estableciendo el cauce de participación de las Diputaciones Provinciales, Cabildos y Consejos Insulares en la gestión informatizada del Padrón de habitantes de los municipios con escasez de recursos.

El nuevo texto del Reglamento de Población y Demarcación Territorial de las Entidades Locales, regula el padrón municipal y en su artículo 60.1 dispone: *La formación, actualización, revisión y custodia del padrón municipal corresponde al Ayuntamiento, de acuerdo con las normas aprobadas conjuntamente por el Ministerio de Economía y Hacienda y el Ministerio de Administraciones Públicas a propuesta del Consejo de Empadronamiento.* Mas adelante continua el artículo 60.2, todos los padrones municipales se gestionarán por medios informáticos.

La Ley 4/1996, normaliza la gestión continua e informatizada del padrón municipal, establece que la gestión del padrón municipal se llevará por los Ayuntamientos, con medios informáticos. Y señala este mismo artículo que las Diputaciones Provinciales, Cabildos y Consejos insulares asumirán la gestión informatizada de los Padrones de los municipios que, por su insuficiente capacidad económica y de gestión, no puedan mantener los datos de forma automatizada.

El artículo 15 de la Ley 30/92, dispone que la realización de actividades de carácter material, técnico o de servicios de la competencia de los órganos administrativos o de las Entidades de derecho público podrá ser encomendada a otros órganos o Entidades de la misma o de distinta Administración, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño, sin que la encomienda de gestión suponga cesión de titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda.

Amparándose en esta normativa legal, la Diputación de Barcelona, a través de su Comisión de Gobierno, aprobó un Convenio Tipo sobre la asunción de la Gestión Informatizada del Padrón de Habitantes, dándole publicidad en el Boletín Oficial de la Provincia de Barcelona nº 163, de 9 de julio de 1997. Este Convenio permite a aquellos Ayuntamientos de la provincia que no disponen de los medios necesarios para llevar a cabo la gestión informatizada del padrón municipal, encomendar esta tarea a la Diputación, sin perder la titularidad del fichero, y, por tanto, es el Ayuntamiento correspondiente el responsable del cumplimiento de las obligaciones señaladas en el artículo 18 de la Ley Orgánica 5/1992. Sin embargo, la Diputación como encargada del tratamiento, adopta las medidas necesarias para garantizar la seguridad de la información de los padrones municipales almacenada en sus bases de datos, así como en las comunicaciones, en las operaciones de intercambio con otras Administraciones y en las consultas o transacciones telemáticas realizadas por el propio Ayuntamiento.

Mediante este Convenio, en el año 1997, fueron 68 los Ayuntamientos que encomendaron a la Diputación de Barcelona la gestión de la informatización del padrón de habitantes, que incluye la tramitación en el Registro de la inscripción de los ficheros correspondientes a estos municipios. La formalización de la inscripción en le Registro para los Ayuntamientos de este grupo que no habían realizado anteriormente la notificación de su fichero de Padrón se han continuado realizando durante el año 1999.

En 1998 se produjeron nuevos acuerdos de este tipo con otros 100 Ayuntamientos de Barcelona, y en 1999 estos han alcanzado a 43 nuevos Ayuntamientos.

- Policía Local.

Como consecuencia de las actividades efectuadas durante 1998 en una muestra de Ayuntamientos seleccionados por la Inspección de Datos sobre ficheros con fines de gestión policial, se detectó que algunos de ellos no habían procedido a notificar este tipo de ficheros para su inscripción en el Registro. Al finalizar 1998, únicamente quedaba pendiente de notificar la inscripción de sus ficheros el Ayuntamiento de Marbella, por lo que se remitió el asunto a la Inspección de Datos para que adoptara las medidas oportunas. En fecha 29 de abril de 1999, se recibió la notificación correspondiente habiéndose procedido a la inscripción de los mismos en fecha 7 de mayo de 1999.

6.2.4. **Actuaciones relacionadas con Universidades**

Como ya se indicaba en la memoria del año anterior, a finales de 1998 se requirió a nueve Universidades que se encontraban creadas, y que no habían realizado la inscripción de sus ficheros.

Todas ellas han inscrito sus ficheros en 1999 a excepción de la Universidad Pablo de Olavide de Sevilla y la Universidad Rey Juan Carlos por ser de tan reciente creación, habiendo comunicado que están en periodo de puesta en marcha de sus sistemas informáticos y que tan pronto como estén operativos, notificarán los ficheros para su inscripción en el Registro.

7. **MOVIMIENTOS INTERNACIONALES DE DATOS**

El Real Decreto 1332/1994, de 20 de Junio, por el que se desarrollan diferentes aspectos de la Ley, en su artículo 1.6 define la transferencia de datos como el "transporte de datos entre sistemas informáticos, por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por otro medio convencional".

La Ley Orgánica 5/1992, como se desprende del párrafo segundo del punto cuarto de su Exposición de Motivos, presta especial atención a la transmisión internacional de datos. En este punto, la Ley aplica el artículo 12 del Convenio 108 del Consejo de Europa, estableciendo así una regulación del concepto de "flujo transfronterizo de datos". La protección de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituyen una auténtica necesidad de la vida actual, de la que, las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional son simples ejemplos. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la transferencia con la autorización del Director de la Agencia cuando tal sistema no exista y siempre que se ofrezcan garantías suficientes por parte del responsable del fichero. De esta forma, no solo se cumple con la exigencia lógica de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuenten con garantías adecuadas, sino también con las previsiones de normas internacionales como el Acuerdo de Schengen o futuras normas comunitarias.

Así, en el Título V, artículo 32 de la LORTAD, se indica que "no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable, salvo que, además de haberse observado lo dispuesto en la Ley, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen las garantías adecuadas".

La autorización del Director deberá ser sometida al cumplimiento de las condiciones o cargas modales que se consideren necesarias para que de la transferencia no se deriven perjuicios a los derechos de los afectados y se respeten los principios de protección de datos.

No es necesaria la autorización previa en los siguientes supuestos:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España y en particular:

1. Las transmisiones de datos registrados en ficheros creados por las Fuerzas y Cuerpos de Seguridad en función de una investigación concreta, hechas por conducto de Interpol u otras vías previstas en convenios en los que España sea parte, cuando las necesidades de la investigación en curso exijan la transmisión a servicios policiales de otros Estados.

2. Las transmisiones de datos registrados en la parte nacional española del Sistema de Información Schengen con destino a la unidad de apoyo del sistema, a los solos efectos de una investigación policial en curso que requiera la utilización de datos del sistema.

3. Las transmisiones de datos previstas en el sistema de intercambios de información contemplado en el Título VI del Tratado de la Unión Europea.

4. De las transmisiones de los datos registrados en los ficheros creados por las Administraciones Tributarias, en favor de los demás Estados miembros de la Unión Europea o en favor de otros Estados terceros, en virtud de lo dispuesto en los convenios internacionales de asistencia mutua en materia tributaria.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

7.1. **LA DIRECTIVA EUROPEA, LA NUEVA LEY 15/1999 Y LA TRANSFERENCIA DE DATOS A TERCEROS PAÍSES**

En octubre de 1998 entró en vigor la Directiva 95/46/CE de 24 de Octubre de 1.995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Como su propio nombre indica, uno de sus objetivos es recoger las medidas necesarias para conciliar los derechos fundamentales de las personas en el tratamiento de sus datos personales con la libre circulación de mercancías, personas, servicios y capitales que en una sociedad moderna va a implicar y hacer necesario la circulación de datos a través de medios electrónicos de un Estado miembro a otro, sobre todo teniendo en cuenta el avance de las tecnologías de la información que facilitan considerablemente el tratamiento e intercambio de datos personales.

Para esto establece los siguientes principios a tener en cuenta:

- Considera que aunque el responsable de un tratamiento de datos esté establecido en un país tercero, no debe ser obstáculo para garantizar la protección de las personas contemplada en la Directiva.

- El cumplimiento de la normativa del movimiento internacional de datos no debe impedir el desarrollo comercial internacional, y no se opone a la transferencia de datos personales a terceros países, siempre que se garantice un nivel de protección adecuado.

- Que cuando un país tercero no ofrezca ese nivel de protección debe prohibirse la transferencia de datos personales.

La Directiva establece en su Capítulo IV la regulación que ha de regir la transferencia de datos personales a países terceros. El artículo 25 dispone los principios por los que se ha de regir y en el artículo 26 las excepciones.

A su vez en el Capítulo VI dedicado a la "Autoridad de control y Grupo de protección de las personas en lo que respecta al tratamiento de datos personales" en su artículo 30 apartado 1 b) encomienda al Grupo la emisión de un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros.

En el artículo 26 se recogen las excepciones a los principios enunciados en el artículo 25 y, salvo disposición contraria del Derecho Nacional que regule los casos particulares, los Estados miembros tendrán que disponer que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado, siempre que:

a) El interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) La transferencia sea necesaria para la ejecución de un contrato o para la ejecución de medidas precontractuales entre el interesado y el responsable del tratamiento o un tercero y el responsable a petición del interesado, o

c) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público, o para un procedimiento judicial, por ejemplo en casos de transferencias internacionales de datos entre las administraciones fiscales o aduaneras o servicios con competencias en la seguridad social,

d) La transferencia sea necesaria para la salvaguardia del interés vital del interesado.

Estas excepciones no coinciden en su totalidad con las excepciones que recoge la LORTAD en su artículo 33, siendo, sobre todo, el consentimiento del interesado el que los diferencia de una forma más notable, dado que en nuestra

legislación no se recoge esta exclusión, en la actualidad es necesaria una autorización previa del Director de la Agencia para efectuar una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado, aunque el interesado haya dado su consentimiento.

No obstante, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, al adaptar las exigencias de la Directiva en el Título V dedicado al movimiento internacional de datos, traspone en su artículo 34 íntegramente las excepciones previstas en la Directiva a la norma general.

A su vez, viene a reconocer a la Agencia de Protección de Datos, la facultad para evaluar el carácter adecuado del nivel de protección que ofrece el país de destino.

El carácter adecuado se considerará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tendrá que tener en consideración los siguientes aspectos:

- naturaleza de los datos,
- la finalidad de la transferencia,
- la duración del tratamiento,
- el país de origen y el país de destino final,
- las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate,
- el contenido de los informes de la Comisión de la Unión Europea,
- las normas profesionales,
- la medidas de seguridad en vigor en dichos países.

Los principios que se recogen en la nueva Ley 15/1999, para considerar el carácter adecuado del nivel de protección ofrecido por un tercer país, coinciden plenamente con los principios recogidos en el artículo 25 apartado 2 de la Directiva.

Como ya se indicó anteriormente, es en el artículo 34 de la Ley 15/1999, donde se incluyen los supuestos que excepcionan los principios generales para poder efectuar una transferencia de datos personales a un país tercero que no garantice un nivel de protección equiparable, siendo éstos los siguientes:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

En los apartados 3 y 4 del artículo 25 de la Directiva se determina que los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado, instando en estos casos a los Estados miembros a adoptar las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

En los apartados 4, 5 y 6, se encomienda a la Comisión que en estos casos se prevean procedimientos de negociación entre la Comunidad y países terceros, destinados a remediar la falta de garantías a efectos de protección de datos. En estos casos, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

7.2. **GARANTÍAS SOLICITADAS A LOS RESPONSABLES DE FICHEROS**

La petición de autorización de transferencias internacionales de datos efectuada al amparo del artículo 32 de la Ley Orgánica 5/1992 exige una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia, establecida legalmente en nuestro país. Dicha entidad, como responsable de los ficheros, deberá garantizar el cumplimiento de todas las obligaciones y derechos establecidos en la Ley, así como que se continuará facilitando desde España el ejercicio de los derechos de acceso, rectificación y cancelación de los datos almacenados en terceros países. El Director de la Agencia de conformidad con lo dispuesto en el artículo 32 viene exigiendo las garantías que se exponen a continuación:

a) Toda la información de las circunstancias relacionadas con la transferencia, y en particular:

* la identificación de la entidad destinataria de la transferencia,
* la naturaleza de los datos que se van a transmitir,
* las finalidades para las que se transfieran los datos,
* las medidas de seguridad,
* la duración del tratamiento,
* el país de destino final,
* las normas sectoriales, o profesionales que pudieran existir.

b) Consentimiento inequívoco del interesado para que sus datos se almacenen en un fichero ubicado en un tercer país o en caso contrario que exista una libre y legítima aceptación de una relación contractual o precontractual en la que el interesado sea parte, y sea necesaria la transferencia para el desarrollo, cumplimiento y control de dicha relación.

c) Que la titularidad del fichero corresponda a una entidad domiciliada en territorio español y que dicha entidad, como responsable del fichero, garantice todas las obligaciones y derechos establecidos, así como que se continue facilitando desde España los derechos de acceso, rectificación y cancelación.

d) Que en el país de destino los datos no se van a utilizar para fines distintos de los especificados en la inscripción del fichero, así como que no se cederán a terceros sin el consentimiento de los interesados.

La Directiva además considera la posibilidad que sea el responsable del tratamiento el que ofrezca las garantías para paliar la insuficiencia del nivel de protección en un tercer país, pudiendo derivarse en cláusulas contractuales apropiadas. Y en su artículo 26.2 se dispone que los estados miembros podrán autorizar una transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, cuando el responsable del tratamiento ofrezca garantías suficientes y posibilite el ejercicio de los derechos de acceso, rectificación y cancelación en el país origen de los datos, igualándose en este sentido con el artículo 32 de la LORTAD y el artículo 33 de la Ley 15/1999.

Así mismo, en el apartado 3 del artículo 26 de la Directiva se obliga a los Estados miembros a informar a la Comisión y los demás Estados miembros acerca de las autorizaciones que se concedan con arreglo al apartado 2 del mismo artículo. Y en el supuesto que otro Estado miembro o la Comisión expresaran su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la decisión de la Comisión deberá ser adoptada y los Estados miembros ajustarse a ella.

La primera vez que en la Agencia de Protección de Datos se utilizó la solución contractual en el contexto de la transferencia internacional fue a finales de 1998, habiéndose autorizado 3 transferencias por este sistema en 1999.

Las cláusulas que se vienen exigiendo en estos casos con carácter general son las siguientes:

a) Obligación de las partes de la transferencia de garantizar que se aplica íntegramente el conjunto de principios de protección de datos.

b) Delimitación de la finalidad del tratamiento. Garantía de que los datos de carácter personal no podrán utilizarse para fines distintos de los especificados en el contrato y de que no pueden ser cedidos a terceros en el país de destino de la transferencia, ni siquiera para su conservación, siendo necesaria su destrucción o devolución al responsable una vez cumplida la prestación contractual.

c) Cumplimiento de las Medidas de Seguridad conforme a lo dispuesto en el artículo 9 de la LORTAD.

d) Control de la aplicación de la legislación de protección de datos, así como la de realizar auditorías por la propia Agencia o por un auditor externo independiente designado por ésta, incluida la facultad de realizar inspecciones en el país de destino.

e) Atribución de responsabilidad a la entidad que realiza la transferencia internacional en el caso que se produzca una infracción de las leyes de protección de datos.

f) Garantía expresa del cumplimiento por las partes de todas las obligaciones y derechos dispuestos en la LORTAD y de facilitar desde España, los derechos de acceso, rectificación y cancelación.

g) Aplicación de cláusulas que garanticen al afectado, cuando resulte perjudicado, el pago de indemnizaciones por el

responsable del fichero y la posibilidad en su caso, de imponer sanciones por la Agencia de Protección de Datos española.

h) Exigencia de responsabilidad solidaria de la exportadora y la entidad destinataria frente a la Agencia de Protección de Datos y los Tribunales españoles de los eventuales incumplimientos en que puedan incurrir respecto a las obligaciones asumidas en este contrato.

i) Compromiso de la entidad de informar a los nuevos clientes que vayan incorporándose a sus ficheros de datos.

7.3. **ANÁLISIS DEL APARTADO DE TRANSFERENCIAS INTERNACIONALES A EFECTOS DE INSCRIPCIÓN**

El total de ficheros inscritos en el Registro a fecha 31 de diciembre de 1999, que contienen en su declaración transferencias internacionales de datos es de 1.081 de los cuales 53 corresponden a inscripciones de titularidad pública y 1.028 de titularidad privada.

Igualmente, a tenor de las excepciones contempladas en el artículo 33 de la LORTAD, las transferencias internacionales de datos se realizan amparándose en los siguientes supuestos:

SUPUESTOS LEGALES	TIT.PUBLICA	TIT.PRIVADA
Se ampara en tratado o convenio del que España forma parte	41	0
Se realiza a efectos de prestar auxilio judicial internacional	9	0
Tiene por objeto intercambiar datos de carácter médico y así lo exige el tratamiento del afectado o la investigación epidemiológica	6	24
Se refiere a transferencias dinerarias	15	54
Se efectúa con destino a algún país de los citados en el reglamento con nivel de protección equiparable	47	923
TOTAL FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES	**53**	**1.028**

El total de ficheros inscritos con transferencias internacionales reflejados en la tabla anterior, no corresponde a la suma de los datos que figuran en cada subapartado, ya que un mismo fichero puede estar amparado en varios de ellos.

7.3.1. **Titularidad privada**

Entre los supuestos legales en los que se amparan las declaraciones de los ficheros inscritos con transferencias internacionales de datos, destacan las transferencias amparadas en la norma general del movimiento internacional de datos, cuando se efectúan con destino a países con nivel de protección equiparable al español. El número de ficheros privados declarados en el Registro amparados en este supuesto legal es de 923.

A continuación con 54 inscripciones, se encuentran los ficheros que declaran transferencias dinerarias conforme a su legislación específica, casi todos ellos pertenecientes a entidades financieras que realizan transferencias amparadas en su legislación en materia dineraria, normalmente adheridos al sistema SWIFT (Sistema internacional de intercambio de datos bancarios).

Los ficheros que realizan la transferencia de datos a otros países con objeto de intercambiar datos de carácter médico cuando así lo exija el tratamiento del afectado o una investigación epidemiológica asciende a 24.

7.3.2. **Titularidad pública**

En cuanto a las cifras de ficheros de titularidad pública, en la mayoría de los casos se trata de transferencias internacionales con destino a países de igual nivel de protección, siendo 47 los que declaran este supuesto.

Las amparadas en tratados o convenios se declaran en los ficheros de las Administraciones Tributarias y Seguridad Social, en virtud de lo dispuesto en los convenios internacionales de asistencia mutua en estas materias y en ficheros de las Fuerzas y Cuerpos de Seguridad con fines de investigaciones concretas amparadas en convenios internacionales como Interpol, Schengen y Europol. El número de inscripciones que se amparan en Tratados o Convenios es de 41. El número de transferencias internacionales amparadas en este supuesto, es pequeño debido sobre todo a la inexistencia de textos internacionales que recojan mandatos relativos a la protección de datos. Los existentes, son acuerdos ratificados por Estados que a su vez suelen tener legislación equiparable a la española.

Por otra parte, 15 ficheros declaran transferencias de carácter dinerario, amparándose en el supuesto de legislaciones específicas.

En este caso se encuadran los ficheros de operaciones exteriores inscritos por el Banco de España, los ficheros de

gestión de ayudas económicas de la Unión Europea al sector agrario y los ficheros relacionados con la gestión de los fondos FEDER inscritos por el Ministerio de Economía y Hacienda.

Nueve ficheros declaran las transferencias internacionales a efectos de prestar auxilio judicial internacional.

Seis ficheros tienen por objeto intercambiar datos de carácter médico.

7.3.3. **Expedientes de autorización de transferencia internacional**

Durante el año 1999, se ha producido un aumento en el número de solicitudes de autorización de transferencias internacionales de datos, lo que ha supuesto un incremento del 25,8% respecto del año 1998.

Este crecimiento ha sido debido al impacto de la entrada en vigor de la Directiva comunitaria de protección de datos, lo que ha supuesto que en los países de la Unión Europea se tuviera que cumplir con las previsiones legales de los artículo 25 y 26, en relación a las garantías que se tenían que exigir a los responsables de los ficheros cuando quisieran transmitir datos personales a terceros países que no garantizasen un nivel de protección adecuado al de la Unión Europea.

Aunque en la LORTAD ya existía esta previsión legal y la Agencia de Protección de Datos venía resolviendo las preceptivas autorizaciones de transferencias internacionales cuando se aportaban garantías suficientes en cumplimiento del artículo 32 de la norma, al ser únicamente la Ley española la que contenía la exigencia prevista en la Directiva, era menor el conocimiento que las entidades responsables de ficheros tenían en relación a esta previsión.

El número de solicitudes de autorización de transferencias internacionales ha sido de 151, de las cuales se han autorizado 145 hasta diciembre de 1999, se han archivado por desistimiento cinco, encontrándose únicamente un expediente iniciado durante 1999 en fase de tramitación al finalizar el año.

Durante este año se han iniciado 39 expedientes, encontrándose resueltos a fecha de hoy 38, lo que ha supuesto 36 autorizaciones de transferencia internacional, el archivo de dos expedientes por desistimiento y un expediente en tramitación al finalizar el año. Todas las autorizaciones resueltas tenían como destino Estados Unidos, excepto dos cuyo destino ha sido Filipinas y Marruecos.

Cuadro resumen de solicitudes y autorizaciones de transferencias internacionales de Datos de Carácter Personal a 30 de Diciembre de 1999.

AÑO	SOLICITUDES	AUTORIZACIONES	OTRAS CIRCUNSTANCIAS
1995	15	15	
1996	41	41	
1997	25	25	
1998	31	28 En el año 1998, se autorizan 19 En el año 1999, se autorizan 9	Archivo/Desistimiento del Responsable: 3
1999	39	36	Archivo/Desistimiento del Responsable: 2 Pendiente: 1
TOTAL	151	145	6

Todas las autorizaciones de transferencias internacionales están amparadas en el consentimiento informado de los afectados, a excepción de 4 expedientes que están amparados en la solución contractual.

7.4. **ANÁLISIS DEL MOVIMIENTO INTERNACIONAL DE DATOS**

Las solicitudes presentadas por responsables de ficheros en las que se solicita autorización para realizar una transferencia internacional se basan en diversos motivos que producen variedad de flujos de información.

Los motivos se pueden resumir así:

a) Armonización y puesta en común de los sistemas de información a efectos de centralizar su tratamiento en la empresa matriz y disminuir los costes del grupo.

Los fines más generalizados de los ficheros que se transfieren son todos aquellos relacionados con la actividad comercial, política de personal, política de ventas y compras, publicidad a clientes y seguimiento de las relaciones comerciales con las empresas subsidiarias del grupo.

Normalmente existe una relación contractual entre el interesado y el responsable del fichero. Los sectores que justifican

esta razón para solicitar la autorización de transferencia son muy diversos, pudiéndose resaltar entidades del sector del crédito, seguros, química y fabricantes de bienes informáticos.

Cuantitativamente tienen especial relevancia las autorizaciones otorgadas a empresas multinacionales en que la finalidad de la transferencia internacional es la gestión integral de sus recursos humanos.

b) Mejor servicio al cliente.

Se encuentra en diferentes sectores y para fines distintos tales como:

- Redes de franquicias en las que el propio objeto de su actividad es una mayor penetración en un país determinado o en los mercados internacionales. Suelen ser datos de empresarios autónomos bajo una misma marca y filosofía de empresa.

- Posibilidad de atender al cliente cuando éste se encuentre desplazado en el país destinatario de la transferencia. Siempre se realiza ante la solicitud del interesado. Los sectores de actividad más comunes son la intermediación financiera y bursátil, la banca y los seguros.

c) Actividades que implican necesariamente la transmisión de los ficheros para satisfacer la petición del cliente.

- Sistemas de distribución mundial. La generalización de reserva, emisión de billetes y otros servicios del transporte a nivel internacional en el sector turístico han hecho necesarios los sistemas informáticos dedicados al tratamiento en tiempo real de las solicitudes de sus clientes. La ubicación física de los ordenadores centrales está en terceros países, a los que se envían los datos que obtienen de las agencias de viajes o delegaciones de las compañías aéreas que se encuentran conectadas al sistema y que transmiten dichos datos como consecuencia de la solicitud del cliente.

- Usuarios y poseedores de tarjetas de clientes de una determinada sociedad con sede en diferentes países. Siempre existe una relación contractual de la que es parte el interesado para obtener servicios en otros países. Los sectores más representativos serían los medios de pago y tarjetas de fidelización de clientes de ámbito mundial.

7.5. **ANÁLISIS DE LOS FLUJOS DE INFORMACIÓN**

Los casos más frecuentes planteados ante la Agencia de Protección de Datos en la tramitación de las autorizaciones de transferencias internacionales pueden clasificarse de la siguiente forma:

7.5.1. **La transferencia internacional de Datos se realiza a un gran número de países donde se ubican las delegaciones o filiales de la empresa responsable de la transferencia internacional.**

La entidad ubicada en el territorio español es una de las delegaciones que la compañía matriz (ubicada fuera del ámbito de la Unión Europea) tiene en distintos países para realizar una cobertura mundial de las necesidades de sus clientes.

Los sistemas informáticos centrales de la compañía se encuentran ubicados en el establecimiento de la empresa matriz y desde este punto se transfieren los datos a las distintas sucursales a través de una red mundial.

En estos casos las garantías que se solicitan son las mismas para todos los países. Como criterio básico se exige el consentimiento informado de los titulares de los datos, se prohibe la cesión a terceros, y se solicita un compromiso de la empresa en relación a las normas de seguridad de acceso a la información a nivel mundial.

7.5.2. **La transferencia internacional de Datos se realiza por empresas ubicadas en España que ofrecen productos de terceras empresas ubicadas fuera del territorio de la Unión Europea.**

La empresa ubicada en España tiene un acuerdo de licencia de los productos de una empresa ubicada fuera del territorio de la Unión Europea.

En el caso de extinción del acuerdo de licencia, se exige al responsable del fichero establecido fuera del territorio de la Unión, la obligación de designar otra persona física o jurídica residente en España que será el nuevo responsable del tratamiento y de la transferencia internacional debiendo comunicar este hecho a la Agencia de Protección de Datos.

En la nueva Ley 15/1999 se hace referencia a esta situación en el artículo 5 apartado 1.e):

"Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

7.5.3. **La transferencia internacional se realiza por una empresa española ubicada en territorio nacional, que no tiene delegaciones comerciales fuera del territorio español.**

Se ha producido en el sector de informes comerciales de solvencia patrimonial y crédito.

La transferencia internacional se produce ante una petición individual sobre una persona determinada, pero el país puede ser diferente en cada petición y los destinatarios o las categorías de destinatarios de los datos transferidos son los clientes que mantengan relaciones económico-comerciales con el interesado y que suscriben un contrato con la empresa española.

En este caso al ser diferentes países, por cada petición se exige como garantías:

* Que la estructura del informe sea igual en todos.

* Que solo consten datos comerciales no normalizados y que no se traten automáticamente.

* Si no hubiera consentimiento del interesado para tratar y comunicar los datos que integran el informe comercial, el responsable del tratamiento deberá informar y obtener el consentimiento del interesado antes de realizar la transferencia, de la identidad del destinatario de los datos y el país en el que está establecido.

7.5.4. **La transferencia internacional se realiza por un grupo de empresas con la finalidad de gestionar los recursos humanos de una forma global para el grupo de empresas con sede en diversos países y cuya central estaba establecida en un tercer país.**

El problema residía en que además de tratar los datos del personal de esa empresa se pretendía transferir los datos del cónyuge del interesado.

Se exigió en este caso que la información relativa al cónyuge se recabara de éste así como consentimiento informado para realizarla.

7.5.5. **La transferencia internacional se realiza por empresas españolas con delegaciones en distintos países.**

La empresa solicitante de la autorización dispone de sucursales en todos los estados miembros y en terceros países y la central está establecida en territorio español.

El centro de procesos de datos está ubicado en territorio nacional y las sucursales o delegaciones conectadas por una red de telecomunicaciones.

Las garantías solicitadas para transmitir datos a sucursales ubicadas en terceros países son las mismas que se exigen para el caso que la empresa no fuera española.

7.5.6. **La transferencia internacional se realiza a la empresa matriz ubicada en un país tercero a los únicos efectos de tratamiento automatizado de datos en sus sistemas informáticos.**

La finalidad de la transferencia es el tratamiento automatizado centralizado de los datos de los socios de una cadena de alquiler de videos, a los efectos estrictamente estadísticos y de prestación de servicios de tratamiento informático con consentimiento del interesado.

La transferencia se fundamenta en la necesidad comercial de elaborar estadísticas generales, tanto a nivel local como en relación a todos los países en que esta cadena opera, y la elaboración de estadísticas del negocio requiere un tratamiento informático y una infraestructura informática que la filial española no dispone en la actualidad.

El problema se produce cuando se constata que la empresa matriz establecida en el tercer país, entre otras actividades, se dedica al marketing directo para terceros.

Se exige el consentimiento inequívoco de los titulares de los datos para realizar la transferencia a la empresa matriz.

Se exige además que figure en el contrato que la empresa matriz únicamente podrá tratar los datos a los efectos expuestos anteriormente.

7.5.7. **La transferencia internacional se realiza por una empresa española cuya actividad es el establecimiento de un directorio en un servidor, ubicado en un tercer país, para localización de direcciones de correo electrónico (e-mail) en la red Internet.**

Los datos a transferir son los propios de un sistema de correo electrónico. Dichos datos se transfieren porque el servidor Internet que alberga la información del directorio se encuentra ubicado en un tercer país.

Se exige, además del consentimiento informado del interesado, las garantías adicionales de que en el país de destino los datos no se van a utilizar para fines distintos de los derivados de la prestación de un servicio de alquiler de un servidor en la red Internet.

8. **EL REGISTRO EN CIFRAS**

A continuación se detalla la situación y características principales de los ficheros inscritos en el Registro General de Protección de Datos. Como en años anteriores, se ha tratado de establecer la comparación entre los ficheros según la titularidad del responsable, público o privado, así como el estudio de sus principales características.

A fecha 31 de Diciembre de 1999, el número de ficheros inscritos en el Registro General era de 235.168, de los cuales 30.431 correspondían a inscripciones de titularidad pública y 204.737 a inscripciones de titularidad privada.

RESUMEN DETALLADO SEGÚN LA TITULARIDAD Y AÑO DE INSCRIPCIÓN

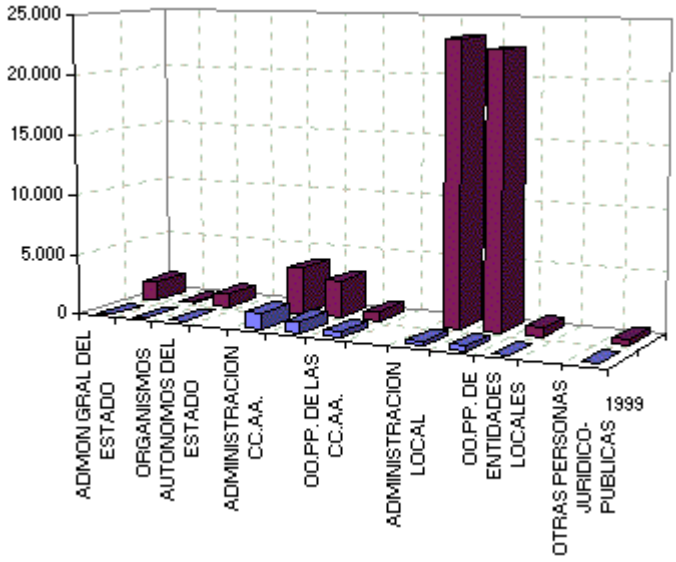
Se recoge en esta tabla el estado de los ficheros a 31 de Diciembre de 1999, en función de la titularidad y año en que se ha realizado la inscripción de los mismos.

ESTADO	INSCRITOS					
AÑO INSCRIPCION	1994	1995	1996	1997	1998	1999
TITULARIDAD PUBLICA	19.580	4.733	1.810	1.479	947	1.882
T O T A L	30.431					
TITULARIDAD PRIVADA	187.546	7.848	2.099	1.701	2.260	3.283
T O T A L	204.737					
TOTAL AÑO	207.126	12.581	3.909	3.180	3.207	5.165
	235.168					

(*) Las cifras que aparecen en esta tabla correspondientes a años anteriores a 1999 no coinciden con las publicadas en memorias anteriores, debido a que durante el año 1999 se han realizado operaciones de supresión sobre ellos

DISTRIBUCION DE FICHEROS PUBLICOS INSCRITOS, SEGÚN EL TIPO DE ADMINISTRACION AL QUE PERTENECEN

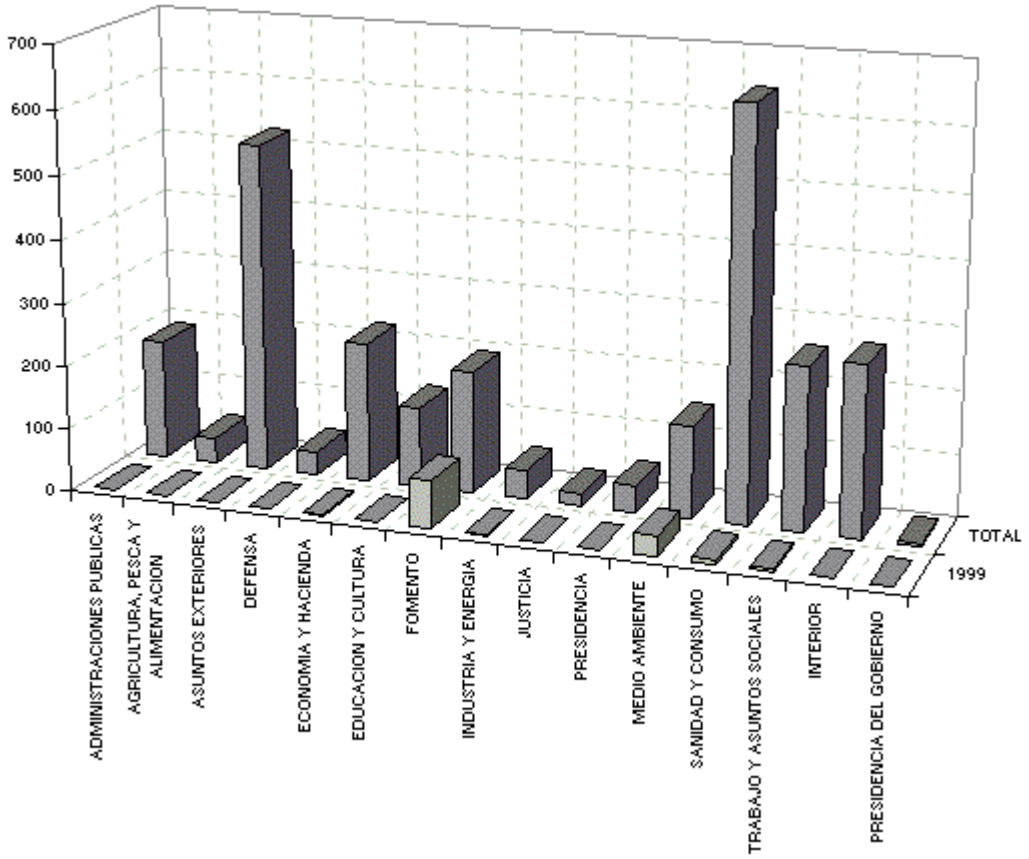
	1999	TOTAL
ADMINISTRACION CENTRAL	**124**	**2.754**
ADMON GRAL DEL ESTADO	10	1.572
ENTIDADES Y OO.AA. DE LA S.S.	2	108
ORGANISMOS AUTONOMOS DEL ESTADO	112	1.074
ADMINISTRACION CC.AA.	**1.385**	**3.869**
ADMON DE LAS CC AA	930	3.103
OO.PP. DE LAS CC.AA.	455	766
ADMINISTRACION LOCAL	**353**	**23.320**
ADMONES LOCALES	340	22.522
OO.PP. DE ENTIDADES LOCALES	13	798
OTRAS PERSONAS JURIDICO-PUBLICAS	**20**	**488**
TOTAL	**1.882**	**30.431**



DISTRIBUCIÓN DE FICHEROS PÚBLICOS INSCRITOS DE LA ADMINISTRACIÓN CENTRAL

Para la elaboración de esta tabla se ha considerado como Administración Central a los ficheros de la Administración Central del Estado, Entidades y Organismos de la Seguridad Social y Organismos Autónomos del Estado, integrando a éstos dentro del Ministerio al que están adscritos.

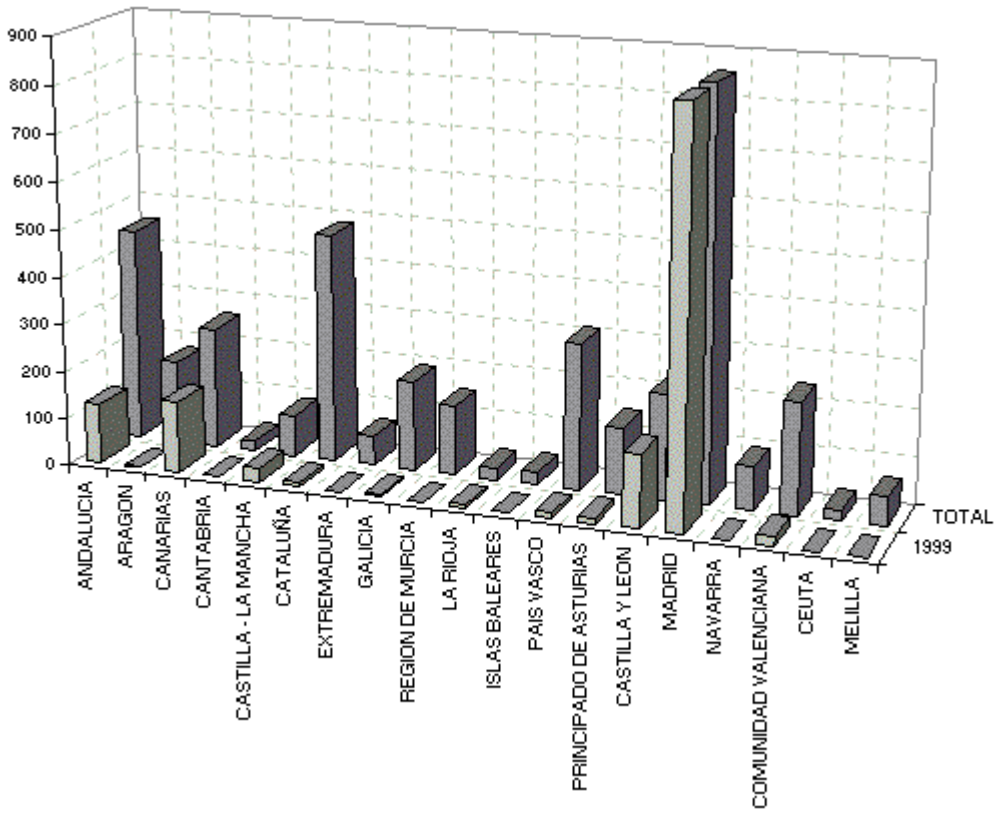
	1999	TOTAL
MINISTERIO DE ADMINISTRACIONES PUBLICAS	0	189
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIO	0	40
MINISTERIO DE ASUNTOS EXTERIORES	0	522
MINISTERIO DE DEFENSA	0	36
MINISTERIO DE ECONOMIA Y HACIENDA	1	222
MINISTERIO DE EDUCACION Y CULTURA	1	127
MINISTERIO DE FOMENTO	75	194
MINISTERIO DE INDUSTRIA Y ENERGIA	1	46
MINISTERIO DE JUSTICIA	0	19
MINISTERIO DE LA PRESIDENCIA	0	42
MINISTERIO DE MEDIO AMBIENTE	33	146
MINISTERIO DE SANIDAD Y CONSUMO	7	643
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	4	256
MINISTERIO DEL INTERIOR	2	268
PRESIDENCIA DEL GOBIERNO	0	4
TOTAL	124	2.754



DISTRIBUCIÓN DE FICHEROS PÚBLICOS INSCRITOS POR LAS COMUNIDADES AUTÓNOMAS

Aparecen aquí los ficheros de la Administración de Comunidades Autónomas, así como los de los Organismos Públicos dependientes de éstas.

COMUNIDAD AUTONOMA	1999	TOTAL
ANDALUCIA	126	454
ARAGON	1	175
CANARIAS	151	258
CANTABRIA	1	21
CASTILLA - LA MANCHA	31	88
CATALUÑA	10	483
EXTREMADURA	0	62
GALICIA	6	191
REGION DE MURCIA	0	146
LA RIOJA	6	25
ISLAS BALEARES	0	25
PAIS VASCO	11	307
PRINCIPADO DE ASTURIAS	13	143
CASTILLA Y LEON	154	221
MADRID	856	857
NAVARRA	1	92
COMUNIDAD VALENCIANA	18	236
CEUTA	0	23
MELILLA	0	62
TOTAL	1.385	3.869



DISTRIBUCIÓN DE FICHEROS PÚBLICOS DE OTRAS PERSONAS JURÍDICO-PÚBLICAS

	1999	TOTAL
CAMARAS DE COMERCIO, INDUSTRIA Y NAVEGACIO	0	187
UNIVERSIDADES	20	262
OTROS	0	39
T O T A L	20	488

FICHEROS PÚBLICOS DE LA ADMINISTRACIÓN LOCAL INSCRITOS, DISTRIBUIDOS POR COMUNIDADES AUTÓNOMAS Y PROVINCIAS

En esta tabla aparecen, diferenciados por Provincias y Comunidades Autónomas, los ficheros de la Administración Local y Organismos Públicos de Entidades Locales.

	ORGANISMOS		FICHEROS	
	1999	TOTAL	1999	TOTAL
ANDALUCIA	**9**	**675**	**28**	**5.450**
ALMERIA	0	104	0	950
CADIZ	2	46	11	329
CORDOBA	1	58	5	243
GRANADA	1	168	1	1.183
HUELVA	0	85	0	1.150
JAEN	1	82	6	468
MALAGA	3	41	4	397
SEVILLA	1	91	1	730
ARAGON	**0**	**434**	**0**	**1.967**
HUESCA	0	156	0	536
TERUEL	0	45	0	152
ZARAGOZA	0	233	0	1.279
ASTURIAS	**2**	**46**	**9**	**277**
ILLES BALEARS	**2**	**67**	**21**	**649**
CANARIAS	**5**	**66**	**21**	**407**
PALMAS, LAS	2	25	12	187
SANTA CRUZ DE TENERIFE	3	41	9	220
CANTABRIA	**3**	**43**	**14**	**192**
CASTILLA-LA MANCHA	**6**	**342**	**24**	**1.850**
ALBACETE	3	74	9	356
CIUDAD REAL	0	107	0	557
CUENCA	0	82	0	556
GUADALAJARA	0	11	0	59
TOLEDO	3	68	15	322

	ORGANISMOS		FICHEROS	
	1999	TOTAL	1999	TOTAL
CASTILLA Y LEON	**1**	**499**	**1**	**2.199**
AVILA	0	7	0	19
BURGOS	0	91	0	318
LEON	0	163	0	801
PALENCIA	0	18	0	76
SALAMANCA	0	80	0	338
SEGOVIA	1	14	1	104
SORIA	0	9	0	31
VALLADOLID	0	82	0	355
ZAMORA	0	35	0	157
CATALUÑA	**44**	**533**	**93**	**2.526**
BARCELONA	43	289	89	1.363
GIRONA	0	55	0	347
LLEIDA	1	106	4	398
TARRAGONA	0	83	0	418
COMUNIDAD VALENCIANA	**4**	**312**	**18**	**2.181**
ALICANTE	0	137	0	1.195
CASTELLON DE LA PLANA	0	35	0	225
VALENCIA	4	140	18	761
EXTREMADURA	**1**	**187**	**4**	**1.559**
BADAJOZ	0	155	0	1.390
CACERES	1	32	4	169
GALICIA	**18**	**223**	**31**	**930**
A CORUÑA	4	87	6	440
LUGO	4	40	6	161
OURENSE	2	36	11	142
PONTEVEDRA	8	60	8	187
RIOJA, LA	**0**	**30**	**0**	**131**
MADRID	**7**	**54**	**58**	**697**
MURCIA	**1**	**36**	**16**	**417**
NAVARRA	**5**	**81**	**5**	**425**
PAIS VASCO	**2**	**178**	**10**	**1.463**
ALAVA	0	39	0	181
GUIPUZCOA	1	66	9	744
VIZCAYA	1	73	1	538

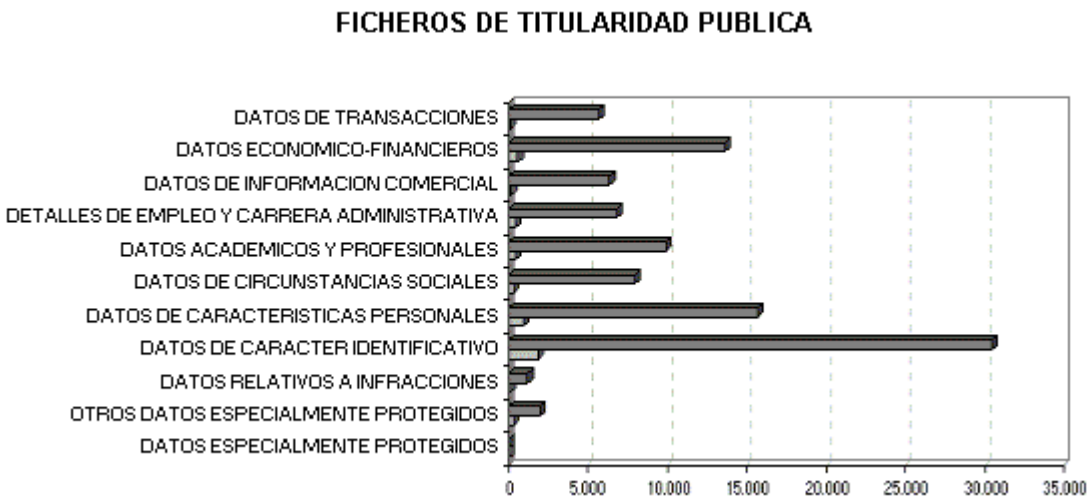
FICHEROS PRIVADOS INSCRITOS DISTRIBUIDOS POR COMUNIDADES AUTÓNOMAS Y PROVINCIAS

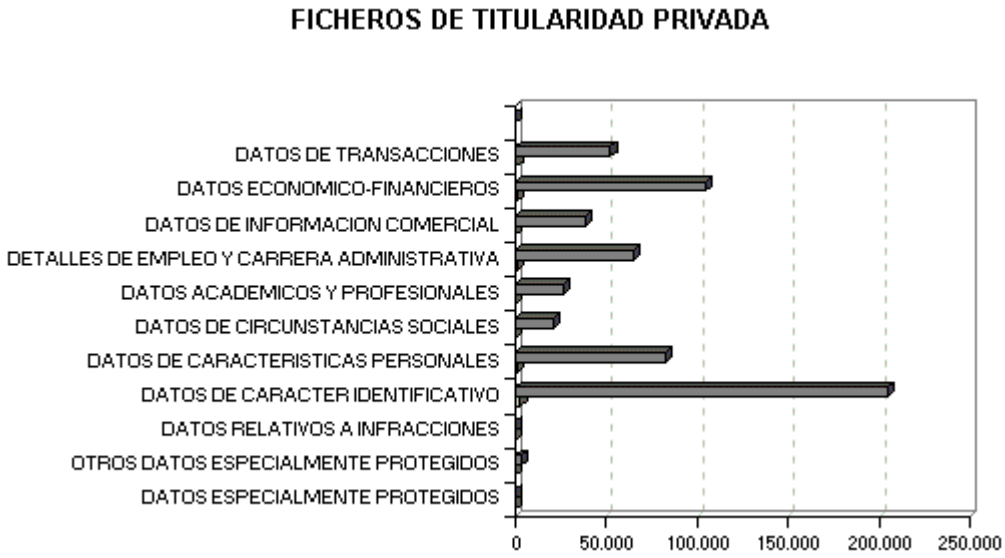
	EMPRESAS		FICHEROS	
	1999	TOTAL	1999	TOTAL
ANDALUCIA	**82**	**9.082**	**254**	**17.095**
ALMERIA	2	415	7	810
CADIZ	21	1.650	51	2.577
CORDOBA	11	1.083	53	2.302
GRANADA	14	740	29	1.409
HUELVA	4	624	12	1.014
JAEN	2	826	4	1.743
MALAGA	12	2.012	72	3.463
SEVILLA	16	1.738	26	3.777
ARAGON	**37**	**7.992**	**84**	**13.066**
HUESCA	1	1.802	1	2.485
TERUEL	2	574	3	895
ZARAGOZA	34	5.621	80	9.686
ASTURIAS	**17**	**1.956**	**69**	**3.576**
ILLES BALEARS	**10**	**1.211**	**13**	**2.818**
CANARIAS	**25**	**1.231**	**41**	**2.243**
PALMAS, LAS	15	705	24	1.287
SANTA CRUZ DE TENERIFE	10	529	17	956
CANTABRIA	**11**	**571**	**33**	**1.260**
CASTILLA-LA MANCHA	**22**	**2.966**	**66**	**5.159**
ALBACETE	5	914	14	1.415
CIUDAD REAL	5	616	9	1.109
CUENCA	2	522	22	838
GUADALAJARA	2	222	2	521
TOLEDO	8	692	19	1.276
CASTILLA Y LEON	**28**	**4.525**	**68**	**8.315**
AVILA	1	196	2	350
BURGOS	6	1.267	23	2.025
LEON	6	645	7	1.220
PALENCIA	3	235	4	456
SALAMANCA	0	531	0	1.248
SEGOVIA	4	284	18	502
SORIA	0	240	0	388
VALLADOLID	7	896	11	1.577
ZAMORA	1	237	3	549

	EMPRESAS		FICHEROS	
	1999	TOTAL	1999	TOTAL
CATALUÑA	**392**	**30.538**	**888**	**55.946**
BARCELONA	338	23.151	775	43.272
GIRONA	12	2.827	19	4.929
LLEIDA	28	2.841	61	4.606
TARRAGONA	15	1.739	33	3.139
COMUNIDAD VALENCIANA	**84**	**14.339**	**132**	**23.681**
ALICANTE	40	5.663	67	9.036
CASTELLON DE LA PLANA	5	2.315	21	3.977
VALENCIA	39	6.368	44	10.668
EXTREMADURA	**64**	**2.130**	**68**	**3.511**
BADAJOZ	47	1.672	47	2.566
CACERES	17	459	21	945
GALICIA	**59**	**6.459**	**80**	**11.596**
A CORUÑA	21	3.360	28	5.894
LUGO	5	861	7	1.339
OURENSE	7	565	10	1.063
PONTEVEDRA	26	1.667	35	3.300
RIOJA, LA	**7**	**1.675**	**9**	**3.080**
MADRID	**454**	**16.520**	**1.361**	**38.139**
MURCIA	**7**	**2.757**	**9**	**4.537**
NAVARRA	**8**	**1.703**	**8**	**3.195**
PAIS VASCO	**69**	**3.745**	**100**	**7.351**
ALAVA	7	531	24	1.021
GUIPUZCOA	12	1.837	19	3.622
VIZCAYA	50	1.384	57	2.708
CEUTA	**0**	**53**	**0**	**116**
MELILLA	**0**	**35**	**0**	**53**

DISTRIBUCIÓN DE FICHEROS SEGÚN LA TIPOLOGÍA DE DATOS QUE CONTIENEN

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1999	TOTAL	1999	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	5	61	7	321
OTROS DATOS ESPECIALMENTE PROTEGIDOS	382	2.021	157	3.522
DATOS RELATIVOS A INFRACCIONES	86	1.224	---	---
DATOS DE CARACTER IDENTIFICATIVO	1.882	30.431	3.283	204.737
DATOS DE CARACTERISTICAS PERSONALES	949	15.730	1.784	82.776
DATOS DE CIRCUNSTANCIAS SOCIALES	322	7.945	665	21.298
DATOS ACADEMICOS Y PROFESIONALES	448	9.954	693	26.406
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	467	6.809	1.424	65.130
DATOS DE INFORMACION COMERCIAL	197	6.367	547	38.617
DATOS ECONOMICO-FINANCIEROS	613	13.670	1.547	105.036
DATOS DE TRANSACCIONES	174	5.721	848	52.423





FICHEROS INSCRITOS CON DATOS SENSIBLES

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1999	**TOTAL**	**1999**	**TOTAL**
DATOS ESPECIALMENTE PROTEGIDOS	**5**	**61**	**7**	**321**
Ideología	1	38	7	136
Creencias	3	20	0	38
Religión	4	16	0	172
OTROS DATOS ESPECIALMENTE PROTEGIDO	**382**	**2.021**	**157**	**3.522**
Origen Racial	22	96	22	52
Salud	381	2.002	157	3.496
Vida Sexual	23	360	4	104
DATOS RELATIVOS A INFRACCIONES	**86**	**1.224**	---	---
Infracciones Penales	24	743	---	---
Infracciones Administrativas	81	889	---	---

---- No aplicable a esta titularidad

DISTRIBUCIÓN DE FICHEROS PÚBLICOS SEGÚN SU FINALIDAD

	1999	TOTAL
GESTION DE ESTADISTICAS INTERNAS	445	8.202
PROCEDIMIENTOS ADMINISTRATIVOS	360	8.501
GESTION DE PERSONAL	352	4.403
HISTORIAL CLINICO	266	856
GESTION Y CONTROL SANITARIO	238	1.336
OTRAS FINALIDADES	228	4.240
FUNCION ESTADISTICA PUBLICA	180	5.273
GESTION ECONOMICA CON TERCEROS	146	5.941
CONCESION Y GESTION DE PERMISOS Y LICENCIAS	142	3.291
GESTION TRIBUTARIA Y DE RECAUDACION	138	6.672
INVESTIGACIONES CIENTIFICAS O MEDICAS Y ACTIVIDADES ANALOGA	129	1.051
SEGURIDAD Y CONTROL INTERNO	102	2.016
PUBLICACIONES	92	642
FORMACION PROFESIONAL	85	1.083
OTRAS ENSEÑANZAS, BECAS Y AYUDAS A ESTUDIANTES	85	1.026
PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONOMICAS	82	1.907
PADRON	73	4.394
OTROS SERVICIOS SOCIALES	65	1.150
FORMACION DE PERSONAL	64	1.397
GESTION SANCIONADORA	63	2.275
PRESTACIONES DE ASISTENCIA SOCIAL	62	1.581
SERVICIOS SOCIALES A LA TERCERA EDAD	62	1.068
SERVICIOS SOCIALES A MINUSVALIDOS	60	777
PROMOCION Y SERVICIOS A LA MUJER	50	611
PROTECCION DEL MENOR	50	647
PROCEDIMIENTOS JUDICIALES	46	867
PROMOCION Y GESTION DE EMPLEO	46	798
RELACIONES LABORALES Y CONDICIONES DE TRABAJO	38	1.363
PROMOCION Y SERVICIOS A LA JUVENTUD	36	667
PROTECCION A LOS CONSUMIDORES	36	212
AYUDAS ACCESO A VIVIENDA	35	1.044
GESTION DEUDA PUBLICA Y TESORERIA	32	2.454
ACCION EN FAVOR DE MIGRANTES	27	408
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD	25	1.810
INSPECCION Y CONTROL DE SEGURIDAD Y PROTECCION SOCIAL	25	685
CONTROL DE INCOMPATIBILIDADES	23	609
DEPORTES	22	882
GESTION DE CATASTROS INMOBILIARIOS RUSTICOS Y URBANOS	21	1.840
PRESTACIONES DE GARANTIA SALARIAL	21	262
ACTUACIONES POLICIALES	20	2.057
NACIONALIDAD	19	960
PRESTACIONES A LOS DESEMPLEADOS	19	961
EDUCACION UNIVERSITARIA	18	452
SERVICIO MILITAR	18	2.131
ACCION SOCIAL EN FAVOR DEL PERSONAL DE ADMONES. PUBLICAS	17	788
EDUCACION INFANTIL Y PRIMARIA	15	722

	1999	TOTAL
ENCUESTAS SOCIOLOGICAS Y DE OPINION	14	151
FOMENTO Y APOYO A ACTIVIDADES ARTISTICAS Y CULTURALES	14	320
SEGURIDAD VIAL	13	1.316
EDUCACION SECUNDARIA	9	626
FORMACION PROFESIONAL Y ESCUELA OFICIAL DE IDIOMAS	9	639
EDUCACION ESPECIAL	7	339
PRESTACION SOCIAL SUSTITUTORIA	7	837
RELACIONES COMERCIALES CON EL EXTERIOR	7	409
PROTECCION CIVIL	6	1.642
PROTECCION PATRIMONIO HISTORICO ARTISTICO	6	101
DEFENSA DE LA COMPETENCIA	4	25
CONTROL DE PATRIMONIO DE ALTOS CARGOS PUBLICOS	3	219
GESTION Y CONTROL DE CENTROS E INSTITUCIONES PENITENCIARIAS	2	317
INDULTOS	0	262
REGULACION DE MERCADOS FINANCIEROS	0	29
TRABAJOS PENITENCIARIOS	0	270

DISTRIBUCIÓN DE FICHEROS PRIVADOS SEGÚN SU FINALIDAD

	1999	TOTAL
GESTION CONTABLE, FISCAL Y ADMINISTRATIVA	1.296	133.922
OBTENCION DE ESTADISTICAS DIVERSAS	1.211	54.970
GESTION DE CLIENTES	1.159	64.894
GESTION DE COBROS Y PAGOS	1.136	88.403
PUBLICIDAD PROPIA	984	20.112
HISTORICOS DE RELACIONES COMERCIALES	703	32.360
GESTION DE PERSONAL	678	53.441
PROSPECCIONES DE MERCADO	460	7.217
ENCUESTAS DE OPINION	364	3.155
SEGURIDAD Y CONTROL INTERNO	338	10.220
OTRAS FINALIDADES	293	8.746
SELECCION DE PERSONAL	206	3.749
PUBLICIDAD PARA TERCEROS	203	2.885
SEGUROS DE VIDA Y SALUD	200	5.497
PRESTACIONES SOCIALES	179	13.668
OTROS SERVICIOS FINANCIEROS	161	3.957
OTRO TIPO DE SEGUROS	147	5.565
GESTION ADMINISTRATIVA DE LOS INTEGRANTES DE CLUBES	132	2.185
CUENTA DE CREDITO	122	4.299
INFORMACION SOBRE LA SOLVENCIA PATRIMONIAL Y CREDIT(	120	3.418
AUDITORIAS, ASESORIAS Y SERVICIOS RELACIONADOS	116	13.479
OTRAS ENSEÑANZAS	106	1.496
GESTION Y CONTROL SANITARIO	106	1.769
HISTORIAL CLINICO	100	1.965
GESTION DE TARJETAS DE CREDITO Y SIMILARES	99	1.628

DISTRIBUCIÓN DE FICHEROS INSCRITOS SEGÚN LA PROCEDENCIA DE LOS DATOS, EL PROCEDIMIENTO Y SOPORTE DE RECOGIDA

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
SOPORTE	**1.999**	**TOTAL**	**1.999**	**TOTAL**
SOPORTE PAPEL	1.582	28.695	2.765	165.683
SOPORTE INFORMATICO/MAGNETICO	691	12.046	938	29.477
VIA TELEMATICA	113	3.313	652	5.991
OTROS SOPORTES	40	3.128	348	33.914
PROCEDENCIA DE LOS DATOS	**1.999**	**TOTAL**	**1.999**	**TOTAL**
ENTIDAD PRIVADA	137	3.178	356	25.882
ADMINISTRACIONES PUBLICAS	425	11.033	97	3.576
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	1.710	28.497	3.081	184.342
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	169	4.050	114	4.215
FUENTES ACCESIBLES AL PUBLICO	67	2.822	298	9.119
PROCEDIMIENTO DE RECOGIDA	**1.999**	**TOTAL**	**1.999**	**TOTAL**
ENCUESTAS O ENTREVISTAS	571	4.354	809	44.686
DECLARACIONES O FORMULARIOS	1.296	25.887	2.241	86.772
REGISTROS PUBLICOS	182	6.766	125	3.846
TRANSMISION ELECTRONICA DE DATOS	141	4.752	496	4.182
DIRECTORIOS TELEFONICOS, COMERCIALES, CATALOGOS, MEMORIAS	25	1.858	207	9.236
OTROS PROCEDIMIENTOS DE RECOGIDA	170	3.022	653	69.664

SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LOS FICHEROS QUE DECLARAN CESIONES DE DATOS

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1999	**TOTAL**	**1999**	**TOTAL**
EXISTE CONSENTIMIENTO DE LOS AFECTADOS	263	6.809	703	17.824
EXISTE UNA RELACION JURIDICA CUYO DESARROLLO, CONTROL Y CUMPLIMIENTO IMPLICA NECESARIAMENTE LA CONEXION DEL FICHERO CON FICHEROS DE TERCEROS	147	3.908	419	12.983
EXISTE UNA NORMA REGULADORA QUE LAS AUTORIZA	580	10.734	303	19.745
SE TRATA DE DATOS RECOGIDOS DE FUENTES ACCESIBLES AL PUBLICO	42	4.778	98	2.413
CORRESPONDEN A COMPETENCIAS IDENTICAS O QUE VERSAN SOBRE LAS MISMAS MATERIAS, EJERCIDAS POR OTRAS ADMINISTRACIONES PUBLICAS	268	10.458	---	---
SON DATOS OBTENIDOS O ELABORADOS CON DESTINO A OTRA ADMINISTRACION PUBLICA	208	9.246	---	---
TOTAL FICHEROS INSCRITOS CON CESIONES	**751**	**17.698**	**1.063**	**35.357**

El total de ficheros inscritos con cesiones reflejados en la tabla anterior, no corresponde a la suma de los datos que figuran en cada subapartado, ya que un mismo fichero puede estar amparado en varios de ellos.

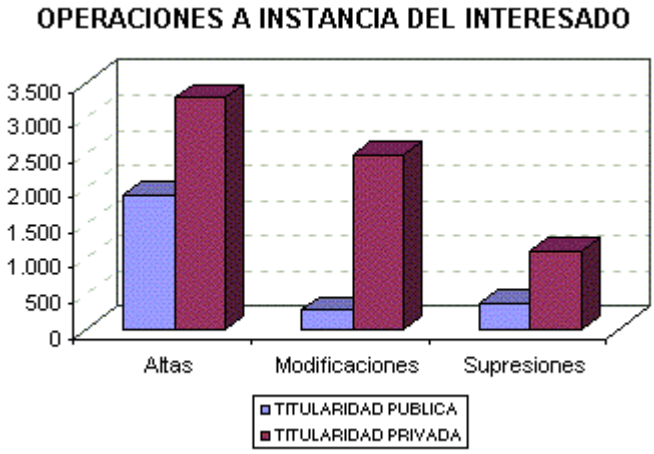
SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LOS FICHEROS QUE DECLARAN TRANSFERENCIAS INTERNACIONALES DE DATOS

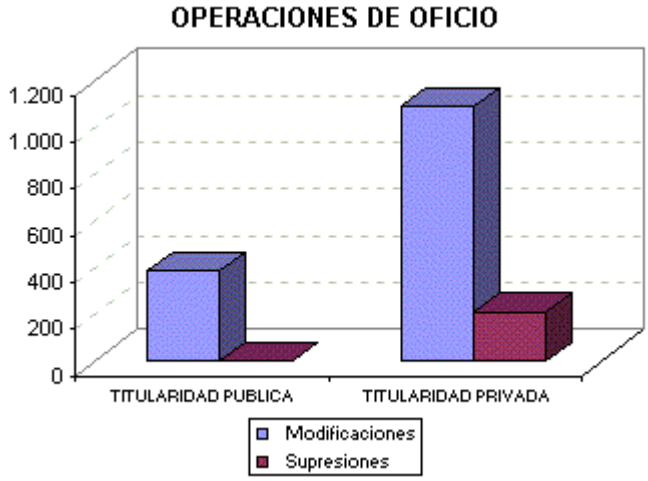
	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1999	TOTAL	1999	TOTAL
SE AMPARA EN TRATADO O CONVENIO DEL QUE ESPAÑA FORMA PART	2	41	0	0
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	0	9	0	0
TIENE POR OBJETO INTERCAMBIAR DATOS DE CARACTER MEDICO Y ASI LO EXIGE EL TRATAMIENTO DEL AFECTADO O LA INVESTIGACION EPIDEMIOLOGICA	1	6	19	24
SE REFIERE A TRANSFERENCIAS DINERARIAS	0	15	6	54
SE EFECTUA CON DESTINO A ALGUN PAIS DE LOS CITADOS EN EL REGLAMENTO CON NIVEL DE PROTECCION EQUIPARABLE	1	47	83	923
SE EFECTUA CON AUTORIZACION DEL DIRECTOR DE LA AGENCIA	0	0	34	200
TOTAL FICHEROS CON TRANSFERENCIAS INTERNACIONALES	**4**	**53**	**98**	**1.028**

El total de ficheros inscritos con transferencias internacionales reflejados en la tabla anterior, no corresponde a la suma de los datos que figuran en cada subapartado, ya que un mismo fichero puede estar amparado en varios de ellos.

OPERACIONES REALIZADAS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS SEGÚN LA TITULARIDAD Y TIPO DE OPERACIÓN

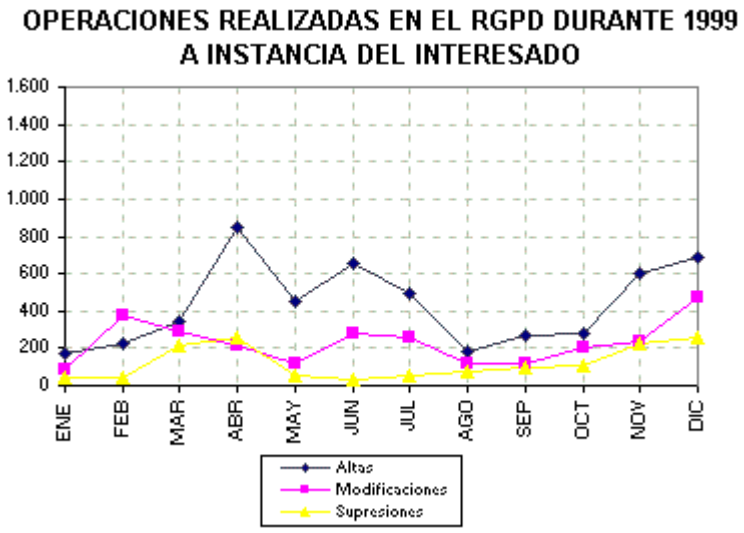
	TITULARIDAD PUBLIC/	TITULARIDAD PRIVAD/	TOTAL
OPERACIONES A INSTANCIA DEL RESPONSAB			
Altas	1.912	3.289	5.201
Modificaciones	268	2.485	2.753
Supresiones	366	1.113	1.479
T O T A L	2.546	6.887	9.433
OPERACIONES SUBSANACION DE OFICIO			
Modificaciones	391	1.094	1.485
Supresiones	0	214	214
T O T A L	391	1.308	1.699
TOTALES	**2.937**	**8.195**	**11.132**

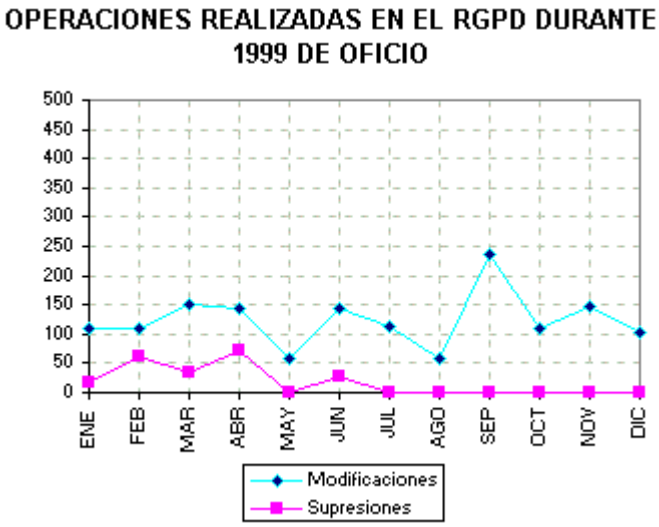




RESUMEN DE OPERACIONES REALIZADAS DURANTE EL AÑO 1999 SOBRE FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
OPERACIONES A INSTANCIA DEL INTERESADO													
Altas	172	225	342	851	450	655	492	185	265	282	597	685	5.201
Modificaciones	87	373	287	213	118	278	258	113	118	199	239	470	2.753
Supresiones	47	48	211	257	50	35	59	79	102	106	223	262	1.479
T O T A L	306	646	840	1.321	618	968	809	377	485	587	1.059	1.417	9.433
OPERACIONES DE SUBSANACION DE OFICIO													
Modificaciones	111	108	149	144	59	145	114	58	236	110	147	104	1.485
Supresiones	18	62	34	72	0	28	0	0	0	0	0	0	214
T O T A L	129	170	183	216	59	173	114	58	236	110	147	104	1.699
T O T A L E S	**435**	**816**	**1.023**	**1.537**	**677**	**1.141**	**923**	**435**	**721**	**697**	**1.206**	**1.521**	**11.132**





1 Operaciones y procedimientos técnicos que permitan: **Recogida** de datos, **Grabación** de datos, **Conservación** de datos, **Elaboración** de datos, **Modificación** de datos, **Supresión** de datos, **Comunicaciones** de datos, **Consultas** de datos e **Interconexiones** de datos.

2 La forma jurídica de dicho establecimiento no es un factor determinante.

3 Cuando el Responsable del tratamiento no esté establecido en el territorio de la Unión Europea..

4 El apartado de *Dirección de Derechos de Acceso* del Modelo de Notificación.

IV. SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS

1. LA INSPECCIÓN DE DATOS E INSTRUCCIÓN DE EXPEDIENTES

1.1. INTRODUCCIÓN: ACTIVIDAD INSPECTORA E INSTRUCTORA DE EXPEDIENTES

La Subdirección General de Inspección de Datos es el órgano de la Agencia de Protección de Datos (APD) al que, bajo la dirección y superior autoridad del Director, le corresponde desempeñar dos de las más importantes funciones para el efectivo cumplimiento de la LORTAD: la función inspectora o investigadora y la función instructora de los expedientes sancionadores y procedimientos de tutela de derechos.

1.1.1. **Función inspectora**

La Inspección de Datos no está contemplada por la LORTAD desde la vertiente orgánica, sino sólo desde la funcional, siendo el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la APD, el que prevé que las funciones inherentes al ejercicio de la potestad de inspección que el art. 39 de la LORTAD atribuye a la Agencia, se ejerzan por un órgano específico y separado de los demás al frente del cual se sitúa a un funcionario con categoría de Subdirector General.

No añade el Estatuto nuevas precisiones sobre el estatuto personal de quienes se encuadran en este órgano a las ya contenidas en la LORTAD, la cual dispone que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus cometidos (art. 39), de donde resulta que la inspección deberá ser desempeñada por funcionarios de carrera.

El Estatuto desarrolla el contenido de la potestad de inspección atribuida a la Agencia en el ya citado art. 39 de la LORTAD, precisando la facultad de la Inspección de Datos para efectuar inspecciones de oficio, aunque pudieran tener su origen en una denuncia de las personas afectadas, y detallando el alcance concreto de su capacidad para requerir y obtener información, así como examinar *in situ* los ficheros y sistemas informáticos en los que se traten datos de carácter personal. En conjunto, se trata de una serie de facultades cuya finalidad es la de obtener información y, en su caso, pruebas sobre posibles incumplimientos de la LORTAD, que permitan posteriormente al órgano decisorio incoar procedimientos sancionadores y adoptar las medidas pertinentes dirigidas a la cesación de actividades ilícitas en los términos previstos en el art. 48 de dicha Ley.

Como lógico correlato de esta función inspectora, se impone a los funcionarios que la ejercen el deber de guardar secreto sobre las informaciones que conozcan en el ejercicio de tal función, incluso después de haber cesado en la misma (art. 39.2); deber cuyo incumplimiento generaría la oportuna responsabilidad disciplinaria mientras se conserve la relación de servicio con la APD, y que se reputaría infracción administrativa grave, una vez extinguida dicha relación, al amparo del art. 43.3 g) de la LORTAD.

1.1.2. **Función instructora**

A la Subdirección General de Inspección de Datos le corresponde también la función instructora en los expedientes sancionadores, esto es, el ejercicio de los actos de instrucción relativos a los expedientes sancionadores (art. 29 del Estatuto).

El ejercicio de esta función instructora correspondiente a la Subdirección General de Inspección de Datos, no es más que la consecuencia obligada de la existencia de la potestad sancionadora atribuida en exclusiva al Director de la Agencia (art. 36.g de la LORTAD) y la necesaria garantía del procedimiento sancionador, cuyo ejercicio exige la separación entre la fase instructora y la sancionadora, encomendándolas o órganos distintos (art. 134 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común).

El procedimiento sancionador, de conformidad con lo previsto en el art. 47 de la LORTAD, ha venido a ser regulado por el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones, estructurándose como cualquier otro procedimiento sancionador en las tres clásicas fases de Iniciación, Instrucción y Resolución, correspondiendo al funcionario instructor el desarrollo completo de la fase de Instrucción u Ordenación del procedimiento y la propuesta razonada al Director de la Agencia de las otras dos, es decir, del acuerdo de inicio del procedimiento sancionador y de la Resolución del mismo.

Por otra parte, la función instructora se concreta en la incoación de tres clases de procedimientos: el procedimiento sancionador incoado contra los responsables de ficheros de titularidad privada por infracción de los principios y reglas contenidos en la LORTAD; el procedimiento por infracciones de las Administraciones Públicas (art. 45) cuando es una Administración de esta clase la que vulnera los preceptos de la Ley; y el procedimiento de tutela de derechos, que se actúa cuando son vulnerados los derechos de acceso, rectificación o cancelación de los afectados (arts. 14 y 15).

La nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (L.O.P.D.), ha venido a reproducir el mismo esquema expuesto hasta aquí en relación con las funciones atribuidas a la Inspección de Datos por la LORTAD, si bien ha introducido una novedad en el procedimiento de tutela de derechos al ampliar el plazo máximo para dictar resolución a seis meses (art. 18.3 L.O.P.D.), siguiendo la pauta general que para los procedimientos administrativos establece la Ley 30/1992, de 26 de noviembre, en su art. 42.2.

1.1.3. **Expedientes relacionados con la función inspectora**

En el ejercicio de la función inspectora realizada por la APD durante el año 1999 se iniciaron **292** actuaciones de investigación o inspección, en su mayor parte promovidas por denuncias presentadas por los ciudadanos ante la APD, con el objeto de comprobar posibles vulneraciones de los principios de la LORTAD.

De estas **292** actuaciones de inspección iniciadas durante 1999, **163** han finalizado en dicho ejercicio, estando el resto: **129**, pendientes de concluir. A las **163** actuaciones de inspección iniciadas y finalizadas en 1999 hay que añadir aquellas otras, en concreto **99**, que iniciadas el año anterior finalizaron en el presente año, lo que hace un total de **262** actuaciones de inspección terminadas en 1999.

Así mismo, y al margen de lo anterior, se han realizado durante el mismo año **23** actuaciones de información previa con el fin de determinar con carácter preliminar si concurrían circunstancias que justificaran la iniciación de una actuación de inspección, y que no dieron lugar a su iniciación debido, en su mayor parte, a que los afectados o denunciantes no aportaron la información requerida desde la Inspección de Datos, imprescindible para poder continuar la tramitación de la inspección.

1.1.4. **Expedientes relacionados con la función instructora**

De las tres clases de procedimientos incoados en 1999 por lo órganos instructores de la Inspección de Datos, **131** corresponden a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad privada; **24** a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública (procedimientos por infracciones de las Administraciones Públicas); y **167** se corresponden a los iniciados por procedimientos de tutela de derechos.

De los **131** procedimientos sancionadores iniciados durante 1999, han finalizado en dicho ejercicio **74**, estando el resto: **57**, pendientes de concluir. A los **74** procedimientos sancionadores iniciados y finalizados en 1999 hay que añadir aquellos otros, en concreto **36**, que iniciados el año anterior finalizaron en el presente, lo que suma un total de **110** procedimientos sancionadores terminados en 1999.

De los **24** procedimientos por infracciones de las Administraciones Públicas iniciados en 1999, gran parte de ellos, en concreto **17**, han finalizado en dicho año, estando los **7** restantes pendientes de conclusión. Así mismo, se han

concluido durante el presente ejercicio **8** procedimientos de esta clase provenientes del anterior, lo que supone la conclusión de **25** procedimientos por infracciones de las Administraciones Públicas en 1999.

Finalmente, de los **167** procedimientos de tutela de derechos iniciados en 1999, la mayor parte de ellos, en concreto **147**, han finalizado en el mismo ejercicio, quedando tan sólo **20** pendientes de concluir. A los **147** antes citados hay que añadir los procedimientos de esta clase iniciados el año anterior, en concreto **48**, y terminados en el presente, lo que hace un total de **195** procedimientos de tutela de derechos concluidos en 1999.

A todo lo anterior debe añadirse la resolución de **65** recursos de reposición resueltos durante el mismo año 1999. La Ley 4/1999, de 13 de enero, de Modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ha restablecido el recurso de reposición contra los actos que ponen fin a la vía administrativa, con carácter potestativo. Toda vez que los actos resolutorios del Director de la Agencia en los procedimientos sancionadores ponen fin a la vía administrativa (art. 2.4 del Estatuto) y dada la novedad introducida por la citada Ley 4/1999, se ha producido por primera vez en la historia de la APD la presentación de recursos de reposición contra las Resoluciones de su Director. De los **65** recursos de esta clase presentados, **4** han sido estimados y **61** desestimados. No obstante, aun en estos últimos, su formulación ha facilitado la petición de suspensión de la ejecución de la Resolución sancionadora, lo que ha sido concedido por la Agencia en todos los casos en que se han considerado cumplidos los requisitos exigidos por la Ley 30/1992, de 26 de noviembre.

1.1.5. **Planes Sectoriales de Oficio**

Al margen de lo expuesto hasta aquí, y tal como se indica luego pormenorizadamente al hacer el análisis de la actividad por sectores, la Inspección de Datos ha desarrollado durante 1999 una intensa actividad en el marco de las actuaciones de oficio que la LORTAD permite.

En efecto, dentro de los Planes Sectoriales de Oficio que puntualmente realiza la Agencia de Protección de Datos para comprobar el grado de adecuación de los ficheros de las Administraciones Públicas y ficheros privados a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, el Director de la Agencia acordó durante el ejercicio 1999 iniciar Planes Sectoriales de Inspección de Oficio de los ficheros automatizados que contuvieran datos personales, tanto en el sector de las Instituciones públicas como privadas, a fin de comprobar el grado de protección que por las mismas se otorga al tratamiento de dichos datos y dictar las pertinentes Recomendaciones del Director de la Agencia de Protección de Datos para mejor adecuación al cumplimiento de la Ley.

Con este objeto, se han iniciado y terminado durante 1999 las Inspecciones de oficio realizadas a la Agencia Estatal de Administración Tributaria, a la Dirección General de Tráfico, al Sector de Investigación Privada, al Hospital Psiquiátrico de Font Calent, y al Hospital Militar Central Gómez Ulla.

Así mismo, ha concluido durante 1999 la Inspección de oficio realizada al Centro Nacional de Epidemiología, que tuvo su inicio en el ejercicio 1998.

En todos los casos se concluye con las pertinentes recomendaciones dictadas por el Director de la Agencia, en virtud de las potestades que le otorga el art. 5, c) y d) del Real Decreto 426/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, recomendaciones que deberán ser observadas por las Entidades inspeccionadas, al objeto de adecuar los tratamientos automatizados que realizan a los principios y prescripciones de la legislación sobre protección de datos.

Igualmente, y con el mismo objeto, se han dictado en 1999 las oportunas recomendaciones del Director de la Agencia dirigidas al Sector de Prestación de Servicios de Información sobre Solvencia Patrimonial y Crédito, y al Sector de Compañías Aseguradoras, cuyas inspecciones de oficio tuvieron lugar a lo largo de los ejercicios 1998 y 1999.

Por último, otra actividad importante de la Inspección de Datos en el área de los Planes Sectoriales de Oficio durante 1999 ha sido el relativo al campo de las telecomunicaciones. Durante dicho ejercicio se han practicado de oficio una serie de inspecciones a los principales operadores de telefonía fija: Telefónica de España, S.A., Retevisión, S.A. Lince Telecomunicaciones, S.A. (UNI2), y Euskaltel, S.A., de cara a conocer no sólo el grado de adecuación a la Ley Orgánica 5/1992, sino también al Real Decreto 1736/1998, de 31 de julio, por el que se desarrolla el Título III de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

1.2. **ESTADÍSTICAS MEDIANTE GRÁFICOS DE LOS EXPEDIENTES REFERIDOS**

1.2.1. **Gráficos correspondientes a la función inspectora**

A continuación, se puede observar en los gráficos I, II y III la distribución geográfica de las actuaciones de investigación o inspección referida anteriormente en el apartado 1.1.3., y separadas por: provincia del denunciante, provincia del denunciado y sectores de actividad inspeccionados.

GRÁFICO I

ACTUACIONES DE INSPECCIÓN INICIADAS
POR PROVINCIA DEL DENUNCIANTE

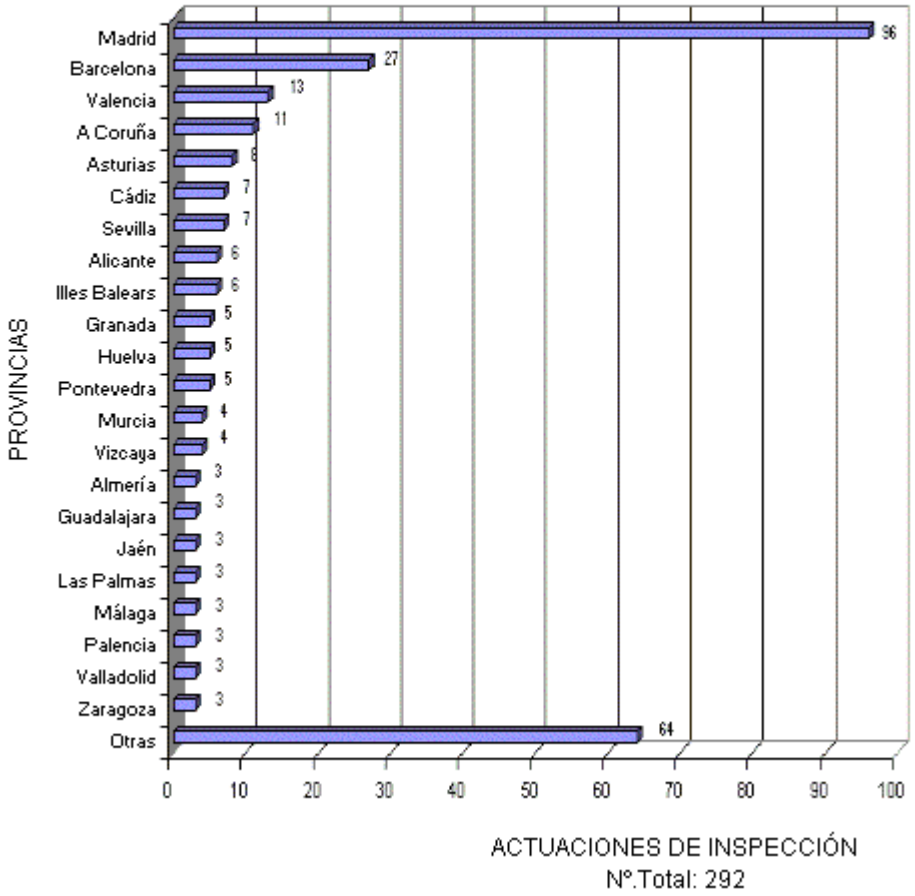


GRÁFICO II

ACTUACIONES DE INSPECCIÓN INICIADAS POR PROVINCIA DEL DENUNCIADO

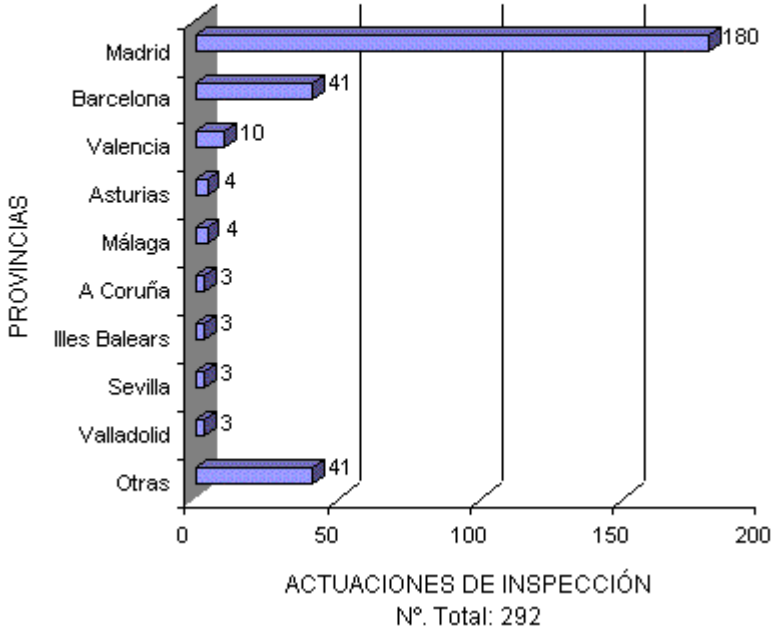
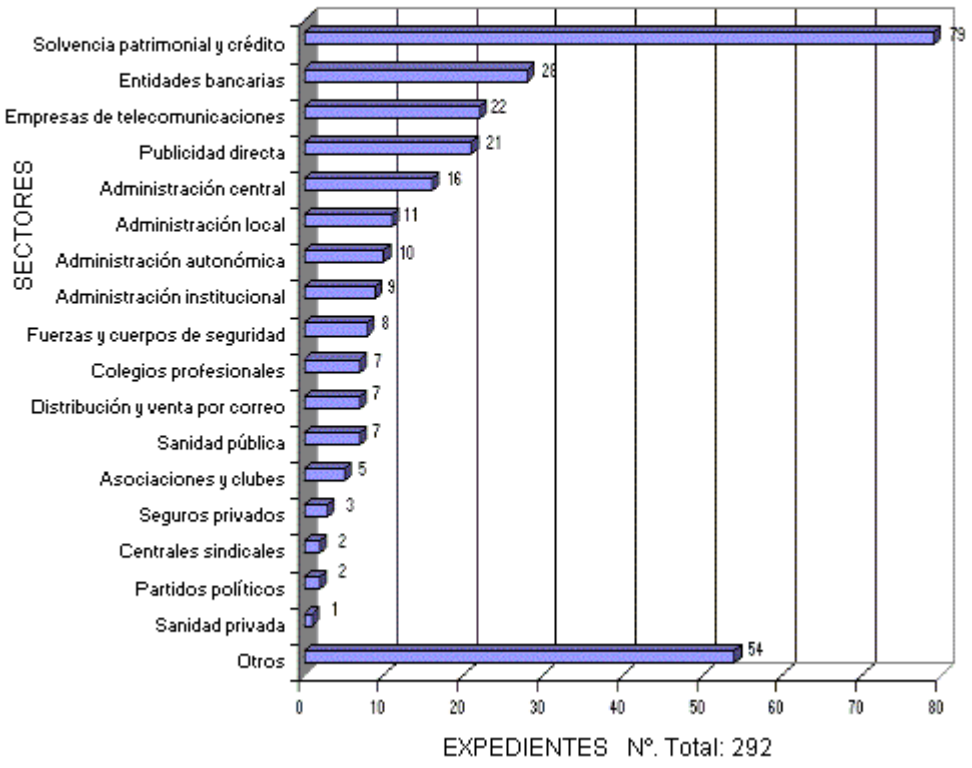


GRÁFICO III

ACTUACIONES DE INSPECCIÓN INICIADAS POR SECTORES DE ACTIVIDAD



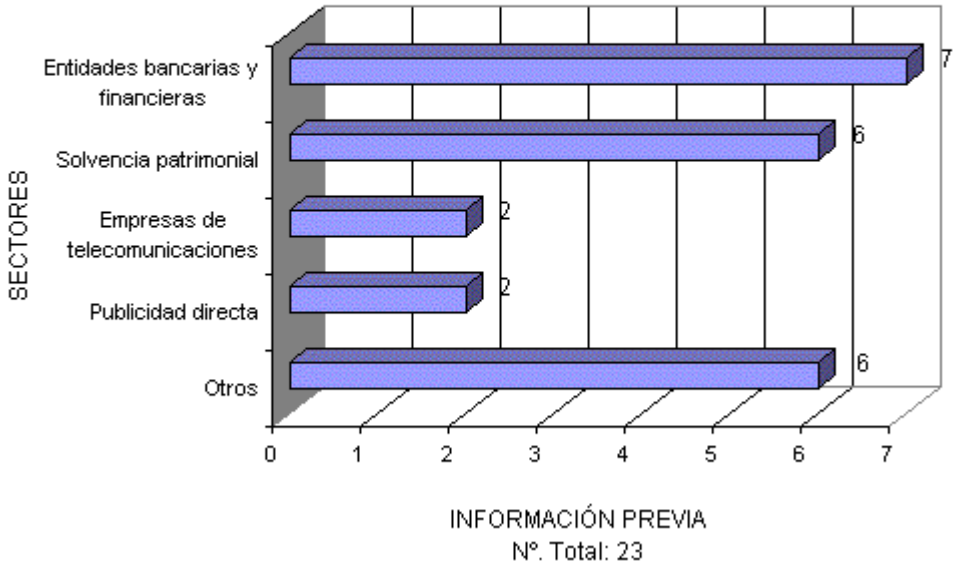
A consecuencia de una obligada reorganización y mejor racionalización del trabajo en la Subdirección General de la Inspección de Datos, en el presente año se han separado los procedimientos de tutela de derechos y actuaciones inspectoras de información previa de las consideradas estricta y más propiamente como actuaciones de investigación o inspección. Por esta razón, en la Memoria del presente ejercicio se ha seguido una sistemática distinta a la de 1998 a la hora de exponer y reflejar las actuaciones correspondientes a la función inspectora realizada en 1999, cuya consecuencia es la dificultad para poder realizar comparaciones referentes a este apartado entre uno y otro ejercicio al no corresponderse con actuaciones y cifras homogéneas.

En efecto, mientras en la Memoria de 1998 figuran iniciados **493** expedientes de inspección, en la de 1999 aparecen **292** actuaciones de esta clase. Ello es debido a que dentro de los **493** se incluyen no sólo las actuaciones de inspección *stricto sensu* **(312)**, sino también **154** procedimientos de tutela de derechos y **27** actuaciones de información previa, que, sin embargo, en la presente memoria de 1999 aparecen como actuaciones independientes y separadas de las primeras, tal como se observa en los gráficos IV y VII

A continuación, en el gráfico IV, se puede apreciar detalladamente la distribución por sectores de actividad de las actuaciones de información previa realizadas en 1999 a las que alude el anterior apartado 1.1.3.

GRÁFICO IV

ACTUACIONES DE INFORMACIÓN PREVIA POR SECTORES



Se observa en el año 1999 una ligera disminución de las actuaciones de información previa iniciadas este año (23) frente a las iniciadas en 1998 (27). Ello es debido a que mientras en 1998 las denuncias de los ciudadanos se concentraban en muy pocos sectores (esencialmente, Publicidad Directa y Solvencia Patrimonial y Crédito), en el presente ejercicio tales denuncias afectan a más y nuevos sectores como los de Entidades Bancarias y Financieras y Empresas de Telecomunicaciones.

Como conclusión de lo expuesto hasta aquí en relación con la actividad de la función inspectora, se aprecia una ligera disminución de tal actividad en 1999 respecto de la desplegada en 1998, pues, en efecto, mientras en 1998 se iniciaron **312** actuaciones de inspección y **27** actuaciones de información previa, en 1999 se iniciaron **292** y **23** actuaciones de una y otra clase, respectivamente.

Sin embargo, a esta conclusión sólo se llega si nos quedamos en un puro análisis cuantitativo y obedece esencialmente al menor número de denuncias presentadas por los ciudadanos en 1999. Pero al margen de esto, la realidad es que la actividad desplegada por la Inspección de Datos en este ejercicio ha aumentado, si bien desde el punto de vista cualitativo, toda vez que, siguiendo las instrucciones del Director de la Agencia, la Inspección ha dirigido sus principales esfuerzos hacia los Planes Sectoriales de Oficio, es decir, hacia una inspección más selectiva, persiguiendo un mejor conocimiento de los sectores más directamente implicados en el campo de la protección de datos personales. Se ha pretendido así dar la mayor difusión posible de los principios rectores de la LORTAD haciendo las pertinentes Recomendaciones a la vez que imponer una mayor disciplina de su cumplimiento en todos los sectores más directamente afectados, tal como se expone *supra* en el apartado 1.1.5.

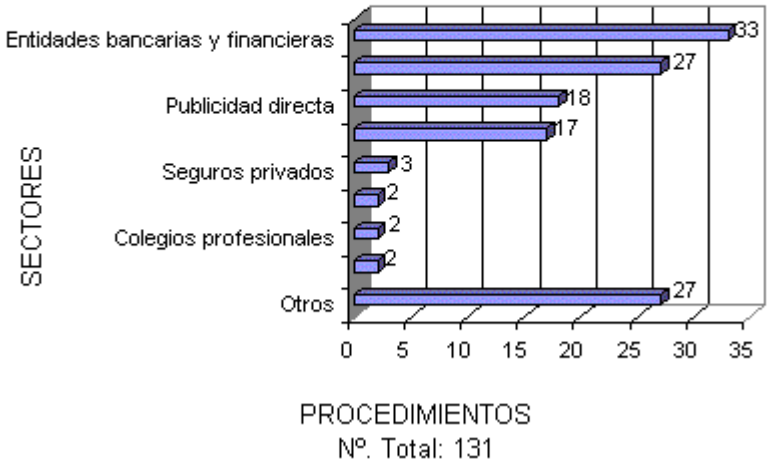
1.2.2. **Gráficos correspondientes a la función instructora**

Seguidamente, en los gráficos V y V bis, VI y VI bis y VII, se puede apreciar, de forma detallada, la evolución del número de expedientes tramitados durante 1999 y que afectan a la función instructora de la Subdirección General de Inspección de Datos, esto es, procedimientos sancionadores incoados frente a responsables de ficheros de titularidad privada, procedimientos sancionadores por infracciones de las Administraciones Públicas, y procedimientos de tutela de derechos.

Así mismo, y dentro de la función instructora se destaca en el gráfico VIII la evolución que presenta la novedad de los recursos de reposición.

GRÁFICO V

PROCEDIMIENTOS SANCIONADORES INICIADOS POR SECTORES

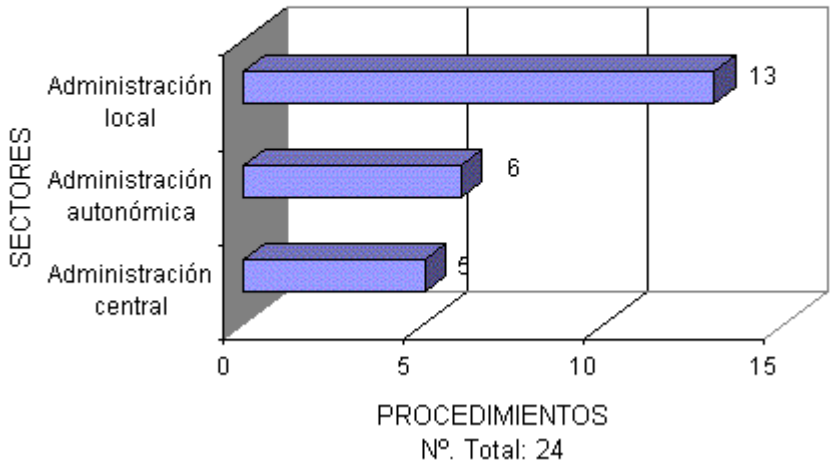


Nº. Total: 131

Comparando los 131 procedimientos sancionadores iniciados en 1999 con los 94 procedimientos de igual clase iniciados en 1998, se observa el notable incremento de procedimientos sancionadores incoados en el presente ejercicio. En concreto, supone un incremento del 40% respecto del año anterior.

GRÁFICO VI

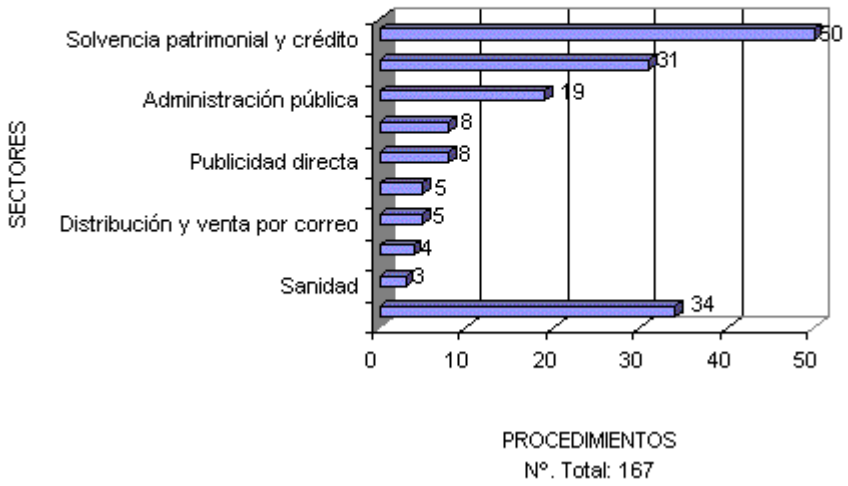
PROCEDIMIENTOS DE LAS AAPP INICIADOS POR SECTORES



En el área de los procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública o procedimientos por infracciones de las Administraciones Públicas es donde se ha producido un mayor salto cuantitativo respecto del ejercicio anterior. Así, frente a 6 procedimientos de esta clase iniciados en 1998, en el año 1999 se han incoado 24 procedimientos por infracciones de las Administraciones Públicas. Ello supone un incremento en 1999 de un 400%. Este aumento se debe al mayor número de denuncias presentadas por los ciudadanos frente a la actividad de la Administración y mayor conocimiento de sus derechos en cuanto a la protección que la LORTAD les otorga frente a posibles actuaciones ilícitas de las Administraciones Públicas.

GRÁFICO VII

PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR SECTORES

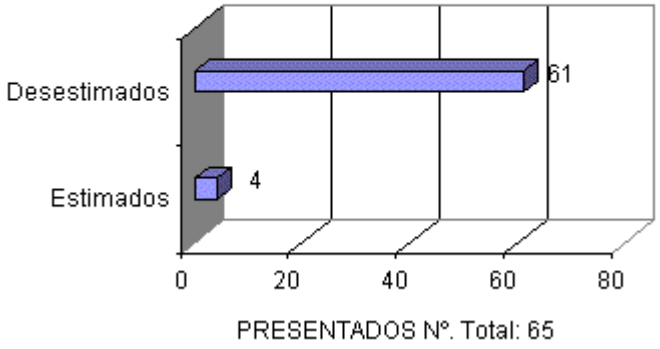


Al igual que en años anteriores, en 1999 la Agencia ha continuado tutelando los derechos de los ciudadanos optando por los procedimientos de esta clase en lugar de incoar procedimientos sancionadores, cuando, de las reclamaciones efectuadas por los ciudadanos, se deducía o expresaba claramente que su principal interés era la tutela de sus dere - chos a través del ejercicio del derecho de acceso, rectificación o cancelación de sus datos personales. Ello sin perjuicio

de la posible incoación posterior del correspondiente procedimiento sancionador si durante la tramitación del procedimiento de tutela de derechos se ponía de manifiesto la vulneración de alguno de los preceptos de la LORTAD.

Esta política de opción unida a un mayor número de reclamaciones de los ciudadanos pidiendo la tutela en el ejercicio de sus derechos reconocidos por la LORTAD ha supuesto la iniciación de 167 procedimientos de esta clase durante el año 1999, lo que supone un incremento del 15% respecto del año anterior.

GRÁFICO VIII
RECURSOS DE REPOSICIÓN



Finalmente, la novedad, introducida por la Ley 4/1999, de 13 de enero, del restablecimiento del recurso de reposición, ha supuesto que durante el año 1999 se presentaran y resolvieran por la Agencia 65 recursos de esta clase, de los cuales 61 han sido desestimados y 4 estimados al reconocerse por la Agencia error en la calificación de la infracción o apreciación indebida de los hechos.

Al margen de la carga de trabajo que el restablecimiento de este recurso ha supuesto para la función instructora, también hay que destacar el incremento de trabajo que tal recurso ha supuesto para la Secretaría General de la Agencia en orden a la calificación de la pertinencia de las garantías presentadas con el objeto de obtener la suspensión del acto impugnado.

2 **ANÁLISIS POR SECTORES DE ACTIVIDAD**

Siguiendo el criterio de Memorias anteriores, una vez presentada la visión global de lo que ha sido la actividad de la Inspección de Datos en 1999, se procede a detallar aquellos aspectos más relevantes puestos de manifiesto en el curso de las inspecciones realizadas en los distintos sectores de actividad público y privado.

2.1. **ADMINISTRACIÓN GENERAL DEL ESTADO.**

Durante el ejercicio 1999 la Agencia de Protección de Datos ha desarrollado una intensa actividad en la inspección de los ficheros de titularidad pública de los que son responsables los distintos órganos de la Administración Central, debido a que algunas de las organizaciones integradas en este sector disponen de ficheros automatizados de tal volumen y riqueza de contenido que incluyen datos de carácter personal de ámbito nacional con información concerniente a millones de españoles.

Las actuaciones realizadas por la Inspección de Datos durante este período se pueden agrupar en dos grandes bloques: Por una parte, las derivadas de atender las quejas formuladas por las personas que han denunciado una vulneración de los principios establecidos en la Ley Orgánica 5/1992, y, de otra, el desarrollo de Planes Sectoriales de Inspección de Oficio para comprobar el grado de adecuación de las Administraciones Públicas a las prescripciones de la normativa vigente sobre protección de datos de carácter personal, habiéndose seleccionado al efecto dos organismos de gran transcendencia para el ciudadano: la Agencia Estatal de Administración Tributaria y la Dirección General de Tráfico.

En el presente epígrafe analizaremos ambas líneas de actuación llevadas a cabo por la Inspección de Datos y concluiremos haciendo mención a las resoluciones del Director de la Agencia de especial relevancia en el sector público.

*2.1.1.**Actuaciones motivadas por quejas de los ciudadanos.***

Durante este año se han recibido en la Agencia un total de 31 escritos de ciudadanos relacionados con posibles infracciones a la Ley Orgánica 5/1992 por parte de diversas instituciones, que han dado origen a la apertura de 21

actuaciones previas y en el caso de diez de ellas a la tramitación de la correspondiente Tutela de Derechos. En cuanto a las Tutelas de Derecho, en cuatro de ellas, la Resolución del Director de la Agencia fue desestimar la reclamación formulada, ya que la solicitud planteada ante los responsables de los ficheros de titularidad pública no se enmarcaba en el ámbito de aplicación de la LORTAD.

Se observa que, como en años anteriores, sigue siendo un porcentaje sorprendentemente bajo las quejas puestas en conocimiento de la Agencia, en relación al número de Organismos incluidos en el sector público y al volumen de información que necesitan manejar para cumplir con las funciones que tienen asignadas.

Los Organismos sobre los que se han centrado las actuaciones previas han sido los siguientes:

* La Agencia Estatal de Administración Tributaria.
* Las Universidades Públicas.
* La Entidad Pública Empresarial Correos y Telégrafos.
* La Tesorería General de la Seguridad Social.
* El Instituto Nacional de la Seguridad Social.
* El Centro para el Desarrollo Tecnológico e Industrial.
* El Ministerio de Agricultura Pesca y Alimentación.
* El Instituto Social de la Marina, y
* El Ente Público Aeropuertos Españoles y Navegación Aérea.

De las 21 actuaciones previas iniciadas, en el caso de trece de ellas se procedió al archivo de las actuaciones al no haberse constatado la existencia de vulneración de lo establecido en la normativa vigente sobre protección de datos.

De las restantes, destacan las actuaciones efectuadas ante diversas Universidades Públicas relativas a la posible cesión de datos personales con objeto de la emisión de Tarjetas-Carnet, que se tratan en otro apartado específico de esta Memoria.

También cabe destacar el acuerdo de inicio de procedimiento de infracción de Administraciones Públicas a la Agencia Estatal de Administración Tributaria, por una posible utilización de los datos personales tributarios de una ciudadana para finalidades distintas de aquellas para las que se suministraron, que fueron las tributarias, con objeto de practicar notificaciones en materia de gestión de personal a terceras personas, por lo que dichos hechos podrían suponer infracción de lo previsto en el artículo 4.2 de la Ley Orgánica 5/1992.

Así mismo, destacan tres actuaciones de investigación practicadas ante la Entidad Pública Empresarial Correos y Telégrafos. Los hechos denunciados se refieren a la posible cesión por parte de dicha Entidad a empresas privadas de datos identificativos de sus trabajadores con objeto de la gestión y control de las ausencias laborales por motivos de salud. Las citadas actividades se enmarcan en un contrato suscrito por ambas partes (Entidad y las empresas adjudicatarias), que permite a éstas manejar datos personales referentes a la salud de los trabajadores. Al finalizar el año quedaban pendientes de concluir las actuaciones por parte de la Agencia.

2.1.2. ***Plan de Inspección de Oficio a la Agencia Estatal de Administración Tributaria.***

Entre las actividades desarrolladas por la Agencia de Protección de Datos se ha procedido a realizar de oficio un plan de inspección a la Agencia Estatal de Administración Tributaria (AEAT), ya que los ficheros de que dispone son unos de los más importantes de aquellos cuya titularidad corresponde a la Administración General del Estado, tanto por su naturaleza, características y colectivo al que afectan, como por la actividad desarrollada por el citado Ente Público, dada su gran transcendencia y repercusión para los ciudadanos.

Los objetivos a nivel general que se establecieron con las actuaciones del plan de inspección fueron los siguientes:

* Conocer los Sistemas de Información y Procedimientos utilizados por el Ente Público para el cumplimiento de las funciones que tiene asignadas relacionadas con el tratamiento automatizado de datos de carácter personal.

* Determinar el grado de cumplimiento y adecuación a las disposiciones de la Ley Orgánica 5/1992, respecto de los ficheros automatizados de los que es responsable.

* Establecer, en su caso, las deficiencias que pudieran existir en los tratamientos automatizados elaborándose las pertinentes recomendaciones con objeto de subsanarlas.

Inicialmente se procedió a realizar un estudio de los Sistemas de Información de que dispone la AEAT, ya que debido a su volumen y complejidad era necesario acotar el ámbito de actuación de la inspección, habiéndose seleccionado aquellos ficheros automatizados que se han considerado de mayor interés por los datos personales que incluyen, como son los procedimientos y ficheros relacionados con la gestión del Impuesto sobre la Renta de las Personas Físicas (IRPF). Posteriormente se elaboró un plan de inspección con la finalidad de determinar el grado de adecuación a la normativa vigente en materia de protección de datos.

Como resultado del análisis de la documentación requerida y de las inspecciones realizadas se obtuvieron las siguientes conclusiones:

* Respecto del cumplimiento del principio de calidad de datos, se ha detectado que la AEAT conserva en sus ficheros

automatizados los datos de las personas físicas que se han dirigido a ella, bien sea a efectos tributarios en el ámbito de la declaración de la Renta o para cualquier otra actividad, como puede ser la emisión de un certificado, no habiéndose producido cancelación de la citada información hasta la fecha. Sin embargo, el artículo 4 de la Ley Orgánica 5/1992, establece que "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".*

* Los formularios que deben cumplimentar los afectados con objeto de efectuar la declaración del IRPF, ordinaria, simplificada o abreviada, no hacen referencia al deber de información previsto en el artículo 5 de la LORTAD, como sería deseable aunque la misma pudiera deducirse de la naturaleza de los datos y de las circunstancias en que se recaban.
* Se ha comprobado que la información facilitada por los ciudadanos relativa a las deducciones por invidente, mutilado, inválido o enfermedad, que podría enmarcarse dentro de lo establecido en el artículo 7 de la Ley Orgánica 5/1992, está incluida en los ficheros automatizados exclusivamente con la denominación del concepto y el importe, por lo que no se puede deducir de la misma ningún dato personal referente a la salud de los contribuyentes.
* Se ha observado que la AEAT no dispone de unas normas documentadas que contemplen los procedimientos y criterios de la tramitación de las solicitudes del ejercicio de los derechos de los ciudadanos en los términos establecidos en la Ley Orgánica 5/1992, en el Real Decreto 1332/1994 y en la Instrucción 1/1998.
* También se han detectado algunas diferencias en cuanto a la inscripción de los ficheros automatizados de que dispone la AEAT

Por parte de la Agencia de Protección de Datos se dictarán a principios del año 2000 las recomendaciones oportunas para que la AEAT adopte las medidas pertinentes a fin de adecuar las deficiencias observadas en los tratamientos automatizados a los principios de la normativa vigente en materia de protección de datos.

2.1.3. ***Plan de inspección de oficio a la Dirección General de Tráfico.***

A finales de 1999 el Director de la Agencia acordó el inicio de un Plan de Inspección de oficio sobre los ficheros automatizados de la Dirección General de Tráfico, con el mismo fin de comprobar el grado de adecuación a las prescripciones de la LORTAD.

Tras analizar la inscripción de los doce ficheros notificados al Registro General de Protección de Datos de esta Agencia por la Dirección General de Tráfico, se consideraron los siguientes criterios para la selección de los ficheros a inspeccionar: a) Tratamiento y cesión de datos especialmente protegidos; b) Volumen de la información registrada en el fichero; c) Entidades que consultan u obtienen datos registrados en el fichero; y d) Reclamaciones recibidas en la Agencia de Protección de Datos. Considerando estos criterios, fueron seleccionados y objeto de inspección los siguientes ficheros:

- Base de Datos Accidentes Datos Personales
- Base de Datos Expedientes de Sanción
- Base de Datos Personas
- Base de Datos Vehículos

De las actuaciones de investigación y comprobación realizadas por la Inspección de Datos en la Dirección General de Tráfico, se han obtenido las siguientes conclusiones tras analizar el contenido de los ficheros y documentación adjunta a los mismos:

* **Respecto a la calidad de datos**

La Dirección General de Tráfico trata un gran volumen de datos personales, incluyendo datos especialmente protegidos, para el cumplimiento de las funciones que legalmente tiene atribuidas.

Tres de los cuatro ficheros: B. D.VEHICULOS (en adelante Vehículos), B. D. PERSONAS (en adelante Personas) y B. D. EXPEDIENTES DE SANCION (en adelante Sanciones) manejan gran cantidad de información: casi 35 millones de registros relativos a Vehículos, casi 27 millones de registros relativos a Personas y más de 5 millones de registros relativos a Sanciones.

Además, los ficheros Personas y B. D. ACCIDENTES DATOS PERSONALES (en adelante Accidentes) tratan datos de salud y los ficheros de Personas y Sanciones datos sobre infracciones administrativas.

* **Respecto al Derecho de Información en la recogida**

Los procedimientos de recogida de datos no ofrecen al afectado la información a la que se refiere el artículo 5.1. de la LORTAD.

La Dirección General de Tráfico ha definido un juego de impresos para cualquier comunicación con los ciudadanos en relación con los ficheros **Personas** y **Vehículos**. Se ha comprobado que en ninguno de los impresos examinados se informa al afectado sobre la inclusión de sus datos personales en un fichero automatizado.

Por su propia idiosincrasia, en el caso del fichero de **Accidentes** tampoco se informa a los afectados de la automatización de los datos recogidos sobre las víctimas y personas implicadas.

En relación con el fichero de **Sanciones**, los Agentes de la Agrupación de Tráfico de la Guardia Civil cumplen puntualmente con sus obligaciones, pero rara vez informan a los denunciados sobre la inclusión de sus datos personales en un fichero automatizado.

* **Respecto al Consentimiento para el tratamiento**

La mayor parte de los datos registrados en los ficheros **Vehículos** y **Personas** son facilitados por los propios afectados utilizando los impresos diseñados por la Dirección General de Tráfico. No obstante, en el fichero **Vehículos** la propia Dirección General de Tráfico registra información recibida de terceros: entidades financieras (limitaciones de disposición), estaciones de ITV (inspecciones y defectos) y Órganos Judiciales (embargos). En el fichero **Personas**, la Dirección General de Tráfico anota las sanciones que implican retirada del permiso de circulación.

En el caso de los ficheros de **Sanciones** y **Accidentes**, los datos son directamente recabados por los agentes de la Agrupación de Tráfico de la Guardia Civil.

En este sentido, el Real Decreto Legislativo 339/1990, de 2 de marzo, por el que se aprueba el Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad vial, prevé en su artículo 5 como competencias del Ministerio del Interior: la matriculación y expedición de los permisos o licencias de circulación; la vigilancia y disciplina del tráfico en toda clase de vías interurbanas y en travesías cuando no exista Policía Local, así como la denuncia y sanción de las infracciones a las normas de circulación y de seguridad en dichas vías; y la coordinación estadística y la investigación de accidentes de tráfico. Estas competencias se ejercen a través de la Dirección General de Tráfico conforme dispone el art. 6 del mismo texto legal.

El citado Real Decreto Legislativo también establece en su artículo 59 la obligación de mantener un registro de conductores y vehículos.

* **Respecto a la Cesión de datos**

La dirección General de Tráfico realiza cesiones a diversas instituciones y organismos públicos, tales como:

Direcciones Generales de la Policía y de la Guardia Civil, Organismos Judiciales, Agencia Estatal de Administración Tributaria, Tesorería de la Seguridad Social, Ministerios de Defensa e Interior, Presidencia del Gobierno, Gobierno Vasco, Generalitat de Cataluña, Consejo General del Poder Judicial y Servicio de Vigilancia Aduanera.

* **Respecto al ejercicio de los derechos de acceso, rectificación y cancelación**

La Ley 16/1979, de 2 de octubre, regula las tasas exigibles como contraprestación de los servicios y actividades prestados por la Dirección General de Tráfico. Entre los servicios que exigen contraprestación, muchos están relacionados con el ejercicio de los derechos de acceso, rectificación y cancelación, por ejemplo: cambios de titularidad en permisos de circulación por transferencia de vehículos; así como las anotaciones de cualquier clase en los expedientes, suministro de datos, emisión de certificaciones, cotejo y desglose de documentos.

Tal vez esta regulación haya condicionado que no exista un procedimiento formalmente documentado para el ejercicio de los derechos de acceso, rectificación y cancelación. No obstante, aunque los procedimientos no hayan sido formalmente definidos, no se han encontrado evidencias de que no se atienda correctamente el ejercicio de estos derechos.

Por todo lo expuesto, teniendo en cuenta que las actuaciones inspectoras al citado Organismo finalizaron a últimos de diciembre de 1999, cuando la nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, ya había sido publicada y prevista su entrada en vigor para el día 14 de enero de 2000, el Director de la Agencia de Protección de Datos decidió aplazar el dictado de las oportunas recomendaciones a la Dirección General de Tráfico, a fin de que las mismas fueran dictadas de acuerdo con la nueva Ley, permitiendo así al citado organismo una mejor adecuación de los tratamiento automatizados que realiza a los nuevos principios establecidos por la normativa vigente en materia de protección de datos.

2.1.4 ***Resoluciones más relevantes del Director de la Agencia de Protección de Datos en este sector de actividad.***

De entre las resoluciones dictadas por el Director de la Agencia referentes a ficheros cuya titularidad es pública merecen especial mención dos ellas: R/291/1999 y R/299/1999, que tienen su origen en denuncias formuladas por sendos ciudadanos en relación al suministro de sus datos personales sin su consentimiento a terceros, por parte de la Dirección General de Instituciones Penitenciarias y de la Agencia Estatal de Administración Tributaria, y que a continuación detallamos:

* Según se desprende de los hechos declarados probados, la Dirección General de Instituciones Penitenciarias comunicó vía fax a una entidad privada, para su incorporación a un fichero automatizado, una relación de las modificaciones de puestos de trabajo habidas en el Centro Directivo, conteniendo los nombres y apellidos de los funcionarios y el puesto de trabajo que desempeñan en la citada institución. La cesión de dichos datos se efectuó sin el consentimiento del afectado. Además, por razones de seguridad no se publican en el Boletín Oficial del Estado los nombramientos de los funcionarios que desempeñan un puesto de trabajo en la citada Dirección General. Por ello, el Director de la Agen-

cia de Protección de Datos resuelve declarar que la Dirección General de Instituciones Penitenciarias ha infringido lo dispuesto en el artículo 11 de la Ley Orgánica 5/1999, lo que constituye infracción tipificada como muy grave en el artículo 43.4.b) de la citada norma.

* La Agencia Estatal de Administración Tributaria ha facilitado a terceras personas un Certificado sobre la declaración del IRPF de un contribuyente sin el consentimiento del afectado y sin la acreditación de su personalidad ante el responsable del fichero. Para obtener certificaciones de las declaraciones del IRPF se exige que el peticionario titular exhiba o presente, junto al modelo de solicitud, una fotocopia del DNI.

El artículo 113.1 de la Ley General Tributaria en la redacción dada por la Ley 25/1995, dispone que "*Los datos o antecedentes obtenidos por la Administración Tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada, sin que puedan ser cedidos o comunicados a terceros".*

Por su parte, el art. 10 de la Ley Orgánica 5/1992 dispone que: *"El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo"*

En consecuencia, y a tenor de los artículos transcritos, se declara que la A.E.A.T. ha infringido el citado art. 10 de la LORTAD, infracción tipificada como grave en el art. 43.3 g) del mismo texto legal.

2.2 FICHEROS DE FUERZAS Y CUERPOS DE SEGURIDAD

Aunque alguna de las actuaciones aquí reseñadas afecten a organismos de la Administración General del Estado, se tratan en epígrafe independiente por su singularidad y unidad de criterio.

Al igual que en el año 1998, la mayoría de las actuaciones que se realizaron en el sector de las Fuerzas y Cuerpos de Seguridad fueron iniciadas de oficio, siendo el número total de las mismas de 9. En concreto, se realizó una inspección en la Jefatura Superior de Policía de Sevilla, se revisaron los ficheros automatizados de las Policías Locales de los Ayuntamientos de Arganda del Rey y Alcobendas, ambos en Madrid, iniciándose en este último caso Procedimiento de Infracción de Administraciones Públicas, y se verificó la inclusión de los datos de varias personas en el Sistema de Información Schengen a petición del Presidente de la Commission Nationale de L'Informatique et des Libertés (CNIL), autoridad competente en materia de protección de datos en Francia.

2.2.1 **Inspección en la Jefatura Superior de Policía de Sevilla**

A raíz de una información publicada en un diario nacional se iniciaron actuaciones de oficio para verificar si la Jefatura Superior de Policía de Sevilla mantenía unas fichas de filiación en las que se recogían datos de raza, color de piel y otras características físicas de los sospechosos.

En la inspección se constató que el personal de policía de la Unidad de Prevención de la Jefatura Superior de Policía de Sevilla recogía, en sus intervenciones de identificación en la vía pública, fichas manuales normalizadas, donde se recababan datos identificativos y de descripción física de las personas intervenidas. Así mismo, se constató que el Gabinete de Coordinación de esa Jefatura de Policía disponía de una base de datos en la que se registraban los que proporcionaban los denunciantes que han sufrido algún tipo de actividad delictiva, recabándose datos identificativos y características físicas del autor del hecho denunciado. Los datos de este fichero automatizado se suprimían cuando la investigación finalizaba y, en todo caso, seis meses después de que fueran registrados en el mismo. Los datos recogidos en las fichas se contrastaban con los recogidos en la base de datos con el fin de tratar de identificar a los autores del delito cometido.

En este caso, las actuaciones fueron archivadas entendiendo que el tratamiento realizado en las fichas manuales estaba fuera del ámbito de la LORTAD y que, en todo caso, la información se recababa en el ámbito de una investigación concreta amparada por el art. 20 de la citada Ley. Por otra parte, la información residente en los ficheros automatizados era cancelada al finalizar la investigación o transcurridos seis meses desde su introducción.

2.2.2 **Policías Locales**

Se iniciaron actuaciones para verificar si los Ayuntamientos de Arganda del Rey y Alcobendas habían procedido a cumplimentar unas fichas de filiación de personas que incluían datos antropomórficos relativos a la vida sexual, origen racial y salud, datos especialmente protegidos de acuerdo con el art. 7 de la Ley Orgánica 5/1992.

En el caso del Ayuntamiento de Arganda del Rey las actuaciones se archivaron, ya que aunque existía una orden de cumplimentar dichas fichas se comprobó que ninguna había sido finalmente cumplimentada y no se encontraron indicios de su posible automatización, resultando por ello no ser de aplicación la Ley Orgánica 5/1992.

En el caso del Ayuntamiento de Alcobendas, finalizadas las actuaciones de investigación, el Director inició Procedimiento de Infracción de Administraciones Públicas al comprobarse durante las mismas que la Policía Local mantenía un fichero automatizado de personas de interés policial en el que se recogían datos especialmente protegidos sin contar con el consentimiento de los afectados y sin cumplir lo señalado en el artículo 20 de la Ley Orgánica 5/1992 (relativo a los ficheros policiales y al tratamiento de datos personales sensibles sólo para investigaciones concretas).

Durante la tramitación de dicho procedimiento se constató que del total de registros con que contaba el fichero (1905), existían 415 casos reales que incluían datos antropomórficos de raza, vida sexual y salud, es decir, datos de los calificados como especialmente protegidos por el art. 7 de la Ley Orgánica 5/1992. Así mismo, se comprobó que efectivamente se infringía lo dispuesto en los artículos 7 y 20 para estos casos, ya que el Ayuntamiento no pudo probar la existencia de una investigación concreta, ni tampoco que dicha información fuera absolutamente necesaria para el buen fin de dichas investigaciones, así como que era injustificable que algunos de dichos datos correspondieran a intervenciones del año 1996.

Hay que resaltar que en este caso el Director de la Agencia había adoptado inicialmente una Medida Cautelar consistente en que ese Ayuntamiento cesara, de manera inmediata, en la utilización ilícita de los datos personales de carácter antropomórficos, de raza, vida sexual y salud que se recogían en el fichero en cuestión, así como que se adoptaran por el responsable de los ficheros las medidas técnicas u organizativas necesarias para que los citados datos no fueran accesibles por ninguna tercera persona física o jurídica ni por personal adscrito al Ayuntamiento. Tras comprobarse en una inspección que aun habiéndose ordenado la adopción de esta medida cautelar los datos en cuestión seguían permaneciendo en el fichero, el Director de la Agencia acordó la inmovilización del mismo en el que residían dichos datos.

También debe resaltarse que en la Resolución del Procedimiento el Director acordó elevar a definitiva la Medida Cautelar adoptada, así como ordenar la destrucción de los datos especialmente protegidos incluidos en el fichero.

2.2.3 **Sistema de Información Schengen**

Durante el año 1999 se han recibido 5 peticiones de la Comisión Nacional de Informática y las Libertades de Francia (CNIL) solicitando la colaboración de la Agencia al amparo del artículo 114.2 del Convenio de Schengen, en relación con peticiones de acceso a los ficheros del Sistema de Información Schengen (SIS) y en caso posible de cancelación, recibidas por personas que figuran incluidas en el SIS como personas no admisibles a territorio Schengen y cuyos datos habían sido introducidos por las autoridades españolas.

Por ello, se iniciaron actuaciones para verificar si los datos de dichas personas habían sido incluidos correctamente al amparo de la legislación vigente. En todos los casos se comprobó que dichas personas habían sido expulsadas del territorio nacional tras la incoación de un expediente de expulsión de conformidad con la Ley de Extranjería, decretándose la prohibición de entrada en el país. En todos los casos investigados se informó a la CNIL de las actuaciones realizadas, así como del motivo por el que figuraban dichas personas incluidas en el SIS.

2.3 ADMINISTRACIÓN AUTONÓMICA.

Durante 1999 se han recibido en la Agencia doce escritos en relación al posible incumplimiento de lo establecido en la Ley Orgánica 5/1992 por parte de responsables de ficheros de titularidad pública en el ámbito de las Comunidades Autónomas. La Inspección de Datos procedió al inicio de las correspondientes actuaciones previas excepto en un caso que se dio traslado a la Agencia de Protección de Datos de la Comunidad de Madrid por ser los hechos a investigar de su competencia, y en otro caso que se procedió a la apertura de una Tutela de Derechos cuya resolución finalizó desestimando la reclamación ya que no se enmarcaba en el ámbito de aplicación de la LORTAD.

Del análisis de los hechos objeto de investigación podemos indicar que la mayoría se referían a la posible cesión de los datos de que disponen las Comunidades Autónomas a entidades privadas. En algunos casos se constató que los citados hechos se podían enmarcar en una prestación de servicios de tratamiento automatizado de datos de carácter personal según lo previsto en el artículo 27 de la Ley Orgánica 5/1992. La mayor parte de las actuaciones finalizaron mediante resolución de archivo ya que no se pudo constatar la existencia de vulneración a lo establecido en la normativa vigente de protección de datos.

De entre estas actuaciones de investigación cabe destacar la iniciada ante la Generalitat Valenciana por disponer en una página Web de Internet de los datos personales relativos al nombre, apellidos y puesto de trabajo de unos diez mil funcionarios adscritos al citado Organismo. La información disponible al público fue utilizada por una entidad privada para remitir publicidad personalizada al puesto de trabajo de los funcionarios. Al finalizar el año quedaba pendiente de concluir las actuaciones por parte de la Agencia.

Otro dato a considerar es que durante 1999 han finalizado tres procedimientos de Administraciones Públicas en el ámbito autonómico con resolución sancionadora y que por su trascendencia detallamos a continuación:

* El Departamento de Economía y Hacienda del Gobierno Navarro facilitó a determinadas entidades, con las que previamente había suscrito un convenio de colaboración, un CD-ROM conteniendo datos identificativos y económicos de los contribuyentes navarros para facilitar la confección de las declaraciones del Impuesto sobre la Renta de las Personas Físicas. El sistema permitía el acceso a los datos tributarios de los clientes de las entidades financieras sin el consentimiento previo de los afectados. De ello se dedujo que el Departamento de Economía y Hacienda ha infringido lo dispuesto en el artículo 11 de la Ley Orgánica 5/1992, lo que supone una infracción tipificada como muy grave en el artículo 43.4.b) de la citada norma.
* La Conselleria de Bienestar Social de la Generalitat Valenciana ha utilizado datos personales tratados automatizadamente para finalidades no contempladas en las normas habilitantes de los ficheros: Pensiones no contributivas, Centros Base, Bonos Residencia, Fondo de Asistencia Social, Amas de Casa y Termalismo, de los que se obtuvieron los datos para la remisión de la invitación a la "Gran Fiesta de la Tercera Edad". Tal conducta supone una transgresión

del artículo 18.2 a) de la Ley Orgánica 5/1992, cuya tipificación se incardina en el supuesto contemplado en el artículo 43.2.d) de la citada norma con el carácter de infracción leve.
* El Servicio Canario de la Salud a instancias de sendos requerimientos de la Agencia de Protección de Datos no procedió a notificar los ficheros automatizados que contuvieran datos de carácter personal y cuya titularidad les correspondiera. Por ello el Director de la Agencia resuelve declarar la infracción del artículo 18 de la LORTAD tipificada como leve en el artículo 42.2.d) de dicha norma.

2.4 ADMINISTRACIÓN LOCAL

Durante 1999 se presentaron diez denuncias por posible infracción de la LORTAD relacionadas con ficheros gestionados por la Administración Local y que dieron lugar a las correspondientes actuaciones de investigación por la Inspección de Datos.

Seis de las denuncias presentadas se referían a la cesión de datos personales por parte de las Entidades Locales a otras entidades públicas o privadas sin el consentimiento de los afectados, y, en la mayoría de los casos, se referenciaba el padrón de habitantes como el origen de los datos cedidos. En cuatro ocasiones la denuncia se basó en el uso de los datos existentes en el padrón de habitantes o el censo electoral para realizar envíos de cartas personales con fines propagandísticos, informando de los logros conseguidos por el Ayuntamiento o para felicitar la onomástica a los vecinos.

El número de procedimientos de infracción de Administraciones Públicas por vulneración de la Ley Orgánica 5/1992 incoados a entidades integrantes de la Administración Local durante 1999 fueron nueve. De ellos, seis se debieron a infracción del artículo 18 de dicha Ley Orgánica, al desantender el requerimiento formulado por la Agencia de Protección de Datos para que procedieran a la inscripción de sus ficheros automatizados en el Registro General de Protección de Datos. En otras dos ocasiones se declaró que la Entidad Local había infringido lo dispuesto en el artículo 11 de la Ley Orgánica 5/1992, infracción tipificada como muy grave en la citada norma. Y en una sola ocasión se archivó el procedimiento al no quedar acreditados los hechos denunciados.

En este ámbito de actuaciones cabe destacar la incoación del procedimiento de infracción de Administraciones Públicas instruido al Ayuntamiento de Palma de Mallorca por haber suscrito un contrato con dos entidades bancarias y la Agrupación Empresarial de Agencias de Viajes de Baleares, con objeto de permitir a los ciudadanos empadronados en dicha ciudad expedir los certificados de residencia a través de la red de cajeros automáticos y de las agencias de viaje.

Según el sistema instaurado por el Ayuntamiento y las mencionadas entidades, para la obtención de un certificado de residencia es necesario disponer de una tarjeta con su respectivo PIN, operativa para la red de dichos cajeros, y tecleando el nº de DNI o el nº de Tarjeta de Residencia de cualquier vecino empadronado, el terminal visualiza los nombres y nº de DNI, o nº de Tarjeta de Residencia en caso de extranjeros, o fecha de nacimiento en caso de menores de edad, de todas las personas incluidas en la misma hoja padronal, pudiendo solicitar el certificado de empadronamiento de cualquiera de ellos.

El acuerdo de inicio del procedimiento sancionador establece que el Ayuntamiento de Palma de Mallorca puede incurrir en falta tipificada como muy grave al infringir lo dispuesto en el artículo 11 de la Ley Orgánica 5/1992, en el que se establece que los datos de carácter personal objeto de tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento de afectado. La resolución definitiva de este procedimiento se dictará en el año 2000.

2.5.SANIDAD

Las actuaciones de la Inspección de Datos en el ámbito del sector sanitario, en el que se enmarcan Hospitales de la Administración, tanto estatal como autonómica, se exponen en epígrafe independiente y separado del de las Administraciones Públicas, no sólo por razón de su singularidad sino también por razones de sistemática, al comprender tanto Hospitales del sector público como del privado.

En el año 1999 se han tramitado diversos expedientes de investigación relacionados con datos de salud, que han sido iniciados en el mismo año y otros cuyas actuaciones se iniciaron en 1998 y finalizaron en 1999. Como en anteriores epígrafes de esta Memoria, vamos a distinguir aquí entre las actuaciones iniciadas a instancia o en virtud de denuncias de particulares y las realizadas en virtud de Planes Sectoriales de Inspección de Oficio.

2.5.1 **Actuaciones realizadas en virtud de denuncias de los particulares.**

Entre las más relevantes podemos destacar las siguientes:

* En general, en 1999 ha habido una cierta inquietud en relación con la gestión de historias clínicas pertenecientes a Hospitales públicos, debido al traslado de dicha gestión a empresas privadas.

En este sentido, se han abierto 5 expedientes de investigación que han dado lugar a las pertinentes inspecciones con objeto de estudiar la gestión de historias clínicas en 9 Hospitales ubicados en Pontevedra, Valencia, Gijón y Madrid.

Algunos de los hospitales investigados ha manifestado realizar la gestión y custodia de las historias clínicas de forma interna en el propio centro.

En relación con todos los hospitales que manifestaron tener subcontratada dicha gestión y custodia con alguna empresa externa, se ha realizado la oportuna inspección a todas las empresas indicadas por aquéllos.

En las inspecciones realizadas, se ha comprobado que todas las empresas contratadas para realizar la gestión y custodia de las historias clínicas han generado ficheros para control de dicha actividad. Sin embargo, en los citados ficheros sólo se ha encontrado número de historia, nombre y apellidos de los pacientes cuyas historias clínicas son custodiadas, y en un sólo caso, también el DNI, lugar de nacimiento y sexo. Es decir, no se han encontrado datos clínicos.

Por esta razón, el Director de la Agencia ha resuelto *archivar* las actuaciones dado que no se ha apreciado infracción a la Ley Orgánica 5/1992, por no efectuarse tratamiento automatizado ni cesión de datos especialmente protegidos relativos a la salud, por las empresas que realizan las labores de gestión y custodia de los archivos de historias clínicas de aquellos hospitales que disponen de contratación externa. Además, dado que las historias clínicas se encuentran en formato papel, dicha gestión queda fuera del ámbito de aplicación de la LORTAD en cuanto que las citadas historias no se hallan informatizadas.

Por otra parte, las actuaciones de gestión y custodia realizadas por las empresas quedan amparadas en el artículo 27 de dicha Ley Orgánica, al mediar un contrato entre las partes implicadas.

Mención aparte merece un caso en el que una de las empresas implicadas ha realizado una digitalización de unos 20.000 episodios de Urgencias, a solicitud del hospital para el cual gestiona y custodia las historias. Dicha digitalización se realizó en el año 97, como prueba para comprobar la efectividad de la misma en la actividad cotidiana del hospital, no realizándose nuevas digitalizaciones con posterioridad. Este hecho está pendiente de resolver por la Agencia, por lo que se tratará en la Memoria correspondiente al año 2000.

* Otra de las denuncias se refiere a una posible cesión de datos a una clínica dental por parte de un médico que trasladó su residencia fuera del ámbito nacional. La denunciante presentó escrito de reclamación en la Agencia tras recibir publicidad de la clínica dental, con la que no había mantenido contacto alguno.

En la inspección realizada en la citada clínica, no se encontraron datos informatizados de la denunciante y, según manifestaron los responsables de la misma, los datos les fueron facilitados por el médico citado en libretas manuscritas con nombre, apellidos, dirección y teléfono de los pacientes, habiéndose destruido las libretas tras realizar el mailing a las personas allí incluidas.

El Director de la Agencia decidió *archivar* las actuaciones, dado que a la vista de los hechos denunciados, y teniendo en consideración que los datos relativos a la denunciante no estaban automatizados y se destruyeron al hacer el envío publicitario, tales hechos se encontraban fuera del ámbito de aplicación de la Ley Orgánica 5/1992.

* Otra de las denuncias se refería a unas fichas de cartulina y un libro-registro de atenciones de urgencias, conteniendo datos, diagnósticos y prescripción de medicamentos de pacientes identificados, correspondientes a una Gerencia de Atención Primaria determinada, que miembros de la Guardia Civil de una Comandancia de La Coruña se encontraron en una pista forestal. Las fichas de cartulina se referían a un período comprendido entre 1973 y 1986 y el libro-registro a 1988, todo ello manuscrito y algunas de las fichas escritas a máquina.

El Director de la Agencia resolvió *archivar* las actuaciones, por no ser de aplicación la LORTAD, dado que los datos contenidos en los documentos encontrados por la Guardia Civil no habían sido informatizados.

* Respecto al derecho de información en la recogida de datos, se ha abierto un Procedimiento de Administraciones Públicas por infracción del artículo 5 de la Ley Orgánica 5/1992 a un Centro de Transfusión autonómico, dado que al reclamante para donar sangre se le avisa sobre los siguientes apartados: exclusión total, exclusión temporal y otras recomendaciones, no apareciendo información sobre la automatización de sus datos, sobre el responsable del fichero, ni sobre la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

Este procedimiento ha sido *resuelto* por el Director de la Agencia de Protección de Datos, declarando que el Centro de Transfusión ha cometido infracción del artículo 5 de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento de Datos de carácter personal, tipificada como grave en el artículo 43.3 c) *in fine* de dicha norma.

2.5.2 Planes Sectoriales de Inspección de Oficio en el Sector Sanitario

Dentro de los Planes de Oficio que puntualmente realiza la APD para comprobar el grado de adecuación de las Instituciones públicas y ficheros privados a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, el Director de la Agencia acordó el inicio de un Plan de Inspección de los ficheros automatizados que contuvieran datos personales en el sector de las Instituciones Sanitarias de carácter público, a fin de comprobar el grado de protección que por las mismas se otorga en el tratamiento de los datos relativos a la salud, que la Ley califica como especialmente protegidos.

Como continuación del Plan de Oficio de Inspección a Hospitales, en 1999 se han inspeccionado los hospitales General Militar Gómez Ulla y Psiquiátrico Penitenciario de Alicante, con dependencia funcional del Ministerio de Defensa y de Justicia, respectivamente.

Así mismo, durante este año han finalizado dos inspecciones de oficio iniciadas en 1998 al Registro Nacional del Sida y

al denominado Proyecto TAIR (Terminal Autónomo de Identificación de Recetas) implantado en Centros de Salud de Atención Primaria del INSALUD.

De las actuaciones de investigación y comprobación realizadas por la Inspección de Datos de esta Agencia en los dos mencionados Hospitales, se han obtenido las siguientes conclusiones:

* ***Hospital General Militar Gómez Ulla***

El HOSPITAL GÓMEZ ULLA dispone de los datos de identificación de todos los usuarios del Instituto Social de las Fuerzas Armadas (ISFAS).

En 1989 el ISFAS, mediante acuerdo verbal, facilitó a la red hospitalaria del Ministerio de Defensa, los datos de identificación de todos los beneficiarios con cobertura sanitaria militar (beneficiarios y familiares con cobertura) al objeto de asignarles un número de historia clínica. Todo ello por razón de un proyecto de informatización de toda la red hospitalaria del Ministerio de Defensa denominado Proyecto Malta.

Posteriormente y con carácter mensual el ISFAS facilita al Hospital GOMEZ ULLA las variaciones habidas, mediante un disquete que incluye *Tipo, Parentesco, DNI, Afiliación, nombre y apellidos*

Estos datos se obtienen a partir de la Tarjeta Sanitaria diseñada al efecto para cuya solicitud es necesaria la cumplimentación de un formulario. Los afectados no han sido informados de que sus datos se facilitan al mencionado Hospital.

El resto de los datos de los pacientes son facilitados al Hospital por ellos mismos o son obtenidos como consecuencia de la asistencia sanitaria prestada por dicho centro.

En el Hospital GOMEZ ULLA no se informa a los afectados de los puntos incluidos en el artículo 5 de la Ley Orgánica 5/1992, de 29 de octubre.

Por otra parte, el impreso de solicitud de tarjeta sanitaria del ISFAS no incluye ninguna cláusula informativa al respecto.

Los afectados no han sido informados, por lo que no han prestado su consentimiento para que sus datos facilitados al ISFAS, sean entregados a la red hospitalaria del Ministerio de Defensa y posteriormente tratados por los hospitales.

Los médicos informan del estado de los pacientes de forma oral a los familiares directos de los mismos cuando así lo solicitan, siendo el propio médico quién decide el tipo de información a proporcionar. Las personas no allegadas únicamente reciben la información relativa a la cama en la que se encuentran ingresados los pacientes.

La solicitud del historial médico suele ser práctica habitual por parte de los pacientes que pasan a la situación de jubilación, por decidir cambiar su cobertura sanitaria al Régimen General de la Seguridad Social.

En estos casos realizan la solicitud por escrito en formato libre, siendo la Secretaría General Técnica del Hospital quien facilita un duplicado de la Historia Clínica en un plazo aproximado de una semana.

Hasta la fecha ningún paciente ha ejercido su derecho de acceso tal como está regulado en la Ley Orgánica 5/1992, de 29 de octubre.

La rectificación de datos de identificación se ejerce directamente en el ISFAS y posteriormente éste comunica al Hospital los cambios producidos. Los datos clínicos no son rectificados a petición del interesado.

Hasta la fecha no se ha producido ningún tipo de cancelaciones, por lo que no existen procedimientos al respecto.

No se recaban datos relativos a raza, ideología, religión o creencias de los afectados. Únicamente, datos relativos a la salud.

Únicamente se ceden datos en las siguientes ocasiones:

- Traslado definitivo del paciente a otro centro.

- Pacientes que se están dializando y se trasladan definitivamente a otros domicilios, por lo que necesitan realizar la hemodiálisis en otros centros.

- En los trasplantes de órganos, el centro que realiza el trasplante recibe datos de los pacientes.

En los anteriores casos se facilita un informe clínico en soporte papel.

Por otra parte, y al efecto de gestión de costes, se remite al Patronato de Seguro Militar la relación nominal de atenciones médicas realizadas. En dicha relación no se incluye el diagnóstico de los pacientes.

Así mismo se remite el Conjunto Mínimo Básico de Datos (CMBD) a la Consejería de Salud de la Comunidad Autónoma de Madrid (CAM) por imperativo de ésta. Como única identificación el CMBD lleva el número de historia.

Además se obtiene un soporte magnético con el I.R.P.F. para remitir a la Delegación de Hacienda correspondiente y otro soporte magnético con las nóminas para remitir a la entidad bancaria concertada para el pago de las nóminas.

En el Laboratorio de Análisis Clínicos, ocasionalmente se solicitan diversas pruebas analíticas al Instituto de Medicina Preventiva y al Instituto de Investigaciones Científicas Carlos III. En tales ocasiones se remite el tubo con la muestra, identificado mediante una etiqueta que contiene nombre y apellidos del paciente. Las muestras de pacientes externos además llevan el número de afiliación al ISFAS o a la Seguridad Social.

En el Servicio de Farmacia se confecciona un listado que se remite al ISFAS, que contiene Nº Asegurado, apellidos y nombre, médico, fecha e importe, a efectos de facturación.

El Hospital GOMEZ ULLA es un hospital integrado en el proyecto de informatización de hospitales militares denominado Proyecto Malta. En dicho proyecto están incluido la gestión asistencial general a pacientes (Admisión, Urgencias, Citaciones, etc.) y la gestión de Personal. El resto de los servicios del Hospital dispone de aplicaciones departamentales, desarrolladas por personal propio unas y por terceras empresas otras.

Las aplicaciones incluidas dentro del Proyecto Malta han sido desarrolladas por la empresa Shared Medical Systems Corp. (S.M.S.) Dado que el contrato formalizado entre dicha empresa y la Secretaría General Técnica del Ministerio de Defensa es de fecha anterior (mayo de 1988) a la entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, no existen cláusulas al respecto. Sin embargo, existe un acuerdo de confidencialidad de fecha 9/2/89 firmado por dicha empresa en el que consta "*Que S.M.S. tiene acuerdo de Seguridad otorgado por Dirección General de Armamento y Material del Ministerio de Defensa en grado de "Confidencial" desde la fecha 9 de febrero de 1989* ".

La aplicación de Anatomía Patológica ha sido desarrollada por la empresa Centro de Cálculo de Sabadell. Para ello, en fecha 28/5/98 se suscribió un contrato entre la Secretaría General Técnica del Ministerio de Defensa y la citada empresa, en el que no figura ninguna cláusula relativa a la Ley Orgánica 5/1992, de 29 de octubre.

En ambos casos se trata de contratos administrativos de prestación de servicios de asistencia realizados al amparo de la legislación sobre Contratos del Estado, que tienen por objeto el "mantenimiento del soporte lógico aplicado en los ordenadores de la Red Malta", en el primer caso, y el "mantenimiento del soporte lógico instalado en los Servicios de anatomía Patológica de los Hospitales de la Red Malta", en el segundo. Se trata de contratos de mantenimiento del Software que no tienen por qué llevar aparejado tratamientos de datos personales.

La inspección realizada en el Hospital GOMEZ ULLA es anterior a la entrada en vigor del Reglamento de Seguridad por lo que únicamente se han contemplado aspectos básicos de la misma.

La inscripción de ficheros actual se corresponde con la Orden de 26 de julio de 1994, del Ministerio de Defensa en la que entre otros ficheros recoge el de "DATOS CLÍNICOS DE PACIENTES", cuyo responsable es la Dirección General de Personal del Ministerio de Defensa.

A este fichero podrían corresponder los ficheros Maestro de pacientes, Episodios de Ingresos y Urgencias y Consultas Externas.

El citado fichero, según escrito del Secretario General Técnico del Ministerio de Defensa, corresponde al Proyecto Malta, por el que se integran todos los hospitales militares en un solo sistema informático con una única base de datos.

Sin embargo en la inspección realizada en el Hospital GÓMEZ ULLA se han encontrado ficheros "departamentales" con datos de carácter personal, no incluidos en el Proyecto Malta (entre otros, Servicio de Farmacia: Informes de farmacocinética, Laboratorio de Inmunología: Analíticas, Servicio de Hemoterapia: donantes de sangre y analíticas asociadas) y no inscritos en el Registro General de Protección de Datos.

A tenor de los resultados expuestos, derivados de las actuaciones inspectoras, el Director de la Agencia de Protección de Datos dictará en el próximo ejercicio las oportunas recomendaciones para una mejor adecuación de las actuaciones del mencionado Hospital a las prescripciones de la LORTAD, señalándose que dichas recomendaciones se circunscriben exclusivamente a la inspección realizada en el Plan de Oficio al Hospital Militar Gómez Ulla, y sin perjuicio del análisis que deba realizarse respecto de la aplicación de la normativa de protección de datos al conjunto del sistema de asistencia de las Fuerzas Armadas.

* ***Hospital Psiquiátrico Penitenciario de Alicante***

Los datos de todos los internos se encuentran en una base de datos centralizada en la Dirección General de Instituciones Penitenciarias, a la cual se tiene acceso desde todos los centros penitenciarios de España, entre ellos, como se ha podido comprobar, el Hospital Psiquiátrico Penitenciario, disponiendo de la opción de agregar nuevas altas o de realizar modificaciones.

Los pacientes nuevos facilitan sus datos de forma oral. En caso de que los pacientes provengan de otros centros, los datos de filiación los suministran dichos centros en formularios en formato papel. Además se dispone de la posibilidad de consultar a la aplicación mencionada en el párrafo anterior.

Por otra parte, se ha comprobado que los trabajadores sociales disponen de datos sociofamiliares de los internos, que han sido facilitados tanto por los propios internos como por familiares de los mismos.

El art. 6.2 del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario dispone que *"La recogida, tratamiento automatizado y cesión de los datos de carácter personal de los reclusos contenidos en los ficheros informáticos penitenciarios se efectuará de acuerdo con lo establecido en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal y sus normas de desarrollo"*

Dadas las características de los internos, en ningún momento se informa a los afectados de sus derechos, conforme a lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

No se obtiene consentimiento de los afectados para tratar sus datos de carácter personal.

El RD 190/96, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario, regula el tratamiento de los datos de carácter personal tratados en los centros penitenciarios. Concretamente el artículo 7.1 especifica que *"cuando los datos de carácter personal de los reclusos se recojan para el ejercicio de las funciones propias de la Administración Penitenciaria no será preciso el consentimiento del interno afectado, salvo en los relativos a su ideología, religión o creencias".* Se ha podido comprobar que el Hospital Psiquiátrico Penitenciario no recoge datos relativos a ideología, religión o creencias.

Todo el personal trabajador del Centro está obligado al deber de secreto tanto por la Ley General de Sanidad como por el Real Decreto 190/1996, relativo al Reglamento Penitenciario que en su artículo 6.3, establece que las autoridades penitenciarias responsables de los ficheros informáticos penitenciarios *"estarán obligadas, junto con quienes intervengan en cualquier fase del tratamiento automatizado de este tipo de datos, a guardar secreto profesional sobre los mismos, incluso después de que haya finalizado su relación con la Administración Penitenciaria".*

No se dispone de ningún procedimiento específico del Hospital Psiquiátrico Penitenciario relativo al suministro de información a terceros. Tanto el Subdirector Médico como los médicos, informan del estado de los pacientes de forma oral a familiares directos de los mismos o a sus propios abogados representantes.

También facilitan informe escrito sobre la situación penal de los internos a petición del interesado o, si lo solicita, alguna otra Institución de las mencionadas en el artículo 7 del R.D. 190/1996, respecto de las cuales está legalmente prevista la cesión.

Existe un modelo de instancia a disposición de los internos, mediante el que pueden solicitar cualquier servicio, entre ellos los derechos de acceso o rectificación.

El derecho de rectificación se encuentra regulado por el R.D. 190/1996, que en su artículo 9 establece que *"los reclusos podrán solicitar de la Administración Penitenciaria la rectificación de sus datos de carácter personal contenidos en los ficheros informáticos penitenciarios que resulten inexactos o incompletos. De la rectificación efectuada se informará al interesado en el plazo máximo de* ***dos meses*** *desde su solicitud, así como al cesionario o cesionarios, en el supuesto de que los datos incorrectos hubiesen sido objeto de cesión previa".*

El derecho de cancelación se encuentra regulado también en el citado art. 9, que establece: *"Los datos de carácter personal de los reclusos contenidos en los ficheros informáticos penitenciarios no serán cancelados cuando, ponderados los intereses de presencia, concurran razones de interés público, de seguridad y de protección de los derechos y libertades de terceros, así como cuando posean un valor intrínseco de carácter histórico y estadístico a efectos de investigación".*

Según declaraciones de los responsables, hasta la fecha no se ha producido ningún tipo de cancelación de datos.

En el fichero que gestiona los ingresos y las altas de los internos, se recogen datos relativos a la salud de los mismos.

En ningún caso se recogen datos relativos a la raza, ideología, religión, creencias o vida sexual de los pacientes. En los ficheros revisados durante la inspección realizada, no se ha encontrado esta tipología de datos.

Según declaraciones de los responsables, únicamente se ceden datos de los internos en los siguientes casos:

- Traslado del paciente a otro centro.

- A otras Administraciones de las citadas en el art. 7 del RD 190/96, y respecto de las cuales está prevista legalmente la cesión.

- Semestralmente se realiza un informe personalizado de todos los pacientes que se emite por triplicado, remitiéndose cada una de las copias a los siguientes destinos: Ministerio del Interior, Tribunal que ha dictado la sentencia de internamiento y Juez de Vigilancia Penitenciaria.

En todos estos casos se facilita un informe clínico en soporte papel.

Por otra parte, periódicamente se envía a la Consejería de Salud de la Comunidad Valenciana el fichero creado a tal efecto CMBD (Conjunto Mínimo Básico de Datos). El CMBD es un subconjunto entre toda la información que puede producir un proceso hospitalario que contiene datos de carácter personal llevando como única identificación el número

de historia clínica, no incluyendo nombre y apellidos de los pacientes. La legislación existente al respecto es la Orden de 8/10/92, de la Consellería de Sanitat i Consum (de la Comunidad Valenciana), por la que regula el conjunto mínimo básico de datos a utilizar en la información hospitalaria.

En el caso de solicitud de información por Instituciones extranjeras, la Dirección General de Instituciones Penitenciarias del Ministerio del Interior, es la que decide su entrega, que únicamente comprenderá datos de internos procedentes del país solicitante.

El art. 7.4 del Reglamento Penitenciario dispone a estos efectos que *"Las transferencias internacionales de datos de carácter personal contenidos en los ficheros informáticos penitenciarios se efectuarán en los supuestos de prestación de auxilio judicial internacional, de acuerdo con lo establecido en los tratados o convenios en los que sea parte España".*

A fecha de la inspección realizada en el Hospital Psiquiátrico Penitenciario, no se había publicado el R.D. 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, publicado en fecha 25/6/99.

En el citado Hospital se dispone de las siguientes medidas:

- Para acceder a los equipos informáticos, al igual que para acceder a las diversas aplicaciones, siempre es necesaria la introducción previa de una contraseña. Dicha contraseña en algunas ocasiones es genérica y en otras es individualizada.

- En algunos casos está limitado el número de intentos fallidos de acceso al equipo informático.

- Algunas aplicaciones disponen de registros de auditoría que permiten conocer el usuario, la fecha y hora de entrada y salida de cada uno de los accesos a los datos realizados.

- Los despachos que contienen equipos informáticos que gestionan datos especialmente protegidos, se quedan cerrados con llave cuando no se encuentran presentes los miembros del propio despacho.

Tras realizar la inspección en el Hospital Psiquiátrico Penitenciario, con fecha 8/7/99 se informó al Registro General de Protección de Datos acerca de los ficheros automatizados encontrados en dicho Hospital.

Con fecha 20/7/99 la Subdirección del Registro General de Protección de Datos informó que tras realizar un análisis sobre la inscripción de ficheros realizada por el Ministerio del Interior, se han encontrado una serie de ficheros que por su finalidad, podrían corresponderse con la mayoría de los indicados en el escrito remitido por la Inspección de Datos. Sin embargo no se ha localizado entre los ficheros inscritos, ninguno con los que pudieran corresponderse los ficheros ARCHIVO y SOCIAL encontrados en la inspección realizada.

A la vista de los resultados de las actuaciones practicadas por la Inspección de Datos, el Director de la Agencia de Protección de Datos dictará en el año 2000 una serie de recomendaciones que deberán ser observadas por dicho hospital, de las cuales se dará información en la Memoria del próximo año.

* ***Registro Nacional del Sida***

En la Memoria correspondiente a 1998, se describió el funcionamiento del fichero denominado *Registro Nacional del SIDA*, inscrito en el Registro General de Protección de Datos con el código 1942346891, cuya inspección ha finalizado en el presente ejercicio.

De las actuaciones de investigación y comprobación realizadas por la Inspección de Datos de esta Agencia al Centro Nacional de Epidemiología, se han obtenido las siguientes conclusiones:

El Registro Nacional del SIDA, encuadrado en el Centro Nacional de Epidemiología, contiene la información nacional de personas que han desarrollado SIDA referente a 52.000 afectados, de los cuales el 50% han fallecido.

Dicho registro es comprensivo de datos relativos a nombre, apellidos y fecha de nacimiento de los afectados con el fin de evitar duplicados y poder incorporar información de interés epidemiológico que se genere a posteriori, especialmente datos del fallecimiento. La detección de duplicados es frecuente ya que un mismo enfermo puede ser notificado desde diferentes hospitales e incluso desde diferentes provincias.

Además se recogen datos de sexo, edad, provincia de residencia, país de residencia y país de origen, que se utilizan para estudios epidemiológicos.

Como subproducto de este fichero se obtiene un fichero con datos anonimizados para remitir al Centro Europeo de la Organización Mundial de la Salud en París y otro que se remite al Instituto Nacional de Estadística con datos no identificables.

El flujo de información para nutrir el fichero Registro Nacional del SIDA es el siguiente:

Los Centros Públicos y Privados, que atienden a pacientes que han desarrollado SIDA, recogen los datos en formula-

rios diseñados al efecto a nivel nacional.

Desde 1994, una vez que los formularios han sido cumplimentados en los distintos Centros, son remitidos a las Consejerías de Salud de las Comunidades Autónomas (CC.AA.) donde son automatizados mediante una aplicación desarrollada por el Ministerio de Sanidad y Consumo.

Las CC.AA. trimestralmente remiten al Centro Nacional de Epidemiología un disquete que contiene tanto, los nuevos casos producidos, como las modificaciones que se produzcan en los ya registrados. Cuando las modificaciones no son numerosas, éstas se remiten en formato papel con la única identificación del número de caso.

Una vez han sido descargados en el Registro Nacional del SIDA los datos remitidos por las CC.AA., el Centro Nacional de Epidemiología devuelve a la CC.AA. su fichero, con el espacio reservado para el "nº de caso" cumplimentado.

Igualmente se devuelve a las CC.AA. un listado con los "números de caso" de duplicados.

El Centro Nacional de Epidemiología remite a cada CC.AA. sus propios casos de afectados por la enfermedad.

Los médicos a los que acuden los afectados son parte activa del sistema y el único punto de contacto directo del sistema de información con los afectados.

El médico que trata al enfermo es el que está obligado a declarar el caso al Registro del SIDA de las CC.AA., de acuerdo al Real Decreto 2210/1995 de Creación de la Red Nacional de vigilancia Epidemiológica, y es quien debe informar a los afectados de su notificación a los Registros del SIDA Autonómico y Nacional. El Registro Nacional del SIDA no cuenta con información sobre si por el médico correspondiente se informa al enfermo de la inclusión de sus datos en el fichero del SIDA Autonómico y Nacional. No obstante, se deduce su conocimiento por el enfermo de su inclusión en el Registro del SIDA Autonómico, habida cuenta de que para acceder a la prestación farmacéutica (abonan el 10% de los medicamentos) necesitan acreditar que cumplen los criterios del SIDA mediante un certificado emitido por el Registro Autonómico correspondiente.

En casos especiales, existe la posibilidad de acceso a la información del Registro Nacional del SIDA por parte de Instituciones ó personal sanitario con fines de investigación, requiriéndose la solicitud justificada del investigador, la valoración positiva por parte del organismo responsable y la firma del compromiso de confidencialidad por el investigador. En tales casos, el acceso a los datos identificativos del paciente siempre se canalizará a través del médico ó del centro encargado de su tratamiento.

No obstante lo anterior, según se ha constatado en la inspección realizada, hasta la fecha no se ha producido ninguna cesión de datos a médicos ó a investigadores con datos nominales.

Las peticiones de información son estudiadas por la Secretaría General del Plan sobre el SIDA, la cual autorizará en su caso la cesión de la información solicitada en función de la legislación vigente.

La única transferencia internacional que se realiza es al Centro Europeo de la Organización Mundial de la Salud ubicada en París, donde se centraliza a nivel europeo toda la información relativa al SIDA. Los datos se remiten anonimizados en una estructura de registro normalizada por dicho organismo.

Según el Acta de Inspección, hasta la fecha, sólo un afectado ha ejercido su derecho de acceso cuyos datos no fueron encontrados en el fichero, probablemente porque no se tratara de un caso de SIDA, sino de un infectado.

El Registro Nacional del SIDA únicamente es gestionado por tres personas, siendo una de ellas el responsable de dicha gestión.

El ordenador que contiene el fichero está ubicado en un despacho que se cierra con llave cuando no se encuentran en él los responsables de la gestión.

Aunque en alguna ocasión se imprimen datos de los afectados al objeto de realizar algún control en ningún caso se generan informes con los datos de identificación de los afectados. Sólo se realizan informes estadísticos que son públicos y accesibles a través de Internet. No se guarda el soporte papel que se obtiene siendo destruido en el mismo despacho.

Existe una contraseña de "setup" para acceder al ordenador. La contraseña de acceso a la aplicación se cambia cuando hay alguna incidencia (v.gr.: cambio de personas responsables).

No se guardan registros de auditorías de las operaciones que pueden afectar a los usuarios sobre los datos del fichero a través de la aplicación ó desde el propio Dbase.

La base de datos está comprimida y cifrada y el ordenador que la contiene está encendido en tanto se utiliza, permaneciendo apagado el resto del tiempo.

El mantenimiento del sistema se lleva a cabo por los propios profesionales que trabajan en el Registro Nacional del SIDA. Ocasionalmente se ha recurrido a personal del Área de Informática del Instituto de Salud Carlos III, siendo aplicadas las soluciones por los responsables del registro.

Ninguna empresa informática de mantenimiento tiene acceso al ordenador donde se encuentra la base de datos del Registro Nacional del SIDA.

El Centro Nacional de epidemiología tiene inscrito en el Registro de Protección de Datos de la Agencia de Protección de Datos el fichero denominado "Registro Nacional del Sida", con fecha de inscripción 22/08/1994 y número de código 1942346891, cuyo objeto es la información específica a la Administración Sanitaria para garantizar la salud pública y prevención del SIDA, tratamiento estadístico y estudios epidemiológicos e investigación sanitaria.

A la vista de los resultados de las actuaciones practicadas por la Inspección de Datos en el Registro Nacional del Sida, el Director de la Agencia de Protección de Datos dictará en el año 2000 una serie de recomendaciones que deberán ser observadas por el Centro Nacional de Epidemiología, de las cuales se dará información en la Memoria del próximo año.

* ***Proyecto Tair***

Las actuaciones de investigación del denominado proyecto TAIR (Terminal Autónomo de Identificación de Recetas), implantado en los Centros de Salud de Atención Primaria del INSALUD comenzaron en 1998 (describiéndose en la memoria correspondiente a dicho año el funcionamiento del TAIR) y han finalizado en 1999. Dichas actuaciones fueron originadas por denuncias presentadas ante la Agencia de Protección de Datos por posibles vulneraciones de la LORTAD.

De las actuaciones practicadas se desprende que a partir del TAIR se generan dos flujos de información:

a) Interno, relativo a la actividad asistencial y recetas médicas sin que se recoja en ellas el medicamento prescrito.

b) Externo, relativo a la información generada por la receta médica, su grabación por los colegios de farmacéuticos y su remisión posterior al INSALUD.

Las denuncias presentadas han exigido que fuera éste último circuito externo el analizado para la inspección, de la que resultó lo siguiente:

El TAIR genera una etiqueta para adherir a la receta, que contiene: datos del paciente, del médico, el nº de orden de la receta y la fecha de prescripción.

Dado que el TAIR no recoge el dato relativo al medicamento prescrito, éste es incluido en la receta de forma manual por el médico.

Las oficinas de farmacia dispensadoras de los medicamentos, recogen las recetas agregando físicamente el cupón precinto que contiene otro código de barras que corresponde al medicamento, así como los datos relativos a la propia farmacia.

Posteriormente, las recetas son enviadas a los respectivos Colegios Farmacéuticos, donde, generalmente a través de terceras empresas contratadas al efecto, se graban en un CD ROM para ser enviado mensualmente al consejo General de Colegios Farmacéuticos.

Una de las innovaciones que ofrece el nuevo proyecto respecto a la grabación de recetas que se viene haciendo desde hace años, es la incorporación de la identificación del paciente mediante el Código de Identificación Personal (CIP) incluido en la Tarjeta Sanitaria, identificación que con anterioridad se efectuaba escribiendo el nombre del paciente.

La única información identificativa personal que se puede grabar en los Colegios Farmacéuticos es el Código de Identi - ficación Personal (CIP) de los pacientes y el Código de Identificación de Área Sanitaria (CIAS) de los médicos.

La actuación de los Colegios Farmacéuticos, se rige por el Concierto firmado con fecha 17/11/98, -"Concierto por el que se fijan las condiciones para la ejecución de la prestación farmacéutica a través de las oficinas de farmacia"- que fue suscrito entre el Presidente Ejecutivo del INSALUD y el Director General de la Tesorería de la Seguridad Social, por una parte, y el Presidente del Consejo General de Colegios Oficiales de Farmacéuticos, por otra.

El Concierto se rige por sus condiciones particulares, siendo de aplicación directa la normativa sanitaria por la que se regula la prestación farmacéutica en general y, en su caso la de Seguridad Social en particular, así como la Ley Orgá - nica 5/1992, de 29 de octubre, y resultando aplicable subsidiariamente la legislación reguladora de contratación del Estado.

La cláusula 6 garantiza la confidencialidad de los datos de carácter personal. Cualquier uso distinto de la facturación deberá ser autorizado por el INSALUD.

Los datos se graban en un CD ROM por cada uno de los Colegios Farmacéuticos que, a través del Consejo General, los entregarán a las dependencias del INSALUD señaladas por éste.

En algunos casos los Colegios Farmacéuticos proceden a contratar la grabación de datos obligándose a las empresas a salvaguardar la identidad y el secreto de los mismos, de acuerdo con las instrucciones del cliente y lo que establece

al respecto la legislación vigente.

Por Resolución del Director de la APD de fecha 24-4-99 se acordó el archivo de las actuaciones en relación con el tratamiento de datos de las recetas. Los fundamentos de la Resolución de archivo son, sintéticamente, los siguientes:

a) Según se desprende de las actuaciones practicadas por la Inspección, las únicas novedades derivadas de la introducción del TAIR consisten en la incorporación a la receta del Código de Identificación del Paciente (CIP) en texto y en Código de barras y en la impresión en código de barras del Código de Identificación de Asistencia Sanitaria (CIAS) correspondiente al médico, dato que ya se incluía con anterioridad en la receta.

La norma habilitante para la creación e ficheros automatizados del Ministerio de Sanidad y de sus organismos autónomos es la O.M. de 21 de julio de 1994. En ella se contempla un fichero específico de "usuarios nacionales de la tarjeta sanitaria", inscrito en el Registro General de Protección de Datos, que comprende, en el apartado relativo a la finalidad y usos, el correspondiente a la gestión y control sanitario. Las personas o colectivos afectados son todos los usuarios del sistema nacional de salud y los organismos oficiales de estadística.

De lo expuesto anteriormente se desprende que la novedad del TAIR, en lo que se refiere al tratamiento de nuevos datos de usuarios del sistema nacional de salud y, en particular, de personas con derecho a la prestación farmacéutica, se limita a la información relativa al CIP, contenida en la TSI (TARJETA SANITARIA INDIVIDUAL).

El nuevo tratamiento de datos de titulares de la TSI tiene habilitación normativa puesto que es subsumible en el fichero de "usuarios nacionales de la tarjeta sanitaria" incluido en la O.M. de 21 de julio de 1994 e inscrito en el Registro General de Protección de Datos. En consecuencia no cabe apreciar la existencia de una infracción administrativa.

b) En lo que se refiere al consentimiento de los afectados para la obtención de datos personales, la regla general del art. 6 de la LORTAD es la exigencia del mismo salvo que la Ley disponga otra cosa.

Sin embargo, el apartado 2 de dicho precepto exceptúa la obtención del consentimiento de los afectados cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.

Dado que el art. 85 LM exige que la receta contenga los datos básicos de identificación del paciente y que tales datos se han asociado a los contenidos en la TSI, debe estimarse que la Administración Sanitaria está actuando en el marco de sus competencias y que la recogida y el tratamiento de los datos que figuran en la TSI son adecuados, pertinentes y no excesivos en relación a aquéllas, conforme al art. 4 LORTAD, por lo que cabe prescindir del consentimiento del afectado de acuerdo con el art. 6.2 de la misma ley.

c) El art. 8 de la LORTAD habilita para proceder al tratamiento automatizado de los datos personales relativos a la salud de las personas que acudan a las instituciones y centros sanitarios o hayan de ser tratados en los mismos, siempre que dicho tratamiento se realice de acuerdo con la normativa sanitaria.

Dado que los aspectos operativos del Proyecto TAIR se limitan a la grabación e los datos incorporados en las recetas con la finalidad de efectuar su facturación y el control de ésta, y no a otros desarrollos pendientes en los términos expuestos en los antecedentes de hecho, la habilitación para el tratamiento de datos por parte de la Administración sanitaria encuentra su fundamento en los arts. 85, 95, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento (LM).

El primero de ellos porque contempla los datos básicos de la receta, entre los que se incluyen la identificación del prescriptor, del paciente y del medicamento.

El art. 95 de la LM conforma la habilitación de las Administraciones Sanitarias al imponer a los usuarios la obligación de justificar su derecho a la prestación cuando le sea requerida por el personal facultativo del Sistema Nacional de Salud o en las farmacias dispensadoras. Tales previsiones se contemplan con las del art. 96 de la misma norma cuando atribuye a las Administraciones Públicas Sanitarias la evaluación de las prescripciones al disponer que el Ministerio de Sanidad y Consumo establezca las medias de control correspondientes.

El art. 98 de la LM, contempla la agregación de la información relacionada con las recetas, atribuyendo su gestión al Estado y a los Servicios de Salud autonómicos.

d)El art. 97 LM, que regula la colaboración farmacias- Sistema Nacional de Salud, destaca la calificación de las oficinas de farmacia como establecimiento sanitarios, el deber de colaboración que se les impone para garantizar el uso racional de los medicamentos y la posibilidad de ser objeto de concertación en cuestiones distintas a las obligaciones legales, que se les imponen.

Por su parte, la Ley 21/1974, de 13 de febrero, de Colegios Profesionales (LCP) configura a estas Corporaciones como de Derecho Público, y les atribuye la representación de la profesión y el ejercicio de las funciones que les sean encomendadas por la Administración. La LCP regula los Consejos Generales de los Colegios como Corporaciones de Derecho Público, con personalidad jurídica propia y plena capacidad.

Entre sus funciones incluye las de los propios colegios, en cuanto tengan ámbito o repercusión nacional (arts. 1 5 y 9 LCP).

Atendiendo a las normas citadas debe estimarse que las actuaciones que el Concierto exige de los Colegios Profesionales en las recetas, constituye un supuesto de cesión de datos entre administraciones públicas (art. 19 de la LORTAD). En efecto, el objeto del Concierto es la fijación de las condiciones en que las oficinas de farmacia deben colaborar profesionalmente con el INSALUD. A tal efecto contempla los términos y actuaciones necesarias para que el INSALUD abone a aquéllas las recetas y su mecanización exigiendo que ésta garantice, a favor del INSALUD, el conocimiento de los datos necesarios para el citado proceso de facturación y para la grabación de los datos necesarios en orden al correcto control de la prestación farmacéutica y limita la utilización de la información procedente de la mecanización en los términos ya expuestos.

d) La participación de empresas privada en la grabación de datos se encuentra amparada por el art. 27 de la LORTAD, que prevé la posibilidad de realizar el tratamiento de datos personales por cuenta de terceros siempre que cumplan las garantías de dicha norma y, en particular, la confidencialidad.

e)La Agencia de Protección de Datos tiene una especial sensibilidad en el tratamiento de datos especialmente protegidos, como son los relativos a la salud. Como manifestaciones concretas de dicha preocupación la Agencia iniciará a principios del próximo año actuaciones inspectoras sobre la ejecución del Convenio en relación al tratamiento de datos personales.

Así mismo velará para que continúen desarrollándose las actuaciones de colaboración con el INSALUD para el desarrollo posterior del Proyecto TAIR, a fin de que éste se adecue a las exigencias derivadas de la normativa de protección de datos.

2.6 PARTIDOS POLÍTICOS

Han sido muy escasas las denuncias recibidas en este sector. Entre ellas cabe destacar las dos siguientes:

* Escrito de reclamación recibido en la Agencia por el que el denunciante manifiesta haber recibido una convocatoria para asistir a una Conferencia Nacional convocada por un determinado partido político. El denunciante aseguró no haber estado nunca afiliado al citado partido.

Solicitada información al partido político, éste respondió que los datos de militantes y simpatizantes los obtienen a partir de las solicitudes de inscripción como tales. Asimismo, informa que los datos del denunciante no forman parte de su fichero y que han sido obtenidos a partir de la agenda personal de un militante. La invitación fue realizada por el carácter abierto y no partidista del evento.

Dado que los datos del denunciante fueron obtenidos a partir de la agenda personal de uno de los militantes del partido, no formando parte de los ficheros, no ha existido tratamiento automatizado de datos personales, no siendo de aplicación, en consecuencia, la Ley Orgánica 5/1992.

* Escrito de reclamación recibido en la Agencia en el que la denunciante manifiesta haber recibido en uno de sus domicilios particulares, en cuyo municipio no está empadronada, impresos de propaganda electoral de un determinado partido político. La denunciante manifiesta no haber estado nunca afiliada al citado partido.

Las actuaciones de investigación continúan en el año 2000.

2.7 SINDICATOS

Durante el año 1999 sólo se realizaron en este sector dos actuaciones de inspección en ambos casos a consecuencia de denuncias de los afectados.

En el primer caso se investigó la procedencia de los datos de los destinatarios de un envío por correo remitido por un Sindicato de Labradores con motivo de la celebración de un acto sindical, ya que se había recibido una denuncia de varias personas manifestando que no habían proporcionado sus datos personales a esta organización. Durante las actuaciones realizadas se comprobó que el Sindicato disponía de un fichero automatizado en el que recogía los datos personales de no afiliados asistentes a actos organizados por el Sindicato y que aquéllos habían facilitado para posteriores informaciones. No obstante, dado que no se acreditó contar con el consentimiento de los afectados para automatizar dichos datos, se inició procedimiento sancionador por infracción del artículo 6.1 de la Ley Orgánica 5/1992.

También hay que destacar en este sector la resolución del Director de la Agencia en un procedimiento sancionador incoado contra una empresa que había facilitado los datos personales de sus trabajadores a un Sindicato. Se sancionó a la empresa por infracción del artículo 11.1 de la Ley Orgánica 5/1992 al ceder datos de sus trabajadores sin contar con el consentimiento de los mismos y en el caso del sindicato por infracción del artículo 6.1 al automatizar dichos datos sin disponer así mismo del consentimiento.

Durante la tramitación de dicho procedimiento quedó acreditado que la empresa había facilitado al Sindicato los datos de nombre, apellidos, dirección y número de NIF del personal de dicha empresa. También que el Sindicato había utilizado dichos datos para remitir a través de una sociedad instrumental una carta ofreciendo sus servicios al domicilio particular de los empleados activos de la empresa, partícipes en un Plan de Pensiones promovido por esta entidad, así como a los trabajadores pasivos de la misma, realizando un tratamiento automatizado de dicha información.

El Director de la Agencia resolvió finalmente que se habían infringido los preceptos antes señalados. En el primer caso porque aunque la empresa hubiera facilitado al Sindicato los datos relativos a los trabajadores para el cumplimiento de sus funciones representativas (al amparo de lo establecido en las disposiciones legales vigentes, especialmente en el Estatuto de los Trabajadores y en el artículo 19 de los Convenios colectivos suscritos entre la empresa y la representación sindical de su personal asalariado), no se justificaba en concreto la cesión de los datos relativos a domicilio y NIF, por lo que en este caso debían haber solicitado el consentimiento de sus trabajadores. Así mismo, se había comprobado durante la fase de práctica de pruebas que en el Escalafón del Personal que la empresa entregaba a los sindicatos representados en el Comité de Empresa, no constaban los datos de domicilio y número de NIF. En el caso del Sindicato, el Director de la Agencia consideró por idéntica razón que era también necesario contar con el consentimiento de aquellos afectados que no estuvieran afiliados para la automatización de sus datos relativos al domicilio y número de NIF.

2.8. COLEGIOS PROFESIONALES

Del análisis de las actuaciones realizadas por la Agencia de Protección de Datos en este sector durante el año 1999, cabe destacar que la mayor parte de los escritos son relativos a denuncias relacionadas con los artículos 6 y 11 de la Ley Orgánica 5/1992, donde se regulan el consentimiento del afectado y la cesión de datos, respectivamente.

Durante este año se han recibido en la Agencia de Protección de Datos nueve escritos donde se pone de manifiesto la posible utilización irregular de los datos de profesionales colegiados y la comunicación o cesión de datos a Colegios, Consejos de Colegios Profesionales y a otras entidades. Agrupando las reclamaciones por sectores, se observa que la mayor parte se han referido al sector médico, con la apertura de tres procedimientos sancionadores. Dos denuncias se refieren a los Colegios de Abogados de Madrid y de Vigo. Y la tercera de las reclamaciones concierne a los Consejos de Colegios Profesionales.

Respecto a la tipología de las reclamaciones formuladas cabe destacar que la mayor parte de ellas denuncian la cesión de datos de los Colegios Profesionales a sus respectivos Consejos. Sin embargo, la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, en su artículo 9 dice que: *"Los Consejos Generales de los Colegios tiene a todos los efectos la condición de Corporación de Derecho público, con personalidad jurídica propia y plena capacidad",* lo que unido a la interdependencia existente entre ambos tipos de instituciones según los distintos Estatutos, justifica la relación jurídica existente entre ellos y por tanto la comunicación de datos. Algunas denuncias se refieren a la cesión de ciertos datos en particular, como sucedía en el caso del Consejo Superior del Colegio de Ingenieros de Minas que recababa datos de los cónyuges de los colegiados. En este caso, se procedió a su archivo ya que el dato "nombre del cónyuge" era de carácter voluntario y fue incorporado al fichero de la institución por ser necesario su conocimiento a la hora de tramitar las prestaciones de viudedad.

Entre las actuaciones practicadas por la Agencia en este sector de actividad merece destacar el caso concreto del Ilustre Colegio de Abogados de Madrid, el cual posee un fichero automatizado con datos de carácter personal obtenidos de procedimientos judiciales en los que han intervenido sus colegiados y que están siendo utilizados por el Colegio para reclamar derechos de intervención profesional a aquellos. Efectivamente, el Servicio de Comprobación del citado Colegio se encarga de verificar si sus colegiados cumplen con las obligaciones dinerarias en relación con el pago de los derechos de intervención profesional y de las cuotas. Para ello accede a los Libros-Registro de los órganos judiciales y a los Poderes otorgados en cada procedimiento. Este personal designado por el Ilustre Colegio de Abogados de Madrid está autorizado por la Audiencia Provincial y el Tribunal Superior de Justicia de Madrid, así como por el Tribunal Supremo. La reforma a la ley 5/1985 de 1 de julio, Ley Orgánica del Poder Judicial realizada por la Ley 16/1994 de 8 de noviembre, en su articulo 230.1 dice textualmente. *"Los Juzgados y tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos para el desarrollo de su actividad y ejercicio de sus funciones con las limitaciones que a la utilización de tales medios establece la Ley Orgánica 5/1992 de 29 de octubre y demás leyes que resulten de aplicación".* De este modo la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal se convierte en el punto de referencia de los niveles de protección de que han de gozar los ficheros jurisdiccionales.

El art. 230.5 reformado de la LOPJ precisa que: "Reglamentariamente se determinarán por el Consejo General del Poder Judicial los requisitos y demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos judiciales de forma que se asegure el cumplimiento de las garantías y derechos establecidos en la Ley Orgánica 5/1992". El desarrollo reglamentario de esta norma se ha llevado a cabo por el Reglamento 5/1995, de 7 de junio, sobre Aspectos Accesorios de las Actuaciones Judiciales.

La LOPJ parte, pues, de la aplicación plena de la LORTAD pero se remite a la citada disposición reglamentaria en cuanto a la regulación de los ficheros automatizados que se encuentren bajo la responsabilidad de los órganos jurisdiccionales. En este sentido, el art. 82 del citado Reglamento 5/1995 señala como responsable del fichero al Secretario del Juzgado o Tribunal correspondiente, añadiendo el art. 84 que los derechos de acceso, rectificación y cancelación podrán ejercerse por el afectado en la sede del órgano judicial o gubernativo titular del fichero y ante el responsable del mismo.

Por su parte, el art. 85 dispone que "Contra las resoluciones expresas o presuntas del responsable del fichero denegatorias del acceso, rectificación o cancelación que se haya solicitado, el afectado podrá interponer los recursos previstos en el art. 4.3 de este Reglamento", artículo que prevé la posibilidad de que el acuerdo denegatorio del Secretario judicial sea revisable por el Juez o Presidente a petición del interesado. Y finalmente, contra el acuerdo del órgano jurisdiccional se podrán interponer los recursos establecidos en el Reglamento 4/1995, de 7 de junio, de órganos de Gobierno de los Tribunales, todo ello como paso previo a la vía contencioso-administrativa.

En consecuencia, habiéndose residenciado reglamentariamente y en virtud de mandato legal en el Consejo General del Poder Judicial la competencia sobre la materia, atribuyéndose aquélla a la autoridad judicial y a sus órganos de gobierno, es por lo que tratándose de ficheros jurisdiccionales que contengan datos personales, toda información requerida por tercero deberá contar con el consentimiento del afectado o, en su caso, ser autorizado por el titular del órgano jurisdiccional, correspondiendo a éste velar por la defensa de los derechos reconocidos en el art. 18.4 de la Constitución y en la Ley Orgánica 5/1992.

En el presente caso ha quedado acreditado, conforme a lo expuesto en los Antecedentes de Hecho, que el Servicio de Comprobación del Colegio de Abogados de Madrid ha recabado datos que se introducen y almacenan en el fichero denominado ICAM, los cuales se obtienen del acceso a los Libro-Registro de los órganos judiciales y a los Poderes otorgados en cada procedimiento, tanto se constan en soporte papel como si lo están en soporte automatizado.

El citado acceso ha sido autorizado por la Sala de Gobierno del Tribunal Supremo, el Tribunal Superior de Justicia de Madrid y la Audiencia Provincial.

Por tanto, el pronunciamiento de la Agencia de Protección de Datos sobre la adecuación o no a la LORTAD del fichero denominado ICAM exige, inexcusablemente y con carácter previo, una decisión sobre la licitud del acceso autorizado por los propios órganos jurisdiccionales, ya que, de ser éste legítimo y conforme con la citada Ley Orgánica, el tratamiento posterior de los datos en aquel fichero no infringiría la normativa de protección de datos.

Sin embargo, de conformidad con las disposiciones citadas en los Fundamentos de Derecho anteriores, la decisión sobre la licitud y alcance de los accesos autorizados corresponde a la autoridad judicial y a sus órganos de gobierno, y, en su caso, a la jurisdicción contencionso-administrativa.

En virtud de todo ello, se acuerda el archivo de las actuaciones.

Por otra parte, es interesante destacar también el gran número de denuncias de profesionales que integran algunas organizaciones colegiales y que en el fondo están relacionadas con la obligatoriedad de la colegiación. Según la Ley 2/1974, de Colegios Profesionales, para ejercer algunas de estas profesiones es obligatoria la colegiación. Este es el caso del sector médico donde se han recibido varios escritos generalmente denunciando la comunicación de datos de los colegiados médicos a otras entidades con finalidad publicitaria, así como a otras instituciones públicas o privadas.

Durante el año 1999 se presentaron ante esta Agencia de Protección de Datos cinco reclamaciones consistentes en la denegación del derecho de cancelación por distintos Colegios y Consejos Profesionales, ante las cuales se procedió a incoar las consiguientes Tutelas de Derecho por parte de la Agencia. De ellas, tres fueron estimadas procediéndose a la cancelación solicitada por los denunciantes. Las otras dos tutelas, referidas a la colegiación en los Colegios de Médicos y Consejo General de Colegios de Médicos, fueron desestimadas ya que según sus Estatutos es obligatoria la colegiación para el ejercicio de la profesión y no se puede proceder a la cancelación cuando los datos son necesarios para el mantenimiento de la relación colegial, a tenor de lo dispuesto en el artículo 6 de la LORTAD.

Dentro de este sector, lo más destacable corresponde a tres resoluciones dictadas por el Director de la Agencia de Protección de Datos en 1999, que se exponen a continuación.

La primera proviene de un escrito de denuncia en la que se manifiesta que el Colegio Oficial de Médicos de A Coruña suscribió un contrato con una entidad bancaria donde ponía a disposición de esta entidad los datos personales de sus colegiados, los cónyuges y el personal contratado por el Colegio, para la oferta de un Plan de Pensiones. Así mismo, y a pesar de haber solicitado el afectado la cancelación de sus datos ante dicho Colegio, siguió recibiendo publicidad en su domicilio particular.

En la resolución firmada por el Director en septiembre de 1999, queda acreditada la cesión de datos por parte del Colegio Oficial de Médicos de A Coruña a la entidad bancaria sin que conste el consentimiento de los afectados y sin que los datos provengan de fuentes de acceso público, con lo cual ha infringido lo dispuesto en el articulo 11 de la Ley Orgánica 5/1992.

Respecto a otra denuncia, el Colegio alega en su descargo que efectuó una consulta el 29 de mayo de 1997 sobre "si un colegiado tenía derecho a prohibir al Colegio la remisión de información y circulares, y la cesión de sus datos", consulta que fue contestada por la Agencia el 15 de julio de 1997 en el sentido de que no puede prohibirse al Colegio la remisión de circulares, publicaciones o la cesión de los datos de un determinado colegiado, toda vez que son elementos imprescindibles para tratar de asegurar el ejercicio profesional de sus colegiados. Ahora bien, la contestación que la Agencia de Protección de Datos dio al Colegio se centraba en que las publicaciones remitidas a los colegiados deberían ser *publicaciones propias o relativas a la profesión que se ejerce o de datos que se ceden con el mismo fin, con eliminación de los superfluos o no necesarios.* Por tanto, la remisión de publicidad de un plan de pensiones poco o nada tienen que ver con su profesión, y por ello ha infringido lo dispuesto en el artículo 6 de la Ley Orgánica 5/1992. En el mismo sentido, la entidad bancaria ha infringido este mismo artículo sobre "tratamiento de datos sin consentimiento de los afectados".

La segunda resolución dictada en 1999, tiene igualmente que ver con los artículos 6 y 11 de la Ley Orgánica 5/1992. Los afectados, dos en esta reclamación, denuncian la cesión de sus datos personales contenidos en los ficheros automatizados del Consejo General de Colegios de Médicos a una entidad bancaria con el fin de realizar una campaña publicitaria de ámbito nacional respecto a préstamos hipotecarios para la adquisición de viviendas y planes de

pensiones para ese colectivo. De manera similar al caso anteriormente expuesto, la Agencia de Protección de Datos, después de quedar acreditada la cesión en un disquete de 158.000 datos personales de médicos facilitados por el Consejo, considera que se ha cometido una infracción al artículo 11 de la LORTAD. Igualmente, la entidad financiera ha cometido una infracción al artículo 6.

De esta resolución cabe resaltar la valoración realizada por la Agencia a la alegación presentada por el Consejo sobre el hecho de considerar los datos de sus colegiados como obtenidos de *fuentes de acceso público,* según el artículo 1.3 del Real Decreto 1332/1994 de 20 de junio, donde se expone que las fuentes de acceso público han de definirse como *los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.* Sin embargo, en el caso que nos ocupa, los datos personales estaban contenidos en un disquete y esos datos provenían directamente de sus ficheros automatizados. Los ficheros automatizados propiedad del Consejo General no constituyen fuentes accesibles al público y los datos contenidos en dichos ficheros sólo se convierten en fuente de acceso público cuando son publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo, siendo entonces cuando se pueden incorporar a ficheros automatizados de terceros que recaban los datos directamente de esos listados.

La tercera resolución del Director de la Agencia se refiere a un procedimiento sancionador abierto y resuelto durante 1999 al mismo Consejo General de Colegios, el cual procedió a realizar la rectificación de datos de un colegiado, relativos al número de teléfono, estado civil e identidad del cónyuge. Sin embargo, posteriormente y dejando sin efecto la petición del afectado de que no fueran tratados automatizadamente esos determinados datos, el Consejo vuelve a dar de alta en sus ficheros los citados datos realizando de nuevo un tratamiento, vulnerando con ello el principio del consentimiento consagrado en el artículo 6 de la ley Orgánica 5/1992.

2.9 FICHEROS DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO.

Como en años anteriores, la actividad de la Agencia de Protección de Datos durante 1999 en relación con los ficheros cuya finalidad es la prestación de servicios de información sobre la solvencia patrimonial y el crédito ha sido especialmente intensa, dado que el tratamiento de este tipo de información influye en las relaciones entre los usuarios de servicios y productos financieros y las entidades que prestan éstos últimos, y por tanto es causa de particular preocupación entre los usuarios.

A lo largo de este epígrafe se tratarán en primer lugar las actuaciones de la Agencia motivadas por reclamaciones y denuncias de los ciudadanos. En segundo lugar, se tratarán las Recomendaciones elaboradas por el Director de la Agencia dirigidas a las empresas responsables de ficheros dedicados a la prestación de servicios de información sobre solvencia patrimonial y crédito. Estas recomendaciones culminan el proyecto iniciado en el año 1998 y recogido en la Memoria de ese año, que consistió en la realización y ejecución de un Plan de Inspección de oficio a ficheros regulados por el artículo 28 de Ley Orgánica 5/1992, y que ha finalizado en 1999.

Por último, se expondrán los aspectos más importantes de las resoluciones de especial relevancia dictadas a lo largo del año 1999 por el Director de la Agencia en relación a estos ficheros de solvencia patrimonial y crédito.

2.9.1. Actuaciones motivadas por reclamaciones y denuncias de los ciudadanos

Siguiendo la tendencia de años anteriores, durante el año 1999 los ficheros dedicados a la prestación de servicios de información sobre solvencia patrimonial y crédito han originado un elevado número de reclamaciones de tutela de derechos y de denuncias de posibles infracciones a la Ley Orgánica 5/1992. Del total de reclamaciones y denuncias recibidas relacionadas con este sector, el 97% hacen referencia a los cuatro ficheros de información sobre solvencia patrimonial y crédito más significativos.

De las 292 actuaciones iniciadas por la Subdirección General de Inspección de Datos de la Agencia durante el año 1999, 79 de ellas se realizaron sobre ficheros regulados por el artículo 28 de la Ley Orgánica 5/1992, relativo a ficheros dedicados a información sobre solvencia patrimonial y crédito.

En cuanto a las Tutelas de Derecho, de las 195 resueltas en 1999, se tramitaron 23 sobre derechos de acceso, rectificación y cancelación a ficheros de solvencia patrimonial y crédito. De estas últimas, el 13% tutelaron derechos de acceso, mientras que el 87% restante tutelaron derechos de cancelación.

Y de los 110 procedimientos sancionadores que en 1999 fueron concluidos, 14 de ellos supusieron la imposición de sanciones a empresas responsables de ficheros de información sobre solvencia patrimonial y crédito. Las principales infracciones sancionadas fueron:

a) Falta de notificación a los afectados respecto de los que se han registrado datos personales en este tipo de ficheros, en los términos establecidos por el punto 1 del artículo 28 de la Ley Orgánica 5/1992.
b) La conculcación del principio de calidad de datos establecido en el artículo 4 de dicha Ley.
c) La vulneración del principio de consentimiento del afectado en el tratamiento automatizado de sus datos personales, regulado por el artículo 6 de la misma.

d) La cesión no legítima de datos entre entidades cedente y cesionaria, conculcando los principios establecidos en el artículo 11 de la susodicha Ley.

En resumen, cabe señalar que el gran volumen de actuaciones desarrolladas por la Agencia y en particular por la Subdirección General de Inspección de Datos en relación a los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito, sigue la tendencia de años anteriores. Pero también resulta necesario destacar, a la vista de un examen detallado de las cifras en relación con las de años pasados, que el número de procedimientos sancionadores que han dado como resultado la imposición de sanciones a empresas del sector sigue la tendencia descendente que se venía observando en 1998, lo cual puede explicarse como un resultado lógico de las acciones preventivas y correctivas que la Agencia ha venido desarrollando en los últimos años, y que han dado como resultado un mejor funcionamiento y adecuación de estos ficheros a lo establecido por la LORTAD.

2.9.2. Recomendaciones de la Agencia de Protección de Datos a las empresas responsables de ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.

A lo largo del año 1998, la Agencia de Protección de Datos llevó a cabo un Plan de Inspección de oficio sobre este tipo de ficheros. El alcance, criterios de inspección, objetivos y resultados de la ejecución del plan de inspección fueron descritos en la Memoria de la Agencia correspondiente a dicho año.

En 1999, como colofón a las actuaciones derivadas del Plan de Inspección, y en la línea de trabajo habitual en relación a este tipo de actuaciones, el Director de la Agencia dictó una serie de recomendaciones dirigidas a las empresas del sector responsables de ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.

El objetivo fundamental de las recomendaciones, que se incluyen al final de este apartado, era conseguir una mejor adecuación del funcionamiento de este tipo de ficheros a lo establecido en el art. 28 de la Ley Orgánica 5/1992, así como a lo dispuesto en la Instrucción 1/1995 de la Agencia de Protección de Datos.

Las recomendaciones, tal y como apreciará el lector, se desarrollan en tres grupos. Los dos primeros grupos hacen referencia respectivamente a los dos grandes tipos de ficheros dedicados a la prestación de servicios sobre solvencia patrimonial y crédito. Así, el primer grupo de recomendaciones está dedicado a los ficheros que tratan datos relativos al incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúa por su cuenta e interés, mientras que el segundo grupo de recomendaciones afecta a aquellos ficheros que tratan datos obtenidos de fuentes accesibles al público. Finalmente, en el tercer grupo de recomendaciones se incluyen aquellas relativas al Reglamento de Medidas de Seguridad (Real Decreto 994/1999, de 11 de junio). A continuación, se incluye el texto íntegro de las mismas.

RECOMENDACIONES DE LA AGENCIA DE PROTECCIÓN DE DATOS A LAS EMPRESAS DEL SECTOR RESPONSABLES DE FICHEROS DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO PARA LA ADECUACIÓN DE SU FUNCIONAMIENTO A LA LEY ORGÁNICA 5/1992.

I. INTRODUCCIÓN

Como consta en la Memoria de 1998, desde sus albores la Agencia de Protección de Datos ha mantenido una constante preocupación por el funcionamiento de los ficheros sobre solvencia patrimonial y crédito derivada de la repercusión social y económica que para el ciudadano puede generar un uso indebido de los datos de carácter personal que son tratados en estos ficheros.

En un primer momento, la Agencia concentró su línea de actuación en la ineludible obligación de atender las reclamaciones y denuncias presentadas por los afectados. Atendida esta prioridad y sus lógicas derivaciones de iniciar concretas actuaciones de inspección y, en su caso, los procedimientos sancionadores correspondientes a determinadas empresas del sector, se evidenció la necesidad de continuar con una línea de actuación más ambiciosa que abarcase si no a todo el sector, sí a las empresas más significativas del mismo, con el fin de obtener una visión global del funcionamiento y operatividad de aquéllas que permitiese a esta Agencia dictar las oportunas instrucciones o recomendaciones para una mejor adecuación de su funcionamiento a las prescripciones de la LORTAD.

Con este objetivo se instrumentó un Plan de Inspección de Oficio, iniciado en el año 1998 y concluido en el presente año 1999, sobre los ficheros a los que hace referencia el art. 28 de la LORTAD, cuya repercusión en la actividad de la Agencia de Protección de Datos (aproximadamente el 40% de las actuaciones de inspección de la Agencia se desarrollan sobre ficheros de esta naturaleza) obliga a conocer en profundidad y de un modo actualizado los tratamientos efectuados sobre los mismos, así como su grado de cumplimiento de la normativa vigente.

II. FICHEROS A INSPECCIONAR

El Plan de Inspección de Oficio comprende los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito negativos a los que se refiere el art. 28 de la Ley 5/1992, de 29 de octubre.

Este artículo se refiere a dos tipos de ficheros claramente diferenciados: a) los que tratan información relevante para la información de la solvencia patrimonial, obtenida de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, y b) los ficheros que tratan datos sobre el cumplimiento o incumplimiento de obligaciones dinerarias, usualmente denominados "ficheros de morosos".

De ellos, las actuaciones inspectoras de la Agencia de Protección de Datos se han centrado en los ficheros en los que el tratamiento de datos de personas físicas suponen un porcentaje importante de la información almacenada, tanto si la información relativa a la solvencia patrimonial o al incumplimiento de obligaciones dinerarias se obtienen de fuentes accesibles al público, como si han sido facilitados por el acreedor.

III. CRITERIOS DE SELECCIÓN DE FICHEROS A INSPECCIONAR

Si bien el sector económico dedicado a la prestación de servicios de información sobre solvencia patrimonial y crédito está sufriendo en los últimos tiempos un fenómeno de concentración que permite optimizar los servicios que ofrecen, el total de ficheros inscritos en el Registro General de Protección de Datos de la Agencia en los que conste como alguna de sus finalidades la evaluación de solvencia patrimonial es aún y con todo elevado: aproximadamente 3.000, aunque la mayoría de éstos se circunscriben a datos de sus propios clientes que no se incorporan a ficheros comunes. Por ello la actuación inspectora se ha ceñido a los operadores de ficheros comunes que tratan un volumen masivo de información. Los criterios de selección han sido los siguientes:

Volumen de la información registrada en el fichero

Entidades que suministran y acceden a la información del fichero, evaluando la repercusión sobre los afectados

Denuncias recibidas en la Agencia de Protección de Datos

IV. COMPROBACIÓN DEL CUMPLIMIENTO DE LA NORMATIVA VIGENTE: ASPECTOS SOBRE LOS QUE HA INCIDIDO LA INSPECCIÓN

El Plan de Inspección ha tenido por objeto, en primer lugar, poner de manifiesto aquellas deficiencias que se han constatado en el funcionamiento del sector en los aspectos analizados y, en segundo lugar, y sin que ello signifique soslayar la potestad sancionadora de la Agencia de Protección de Datos en aquellos casos en los que se constate una infracción de la Ley, formular las recomendaciones que, a juicio de la Agencia, redundarían en una mejor garantía de los derechos de los ciudadanos en lo que a la defensa de su privacidad se refiere.

Como resultado del desarrollo de las inspecciones realizadas, se ha constatado que si bien se ha producido una continuada mejoría en el funcionamiento de los ficheros de esta naturaleza y un mayor cumplimiento de las disposiciones de la LORTAD, aún se han encontrado deficiencias en la operativa de tales ficheros que una vez subsanadas supondrían una mejora indudable en el acatamiento de la Ley.

Con este objeto se dictan las presentes RECOMENDACIONES al amparo de las potestades que a esta Agencia atribuye el artículo 36 a) de su Ley Reguladora.

PRIMERA: RECOMENDACIONES PARA FICHEROS QUE TRATAN DATOS RELATIVOS AL INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS FACILITADOS POR EL ACREEDOR

1.-El apartado tercero de la Norma Segunda de la Instrucción 1/1995 de la Agencia de Protección de Datos establece que *"La inscripción en el fichero de la obligación incumplida se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan señalando, en esta caso, la fecha de cada uno de ellos".*

Por lo tanto, en cumplimiento de dicha Norma se deberá realizar una anotación por cada operación impagada. En cada anotación aparecerá claramente diferenciada la parte correspondiente al principal de la deuda y a los intereses devengados.

2.-Se ha constatado que en algunos ficheros, en el caso de sociedades, se incluyen datos de los administradores y otros cargos ejecutivos de la sociedad. En estos casos se recomienda que cuando se incluyan datos de administradores o cargos ejecutivos de una sociedad que haya incumplido una obligación de pago, se haga constar claramente si a dichos cargos les son exigibles o no las deudas de la sociedad (avales, obligaciones solidarias, etc.), ya que de no serlo no deberían figurar en el fichero.

3.-En algunos casos se imputan erróneamente datos de un afectado a otro diferente (v. gr.: padre e hijo o personas con apellidos iguales y que son muy comunes), debido a que los datos disponibles para la identificación de los afectados impide que ésta se realice de un modo inequívoco.

Para evitar esta imputación errónea no se deberán registrar incidencias relativas a personas que no puedan identificarse de forma inequívoca.

4.-Conforme a las prescripciones legales, las entidades que facilitan la información tienen la obligación de efectuar las rectificaciones y cancelaciones de las que tengan conocimiento. Sin embargo, se ha comprobado que estas entidades normalmente las comunican al fichero en un plazo superior a la semana, que es el previsto en el apartado cuarto de la Norma Primera de la Instrucción 1/1995.

Al objeto de cumplir la mencionada Norma, se adoptarán todas aquellas medidas de índole técnica y organizativa que garanticen que las actualizaciones de los datos de los que tienen conocimiento las entidades informantes se reflejen en

el fichero común en el plazo de una semana, que es el previsto por la Instrucción 1/1995

5.-En aquellos casos en los que se distribuyen copias de los datos registrados en el fichero común, el tratamiento posterior de dichos datos (actualización, normalización, etc.) provoca, en ocasiones, discrepancias entre la información registrada en el fichero común y en los ficheros copia.

En estos supuestos deberán cumplirse las siguientes recomendaciones:

a)Se deberá garantizar que todas las copias de los ficheros existentes en cada entidad informante sean idénticas. En el caso de que esto no se pueda garantizar, cada entidad informante deberá notificar al Registro General de Protección de Datos la copia del fichero que obra en su poder, siendo responsable de la información contenida en el mismo a todos los efectos.

b)Se deberán habilitar los procedimientos necesarios para garantizar que a los afectados se les informa de forma cabal y actualizada de todos los destinatarios de la información contenida en el fichero de conformidad con lo establecido en el art. 13 del R.D. 1332/1994, de 20 de junio.

c)Se tomarán todas aquellas medidas que impidan la existencia de copias de dichos ficheros en manos de personas físicas o jurídicas no autorizadas a acceder a las mismas o, al menos, aquellas medidas que permitan identificar el origen exacto de la copia que se esté utilizando de manera ilegítima (incluyendo, por ejemplo, marcas diferenciadas en cada una de las copias).

6.-De conformidad con lo dispuesto en el art. 28.2 de la LORTAD, se habilitarán aquellas medidas técnicas y/o organizativas que resulten necesarias para garantizar el derecho de los afectados a conocer las evaluaciones que sobre ellos se hayan realizado en los últimos seis meses.

7.-Se ha comprobado que existen entidades informantes que no otorgan los derechos de acceso, rectificación y cancelación en los términos dispuestos en el apartado tercero de la Norma Cuarta de la Instrucción 1/1998 de la Agencia de Protección de Datos. En particular, se ha comprobado que no se facilitan ni los datos que obran en el fichero común del afectado que solicita el ejercicio del derecho de acceso ni la identidad del responsable del fichero o ficheros comunes que se consultan habitualmente por la entidad informante.

Para evitar estas circunstancias limitativas de los derechos de los afectados se tomarán las medidas necesarias para que cuando los mismos soliciten el ejercicio del derecho de acceso ante una entidad informante, se les comuniquen los datos referidos a ellos que obran en el fichero común a los que la entidad tenga acceso, así como la identidad y dirección del responsable del fichero común para que el afectado pueda, de esa manera, dirigirse al responsable de dicho fichero común y completar así el ejercicio de los derechos que la Ley le reconoce.

8.-Se han detectado casos de permanencia en el fichero común de deudas con una antigüedad superior a los seis años establecidos legalmente.

Al objeto de dar cumplimiento a la prescripción legal se deberán implantar los procedimientos adecuados para garantizar que el periodo de permanencia de los datos en los ficheros comunes no supere el citado límite.

9.-En relación con las notificaciones exigidas legalmente, si como consecuencia del ejercicio del derecho de cancelación se procediera a la baja cautelar de datos de un afectado en el fichero común, la ulterior incorporación al fichero de los datos cancelados requerirá una nueva notificación en el plazo de treinta días.

SEGUNDA:RECOMENDACIONES PARA FICHEROS QUE TRATAN DATOS DE FUENTES ACCESIBLES AL PÚBLICO

Estos ficheros, además de serles de aplicación las recomendaciones señaladas en los números 5 a) y b), 6 y 8 de la recomendación Primera, deberán también ajustar su actuación a las siguientes:

1.- Habiéndose constatado que en ocasiones estos ficheros no reflejan la información debidamente actualizada, se deberán adoptar las medidas necesarias para garantizar que la información que aparece en los mismos se refleje de forma exacta y actualizada a fin de garantizar el principio de calidad de datos, así como los derechos de acceso, rectificación y cancelación.

2.-No podrán consignarse en el fichero datos que permitan confundir el importe de la deuda con los publicados en la fuente accesible al público, tales como el tipo de subasta.

3.-Tampoco podrán consignarse los datos referidos a personas físicas que no sean deudores reales, tales como cotitulares, administradores no responsables o personas no identificadas inequívocamente.

TERCERA:RECOMENDACIONES SOBRE EL REGLAMENTO DE MEDIDAS DE SEGURIDAD

Habiéndose publicado con posterioridad al término de las actuaciones inspectoras el Real Decreto 994/1999, de 11 de junio, resulta conveniente recordar las exigencias del mismo y, particularmente:

Que los sistemas de información que no se encontraran en funcionamiento a la entrada en vigor de la norma citada, deberán cumplir las medidas de seguridad correspondientes desde que se produzca su puesta en funcionamiento.

Que la aplicación del plazo de implantación de las medidas de seguridad de nivel medio no excluye el cumplimiento del plazo más breve previsto para la aplicación de las de nivel básico.

2.8.3. **Resoluciones del Director de la Agencia de Protección de Datos de especial relevancia.**

Entre las resoluciones dictadas a lo largo del año 1999 por el Director de la Agencia de Protección de Datos relativas a los ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, cabe destacar la resolución R/00110/1999, relativa a la inclusión de datos de carácter personal en un fichero dedicado a la prestación de servicios de información sobre solvencia patrimonial y crédito que no proceden de las únicas fuentes habilitadas por el citado artículo 28, esto es: fuentes accesibles al público, informaciones facilitadas por el afectado o con su consentimiento, o información relativa al cumplimiento o incumplimiento de obligaciones dinerarias facilitada por el acreedor o por quien actúe por su cuenta e interés.

En la resolución citada se sancionan actuaciones constitutivas de infracción llevadas a cabo por dos entidades responsables de ficheros dedicados a la prestación de servicios de información sobre solvencia patrimonial y crédito de personas físicas, al quedar establecido que los datos personales recogidos el fichero de una de las entidades eran obtenidos de Boletines Oficiales, Registros y Juzgados de Madrid y Barcelona. Una de las fuentes de los datos obtenidos en los Juzgados citados consistía en los tablones de anuncio existentes en aquéllos. Ambas entidades. suscribieron un contrato mediante el cual se suministrarían mutuamente información procedente de sus ficheros sobre solvencia patrimonial obtenida de fuentes accesibles al público y de acreedores o de quienes actúen por su cuenta e interés, debiendo ser dicha información legitimada por ambas entidades. En las actuaciones practicadas quedó acreditado que una de las entidades suministraba información procedente de los tablones de anuncios para ser incorporados en el fichero de la segunda entidad..

En la Resolución se concluye que *los datos publicados en los tablones de anuncios de los juzgados no son fuentes accesibles al público*, en el sentido definido en Real Decreto 1332/1994. En éste se establece que son fuentes accesibles al público aquellos datos que se encuentran a disposición del público en general, *no impedida por cualquier norma limitativa*. Así, de conformidad con lo previsto en artículo 235 de la Ley Orgánica 6/1985 de 1 de julio del Poder Judicial, se reconoce a los interesados el derecho de acceso a los libros, archivos y registros judiciales, requiriendo por tanto la publicidad procesal, por parte de quien la invoca y ejercita, que concurra en él la condición de interesado. Por ello, establece la resolución que "*debe entenderse que existe una norma limitativa al tratamiento automatizado de dichos datos para que cualquiera que no sea el interesado, pueda tratar los datos recogidos en dichos tablones y cederlos posteriormente...*" .

En definitiva y como conclusión se establece que, la información contenida en los tablones de anuncios de los juzgados, aún siendo accesible a cualquiera que los consulte, tiene por finalidad la de practicar la notificación a los interesados litigantes, siendo la utilización de dichos datos, *y en particular la compilación de los mismos*, contraria a la finalidad para la que se publicó, requiriendo por tanto su tratamiento por terceros *el consentimiento previo del interesado* al que se puedan referir los datos personales reflejados en la publicidad procesal exhibida en los tablones.

2.10 PUBLICIDAD Y MARKETING DIRECTO

Al igual que en años anteriores, el envío postal de publicidad y el marketing directo han sido una de las actividades comerciales que más denuncias ante la Agencia ha ocasionado. En la mayor parte de los casos continúa denunciándose la obtención de datos no ajustada a lo que establece el artículo 29 de la Ley Orgánica 5/1992.

Considerando el número de Procedimientos Sancionadores que han finalizado en 1999 con una resolución sancionadora, se observa que en torno al 22% de ellos versaban sobre actividades relacionadas con el envío postal de publicidad, siendo reseñable que de las resoluciones que se sanciona con una falta muy grave, la tercera parte de ellas se refieren a hechos relacionados con este tipo de actividad.

De éstas últimas, cabe destacar dos sanciones impuestas a un particular, quien en su propio nombre había facilitado los datos personales utilizados para distintas campañas promocionales de terceros, habiendo declarado durante la tramitación de los respectivos Procedimientos que los datos procedían "*de restos de otros ficheros históricos (...) cuya procedencia no es posible especificar en la actualidad*" y no habiéndose acreditado que pudieran haber sido obtenidos de una fuente accesible al público.

Otra de las sanciones por falta muy grave, a raíz de una denuncia presentada ante la Agencia por el Defensor del Menor de la Comunidad de Madrid, recayó sobre una empresa cuya actividad se centraba en la venta de videojuegos y películas clasificadas X. Durante la tramitación del Procedimiento quedó acreditado que una segunda compañía, cuya actividad principal es la venta por catálogo y la exportación e importación de productos audiovisuales para mayores de 18 años, había remitido por correo un catálogo de contenido pornográfico a unas 8.000 personas, cuyos datos se habían obtenido de la primera empresa, no constando que se solicitara el consentimiento de los afectados (en particular, de dos menores) ni para la cesión ni para el tratamiento automatizado de sus datos personales.

Por último, es destacable también la sanción impuesta a la sociedad propietaria de un establecimiento hotelero del País Vasco, al haber incorporado a su fichero automatizado datos relativos a la supuesta ideología política de unas 300 personas con cierta relevancia social, a las que se remitió por correo la invitación para asistir a una fiesta de fin de año. Durante la tramitación del Procedimiento no se obtuvo constancia de que la pertenencia política figurase en ninguna de las fuentes que la sancionada identificó como origen de los citados datos, no habiéndose acreditado tampoco que exis-

tiese el consentimiento expreso y por escrito del afectado para tratarlos automatizadamente.

Respecto de las sanciones por falta grave, merece destacarse la impuesta a la sociedad propietaria de una sala madrileña organizadora de eventos musicales, al haber tratado automatizadamente los datos de una persona que años atrás había expresado su voluntad de no recibir más envíos publicitarios. Durante la tramitación del Procedimiento se puso de manifiesto que al sustituir el sistema informático de la compañía, debido a la existencia de un error en el equipo existente, se había procedido a cargar una antigua copia de seguridad del fichero de clientes, en la cual se hallaban los datos del denunciante tal y como figuraban antes de la cancelación.

2.11 RECLAMACIONES EN EL CAMPO DEL SECTOR INFORMÁTICO DE SUMINISTRADORES DE SOFTWARE

Durante el mes de marzo de 1999 se recibieron en la Agencia diversos escritos de ciudadanos que mostraban su preocupación por dos hechos, de los que se había hecho eco la prensa internacional, que ponían en duda el respeto a la privacidad que debieran guardar los productos distribuidos por una compañía norteamericana de distribución de software.

Estos hechos eran los siguientes:

- El programa "*Asistente de Registro Online*" contenido en un sistema operativo, remitía a la compañía distribuidora del mismo, a través de una conexión telemática, información relativa al hardware del usuario en el momento de registrar el citado producto, de forma inadvertida para el usuario y sin que éste pudiera decidir al respecto.

- Los documentos generados con el paquete ofimático de este producto incluyen de forma automática un código que permitiría identificar todos los documentos generados desde un mismo ordenador, lo que podría entrañar el riesgo de que fueran asignados a una determinada persona en el caso de que su identidad pudiese deducirse una vez identificada la máquina.

A raíz de estos escritos, la Secretaría General de la Agencia se dirigió a la filial en España de la citada compañía con objeto de solicitar aclaración al respecto, la cual fue remitida acompañando copia de la comunicación que la matriz norteamericana había hecho pública a través de su web. Con objeto de obtener una mayor claridad acerca de las circunstancias en que se producían los hechos, el Director de la Agencia ordenó la realización de las oportunas labores de inspección.

En relación con el primero de los hechos investigados:

- Según las declaraciones de la filial española, esta compañía no incorpora a sus propios ficheros (ubicados en España) información relativa al equipamiento físico informático de los clientes procedente de los ficheros residentes en Estados Unidos, no habiéndose obtenido evidencias de lo contrario durante la inspección realizada.

- Se constata a través de la página web de la matriz norteamericana que independientemente de la decisión del usuario, se habrían estado remitiendo a sus ficheros residentes en Estados Unidos datos relativos al ordenador de los usuarios, concretamente un código que se construye siguiendo un procedimiento estándar especificado por la organización internacional OSF (Open Software Foundation) que utiliza, entre otros parámetros, un código que identifica unívocamente el equipo desde el que se generan los documentos y que contendría precisamente el identificador de la tarjeta de red ubicada en el ordenador del usuario.

- Por otra parte, la filial española declaró que: 1) esta circunstancia ya no se produce en la nueva versión del producto; 2) se han suprimido de los ordenadores de la compañía americana todos los códigos previamente almacenados, y 3) la matriz norteamericana ya no almacena en sus ficheros los citados datos incluso en el caso de que sean remitidos por versiones no actualizadas del producto.

Respecto del segundo de los hechos:

- La Inspección comprobó que, efectivamente, los documentos generados con dicho paquete (con cualquiera de los programas que lo constituyen) contienen un código compuesto por cinco campos hexadecimales, el cual, según ha declarado la filial española a la Agencia, se construye siguiendo un procedimiento estándar especificado por la organización internacional OSF (Open Software Foundation) que, al igual que el código antes citado, utiliza, entre otros parámetros, un código que identifica unívocamente el equipo desde el que se generan los documentos y que contendría precisamente el identificador de la tarjeta de red ubicada en el ordenador del usuario.

- La entidad norteamericana había puesto a disposición de los usuarios a través de su Web en Internet una herramienta informática que, según se pudo comprobar, eliminaba el citado código de todos los documentos contenidos en un determinado directorio.

- Así mismo, dicha entidad había ofrecido a los usuarios por el mismo medio un "*parche*" que permitía modificar la funcionalidad del paquete ofimático con objeto de que los documentos generados ya no contuviesen el mencionado código.

- La matriz norteamericana admitió que existió la posibilidad de determinar la probable autoría de un documento (que en principio pudiera ser anónimo) construido con el referido producto, precisamente en aquellos casos en los que su autor se hubiera registrado como usuario en los ficheros de la compañía americana, dado que los dos códigos citados

contendrían un parámetro común que permitiría asociarlos entre sí. Sin embargo, la filial española declaró a la Agencia que esta posibilidad no se había materializado en ningún caso.

A partir de las conclusiones de la Inspección, el Director de la Agencia de Protección de Datos RESOLVIÓ:

PRIMERO: Declarar que, a partir de las actuaciones practicadas y de las manifestaciones realizadas por la filial española. se deduce que durante algunos meses ha podido existir un riesgo para la privacidad de los usuarios españoles que hubieran registrado algún producto en los ficheros de la compañía americana.

SEGUNDO: Tomar en consideración las medidas técnicas llevadas a cabo por la compañía norteamericana para corregir las deficiencias de seguridad observadas, que han sido comunicadas a la Agencia a través de la filial española, estimando que, en los términos en que han sido transmitidas, son adecuadas para subsanar las deficiencias detectadas.

TERCERO: Tomar en consideración las declaraciones realizadas por la filial española en las que manifiesta no haber hecho uso de la citada coincidencia entre identificadores, así como aquéllas otras en las que certifica que "*a través de los productos comercializados por la compañía española no se almacenan en los ficheros automatizados de ..... (en España o en cualquier otro país del mundo) datos relativos al hardware de sus clientes en España sin el consentimiento de éstos*".

CUARTO: Requerir a la compañía filial española, para que en el futuro adopte las medidas técnicas precisas para evitar que se produzcan hechos como los que han ocasionado las citadas actuaciones de investigación, así como a la matriz norteamericana, en lo que afecte a los productos de esta compañía que se comercialicen y sean distribuidos en España.

2.12 INVESTIGACIÓN DE OFICIO SOBRE DATOS OBTENIDOS A TRAVES DE PÁGINAS WEB EN TERCEROS PAÍSES.

Durante 1999 también se iniciaron actuaciones de investigación sobre un fichero inscrito por la anteriormente referida filial española de la también citada matriz norteamericana en el Registro General de Protección de Datos desde el día 5 de noviembre de 1998, denominado "*MARKETING ON-LINE II*", descrito como: "*Base de datos de marketing cuya información y datos es proporcionada on-line por los usuarios de productos .....*" y cuya finalidad declarada es: "*obtención de estadísticas diversas, histórico de relaciones comerciales, seguridad y control interno, prospecciones de mercado, encuestas de opinión, gestión de clientes, publicidad propia y publicidad para terceros*" .

A raíz de las inspecciones realizadas se puso de manifiesto que el fichero "*MARKETING ON-LINE II*" contiene datos relativos al nombre y apellidos, dirección postal y electrónica y perfil profesional de alrededor de 130.000 personas, en su mayoría residentes en España, que se habrían obtenido a partir de una base de datos ubicada en los locales de la matriz norteamericana, en la cual se registran voluntariamente personas residentes en cualquier parte del mundo, interesadas en recibir información de los productos de la compañía, a través de sus páginas web.

Al momento del cierre de esta Memoria se está tramitando en la Agencia un Procedimiento Sancionador con el que se pretende determinar la adecuación legal de este fichero a las prescripciones de la legislación española sobre protección de datos.

2.13 TRATAMIENTO DE DATOS PERSONALES EN LOS SERVICIOS DE TELECOMUNICACIONES: ACTUACIONES MÁS RELEVANTES DE LA AGENCIA DE PROTECCIÓN DE DATOS

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, ha sido traspuesta al ordenamiento jurídico español por Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Dicha Directiva se complementa en el sector de las telecomunicaciones por la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que ha sido incorporada al ordenamiento jurídico por la Ley 11/1998, de 24 de abril, General de Telecomunicaciones -LGT- (arts. 49 a 54) y el Título V del R.D. 1736/1998, de 31 de julio, por el que se aprueba el Reglamento de desarrollo del Título III de la LGT en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones.

Las actuaciones de la APD durante 1999 en el sector de las Telecomunicaciones se han desarrollado en un doble plano de actividad: De un lado, a través de los Planes Sectoriales de Inspección de Oficio y, de otro, atendiendo a las denuncias de los ciudadanos relacionados con el uso de datos personales de los abonados a los servicios de telecomunicaciones.

Las más significativas actuaciones de la APD en uno y otro orden de actividad han sido las siguientes:

2.13.1 Planes sectoriales de Inspección de Oficio en el sector de las telecomunicaciones

En el ámbito de los Planes Sectoriales de Inspección de Oficio realizados durante el año 1999 en el sector de las tele-

comunicaciones, la APD ha llevado a cabo una intensa actividad a raíz de la publicación en el B.O.E. del Real Decreto 1736/1998, de 11 de julio, texto que contiene en su Título V la primera normativa sobre protección de datos específica del Sector de las Telecomunicaciones.

Durante 1999 se ha inspeccionado a los principales operadores de telefonía fija de cara a conocer su grado de adecuación a la legislación sobre protección de datos, tanto en lo referente a la Ley Orgánica 5/1992, de 29 de octubre (Ley vigente hasta el 14 de enero de 2000, en que entró en vigor la nueva L.O.P.D., Ley 15/1999, de 13 de diciembre), como en lo relativo al Real Decreto 1736/1998, específico para el sector de las telecomunicaciones.

Dentro de las Inspecciones de Oficio realizadas a dichos operadores merecen destacarse tres aspectos o actuaciones diferenciadas: El PRIMERO se refiere a la forma de prestación del consentimiento por los abonados para que sus datos personales puedan ser tratados por los operadores. El SEGUNDO se concreta en el análisis sectorial del Real Decreto 1736/1998 y el grado con que los operadores se adecuan a sus prescripciones. Y el TERCERO afecta a los denominados procedimientos de "scoring".

* **PRIMERO: Tratamiento de datos personales sin consentimiento.**

En las inspecciones practicadas se prestó especial importancia al sistema con que las operadoras tratan los datos personales de los abonados, dada la importancia cuantitativa y cualitativa de los datos tratados. En efecto, junto a los datos de tráfico y facturación se tratan otras tipologías de datos, entre las que se encuentran: los datos del cliente obtenidos en base a la propia relación comercial establecida, otros datos del cliente obtenidos mediante encuestas, datos estadísticos socioeconómicos y demográficos que se asignan a cada cliente en base a su domicilio, bases de datos de acceso público, etc.

Todo este conjunto de datos pasan a integrar un fichero automatizado específico, no sólo desde el punto visto lógico sino físico, es decir, se soporta el fichero sobre equipos informáticos y programas dedicados exclusivamente a dicho fichero. Los equipos informáticos y programas utilizados son de última generación y en muchos casos diseñados especialmente para este tipo de tratamientos, tan especiales, que han acuñado sus propia terminología, denominándose DATAWAREHOUSE a toda la infraestructura de equipos y programas necesarios para los tratamientos y DATAMINING a los tratamientos en sí.

El hecho de que estos tratamientos se realicen con un sistema específico y no con los sistemas informáticos ya existentes se debe fundamentalmente a dos motivos: En primer lugar, a que en los sistemas operacionales, esto es, los que se utilizan para las operaciones del día a día y que permiten a la empresa facilitar los servicios ofertados (típicamente son los sistemas de gestión de clientes, facturación, gestión de la red, gestión de proveedores, gestión de empleados), cuentan, cada uno de ellos, con partes de la información sin que ninguno de ellos cuente con la totalidad, por lo que determinados cruces no se pueden hacer. En segundo lugar, porque algunos tratamientos, y en especial los de datamining, requieren tal capacidad de procesamiento que si se realizaran en el propio sistema operacional probablemente se vería comprometida la operación del día a día. Por estas razones los sistemas de datawarehouse suelen constituirse como sistemas autónomos, que copian la información de los sistemas operacionales para no alterar sus respectivas funciones y al disponer no ya de partes, sino del total de la información, permite realizar cualquier tratamiento que se desee.

La incorporación en este campo de sistemas de datawarehouse y datamining, sistemas por otro lado muy costosos, ha surgido como consecuencia de la fuerte competencia existente en el sector y que pone a estas empresas ante la necesidad de obtener ventajas competitivas frente al resto. Una de las formas de obtener estas ventajas es la realización de acciones específicas de marketing sobre colectivos concretos de clientes, acciones más eficaces y eficientes que las costosas campañas publicitarias tradicionales dirigidas al público en general.

Estas campañas de marketing "personalizado" sitúa a los departamentos de marketing ante la necesidad de conocer lo mejor posible a sus clientes. Esta necesidad lleva a que no sea suficiente conocer el grado de utilización de los servicios ofrecidos, sino que se hace necesario conocer también otro tipo de datos, como por ejemplo, datos relativos al entorno familiar (número de miembros de la unidad familiar y edades, régimen de la vivienda, tipo de vivienda), datos profesionales (nivel de estudios, profesión), datos económicos (nivel de ingresos), datos de aficiones y estilos de vida (hobbies, pertenencia a asociaciones, etc.), datos de consumo de servicios de la competencia, y datos de consumo en general, entre otros.

Con esta amalgama de información, los expertos de marketing pueden conocer en profundidad al colectivo de clientes de la empresa, clasificarlos en base a diferentes perfiles de comportamiento y realizar así promociones comerciales específicas.

Si bien es cierto que ninguna de las operadoras investigadas disponía de todas las tipologías de información enumeradas, no es menos cierto que, en mayor o menor medida, disponen de algunas de ellas y que en la mayoría de los casos los sistemas están preparados para disponer del resto.

En la inspección realizada a uno de los principales operadores (dentro del Plan global Sectorial de Inspección), se ha podido constatar este tratamiento masivo de datos que afectaba a dos colectivos de abonados. El primer colectivo, formado por abonados que no habían dado su consentimiento para que sus datos personales fuesen tratados por el operador de telefonía, o a los que ni siquiera se les había dado la posibilidad de prestar o no su consentimiento para dicho tratamiento, y el segundo colectivo, constituido por abonados a los que le fue solicitado por el operador su consentimiento para tratar sus datos, pero mediante una fórmula no considerada válida por la Agencia al no cumplir las

exigencias de la LORTAD.

Respecto del primer colectivo y como resultado de la mencionada inspección se constató que el operador disponía de un fichero automatizado de datawarehouse cuyo objeto era el tratamiento automatizado de los datos de tráfico y facturación telefónica con fines comerciales propios.

El sistema recogía, grababa y almacenaba también los datos de detalle de las llamadas de todos los abonados, manteniendo al día el detalle de varios millones de llamadas diarias durante varias semanas, así como prácticamente la facturación del último año, y todo ello referido a la totalidad de sus abonados, que asciende a varios millones.

Igualmente, el datawarehouse permitía obtener información sobre el nombre, apellidos y domicilio tanto de los titulares de teléfono que realizan la llamada como el nombre, apellidos y domicilio de los titulares de teléfono que reciben la llamada.

Por sus altas prestaciones y flexibilidad, el datawarehouse permite realizar, en segundos, cualquier tratamiento de datos o consulta que se desee. Este sistema carece de registro de pistas de auditorías, por lo que no queda constancia ni de las personas que realizan las consultas ni de los datos personales a los que se ha accedido durante la misma.

El mencionado datawarehouse no tenía en cuenta ningún tipo de selección o filtración de datos, por lo que se incorporaban a él datos de todos los titulares existentes en los demás ficheros de la compañía (fichero de clientes, solicitudes de servicios, órdenes de servicio, ficha de cliente y fichero de facturación) y de todas sus llamadas. En consecuencia, en el datawarehouse se recogía y trataban los datos de las personas que habían manifestado su oposición al tratamiento automatizado de sus datos para fines de promoción comercial de los servicios de telecomunicaciones del operador.

La misma situación se producía respecto de los datos personales de tráfico y facturación telefónica de los abonados que habían adquirido tal condición con posterioridad al mes de enero de 1999, fecha en la que el operador remitió un encarte solicitando el consentimiento de los afectados por no haberse requerido su consentimiento para llevarlo a cabo. Se trata, pues, de abonados a los que ni siquiera se les dio la oportunidad de prestar o no su consentimiento para tratar sus datos personales.

La eliminación de los datos de abonados que habían rechazado prestar el consentimiento para el tratamiento de sus datos personales, así como la de aquéllos a los que no les había sido solicitado el consentimiento, se realizaba al definir cada una de las consultas que los usuarios realizaban a los datos contenidos en el datawarehouse. Esto quiere decir que el operador, después de incorporar los datos de todos sus abonados en el fichero, de tratarlos automatizadamente y de seleccionar el perfil del colectivo al que deseaba remitir encartes publicitarios, eliminaba a aquellos que se habían opuesto al tratamiento de sus datos con fines comerciales y a aquellos abonados que aún no habían prestado su consentimiento, no remitiéndoles promociones comerciales de dichos productos aunque efectivamente había tratado sus datos.

Todo ello ha supuesto la incoación al citado operador de un procedimiento sancionador por infracción del art. 6 de la Ley Orgánica 5/1992, por tratamiento automatizado de datos de carácter personal sin consentimiento de los afectados y con incumplimiento de los preceptos de protección de datos que imponen las disposiciones reglamentarias de desarrollo (art. 65.3 del R.D. 1736/1998), tipificada como grave en el art. 43.3.d) de la Ley Orgánica 5/1992 y pudiendo ser sancionada con multa de 10 a 50 millones de pesetas, de acuerdo con su art. 44.2.

Dentro de este procedimiento sancionador y mediante Acuerdo del Director de la Agencia de Protección de Datos se adoptó la medida cautelar consistente en que, por parte del operador se cesase de manera inmediata en el tratamiento automatizado, dentro del datawarehouse, de los datos de carácter personal relativos al tráfico y a la facturación telefónica de los abonados que se habían opuesto expresamente a que sus datos personales fuesen tratados automatizadamente, así como de los abonados que no habían prestado el consentimiento exigido por el artículo 65.3 del Real Decreto 1736/1998 antes citado, y se concedió al operador un plazo de cinco días hábiles, contados a partir del siguiente a la notificación del citado Acuerdo, para llevar a cabo las medidas acordadas. Dicha medida cautelar fue inmediatamente cumplida por el operador, que procedió a borrar todos los datos de carácter personal del datawarehouse, borrado que afectó a la totalidad de sus abonados y que impidió que el Sistema se volviera a cargar con nuevos datos.

Este procedimiento terminó con una Resolución del Director de la APD confirmatoria de los hechos imputados que sancionó al operador en los términos arriba expuestos con una multa de 50 millones de pesetas.

Respecto del segundo colectivo mencionado y dentro también de la citada inspección, se investigó el procedimiento utilizado por el operador para recabar el consentimiento para tratar los datos de tráfico telefónico de sus abonados. Durante las actuaciones realizadas se constató que el operador había realizado tratamiento de datos personales de sus abonados con fines de promoción comercial de sus propios productos, y para ello había tratado conjuntamente en un mismo fichero (datawarehouse), diferentes tipologías de datos procedentes de otros ficheros, entre los que se encuentran datos de tráfico telefónico, facturación, ficha de clientes, etc.

De los hechos constatados durante la tramitación del procedimientos, se concluyó que la finalidad prioritaria del fichero datawarehouse era la de la promoción comercial, motivo por el cual realizaban cruces de la información, perfiles, categorías de clientes y hábitos de utilización de los servicios de telecomunicaciones; prestaciones que, obviamente, no son necesarias para la facturación, el pago o la gestión del tráfico telefónico. Otra cosa es que el datawarehouse reca-

base o se incrementase precisamente con estos últimos datos, que son la base para realizar perfiles, pero no por ello se utilizaba el sistema con la finalidad exclusiva de gestionar facturación o pago telefónicos, puesto que para ello el operador ya dispone de ficheros expresamente destinados a esos fines, como así consta en el Registro General de Protección de Datos de la Agencia.

Además, con la mera inclusión de los datos personales en el datawarehouse ya se ha producido el tratamiento automatizado de los datos antes de definir la consulta, es decir, antes de definir los parámetros que van a servir para realizar la campaña promocional, tal y como resulta claramente de lo dispuesto en el artículo 65.5 del Real Decreto 1736/98, por lo que, desde ese mismo momento (y no desde que se realiza efectivamente la promoción comercial) se entiende cometida la infracción, si no se cuenta con el consentimiento lícito de los afectados e independientemente de que luego se realice o no la promoción comercial.

El fundamento jurídico de esta conclusión se halla, a juicio de la Agencia de Protección de Datos, en que cuando un abonado no está suficientemente informado sobre los usos y finalidades que sus datos van a tener durante ese tratamiento, entiende que las relaciones entre la empresa y él son, exclusivamente, las necesarias para que reciba el servicio de telecomunicaciones y para abonar el dinero que en contraprestación le corresponda. Por lo tanto, sus datos personales no deben ser incluidos en otro fichero distinto del específicamente destinado al tráfico, al pago o la facturación telefónica, máxime cuando ese fichero está destinado esencialmente a la promoción comercial y se utiliza para crear perfiles y categorías de clientes.

En este sentido, el artículo 65 reconoce la posibilidad de realizar tratamientos con los datos de tráfico y facturación siempre que se disponga del consentimiento de los afectados. Este consentimiento ha de ser informado tal y como se recoge en el considerando 17 de la Directiva 97/66/CE:

"Considerando que los datos relativos a los abonados utilizados para el establecimiento de llamadas contienen información sobre la vida privada de las personas físicas y atañen a su derecho de respeto a la correspondencia, o afectan a los intereses legítimos de las personas jurídicas; que dichos datos sólo podrán almacenarse en la medida en que resulten necesarios para la prestación del servicio, para fines de facturación y para los pagos de interconexión, durante un período limitado; que cualquier tratamiento que el proveedor del servicio público de telecomunicación pretenda llevar a cabo para la prospección de sus propios servicios de telecomunicaciones sólo puede permitirse si el abonado ha manifestado su acuerdo sobre la base de una información plena y exacta facilitada por el proveedor de servicios públicos de telecomunicaciones acerca del tipo de tratamiento que pretende llevar a cabo;"

Para realizar el tratamiento anterior, el operador ha obtenido los datos personales de las siguientes fuentes: datos identificativos (obtenidos del cliente cuando contrata el servicio), datos de equipamiento contratado (obtenidos también del cliente), datos de tráfico (obtenidos de la red telefónica), datos de facturación (procedentes del sistema de facturación), datos socio-familiares (obtenidos mediante encuesta telefónica realizada en el año 1997) y otros datos (cuyo origen es una segmentación interna).

Y para pedir el consentimiento al tratamiento anterior, el operador ha remitido varios encartes a sus abonados junto con una factura: uno, dirigido a aquellos abonados dados de alta antes al 06/09/98, cuyo texto dice:

"*De acuerdo con el compromiso de trasparencia en la gestión de sus datos de tráfico telefónico, le informamos que ..... trata esta información exclusivamente para ofrecerle la mejor calidad de atención y proponerle nuestros servicios. Si no desea que dicho tratamiento se produzca, no tiene más que comunicarlo a: ..... Ref.: DATOS Apartado de Correos ..... 28080 Madrid* "

y otra, dirigida a abonados dados de alta con posterioridad a esa fecha y antes del 09/08/99, cuyo texto es:

"*..... LE INFORMA. De acuerdo con el compromiso de transparencia en la gestión de sus datos de tráfico telefónico, le informamos que ..... va a tratar esta información, exclusivamente para ofrecerle la mejor calidad de atención y proponerle nuestros servicios. Si no desea que dicho tratamiento automatizado se produzca, no tiene más que comunicarlo a: Ref.: DATOS, Apartado de Correos ..... Código Postal 28.080 Madrid* ".

Sin embargo, dichas notificaciones únicamente hacen referencia a los datos de tráfico sin especificar cuáles y, por otra parte, tampoco hacen referencia a los datos de facturación, cuando estos últimos son objeto de tratamiento en el fichero. Tampoco hace referencia al artículo 65 del Reglamento del Servicio Universal (Real Decreto 1736/1998), en base al cual se ha de realizar dicha comunicación y que especifica cuáles son los datos de tráfico y facturación que se pueden tratar con fines de promoción comercial propia; no se especifica el plazo conforme al cual la falta de contestación por el abonado supone el otorgamiento de consentimiento tácito y tampoco se informa de que el tratamiento de los datos de tráfico se va a realizar conjuntamente con otras tipologías de datos, lo cual permite establecer perfiles, categorías de clientes y hábitos de uso de los servicios de telecomunicaciones. Por último, tampoco se informa del plazo referido en la disposición transitoria séptima del R.D. 17836/1998 conforme a la cual transcurrido un mes desde la recepción de la información sin que el abonado se haya pronunciado al respecto, se entenderá que no se opone.

Esta situación ha supuesto la incoación de un procedimiento sancionador al operador por tratamiento de datos personales sin consentimiento con infracción del art. 6 de la Ley Orgánica 5/1992. Esta infracción está tipificada como grave en el artículo 43.3 d) de dicha Ley, pudiendo ser sancionada con una multa de 10.000.001 a 50.000.000 de pesetas, según lo dispuesto en su artículo 44.2. Dicho procedimiento a la fecha del cierre de esta Memoria aún no había concluido.

* **SEGUNDO: Análisis sectorial del Real Decreto 1736/1998, de 31 de julio.**

Otro de los aspectos analizados durante las inspecciones sectoriales de oficio realizadas por la Agencia de Protección de Datos durante 1999 y que aún se encuentran en fase de tramitación, ha ido dirigido específicamente a comprobar el grado de adecuación de estos operadores a las prescripciones del Real Decreto 1736/1998, relativas a la prestación de servicios avanzados de telecomunicaciones.

De los aspectos que abarca dicho Real Decreto 1736/1998, se expone a continuación la panorámica general de cada uno de ellos, excepto el relativo a los datos de tráfico y facturación por haber sido tratado anteriormente.

* **Respecto a medidas de seguridad.**

El artículo 62 establece la necesidad de realizar un análisis de riesgos de los servicios que se prestan de cara a incorporar las medidas de seguridad acordes con los riesgos detectados, así como la identificación de los riesgos concretos de violación de seguridad de la red, debiendo en este último caso el operador informar a los abonados sobre la existencia de dichos riesgos así como de las posibles soluciones y de sus costes.

En las inspecciones practicadas se han detectado deficiencias respecto a lo prevenido en este artículo. Estas deficiencias están relacionadas con la carencia, en general, de análisis de riesgos formales y rigurosos, lo que lleva a que las medidas de seguridad que se implantan y los controles asociados no resultan ser suficientes. Respecto a la identificación de riesgos concretos, hay que decir que en raras ocasiones se informa a los usuarios sobre ellos.

* **Respecto de las datos personales que aparecen en la facturación detallada.**

Lo recogido en el artículo 66 tiene su origen en la confrontación de dos derechos. Por un lado, el derecho del titular de la línea, que como tal es el responsable frente al operador de hacer frente al pago de la factura correspondiente al servicio contratado y quiere, por lo tanto, disponer de información suficiente en la factura para poder dar su conformidad a la misma, y por otro lado, el derecho a la privacidad de las personas que, aún siendo distintas del titular de la línea, hacen también un uso del servicio, como por ejemplo las personas que conviven con el titular o los clientes de un hotel.

Al igual que el texto de la Directiva 97/66/CE, el texto del presente artículo no recoge ninguna solución concreta de equilibrio entre ambos derechos aunque sí apunta dos posibles vías de solución. Una de ellas va en el sentido de suprimir algunas de las cifras menos significativas de la lista de números llamados que aparece en la factura, mientras que la otra apunta hacia la existencia de mecanismos de pago alternativos que permitan que la llamada que realiza un usuario, distinto del titular, pueda ser pagada por el propio usuario, no teniendo que aparecer por lo tanto en la factura del titular. Un ejemplo de éste último procedimiento sería el cargo de una llamada a la tarjeta de crédito del usuario o a una modalidad de tarjeta de pre-pago o post-pago del propio operador.

El artículo deja pendiente de una Resolución de la Secretaría General de Comunicaciones la adopción de una solución o soluciones definitivas. Esta Resolución no ha sido publicada hasta la fecha.

Hasta ahora, el único país comunitario que ha elaborado recientemente una legislación específica de lo prevenido en este artículo ha sido Italia, que se decantó por la supresión de cifras del número llamado en el listado de las facturas. Este hecho ha provocado un fuerte rechazo por parte de los titulares de las líneas hasta tal punto que se están pensando el derogar la citada legislación. A la luz de la experiencia Italiana, parece que lo más conveniente sería el potenciar los mecanismos de pago alternativos ya mencionados anteriormente.

Sobre este tema se ha pronunciado el Grupo de Trabajo del art. 29 en aras de conciliar ambos derechos, en los términos que se exponen en esta Memoria en el apartado correspondiente a relaciones internacionales.

De las actuaciones practicadas se ha concluido que la totalidad de los operadores emiten facturas con el desglose de las llamadas con mayor o menor detalle, respetando el deseo de aquellos abonados que solicitan no recibir facturas detalladas. Respecto de las diferentes modalidades de facturas, los operadores se encuentran a la espera de la mencionada Resolución de la Secretaria General de Comunicaciones. Hasta la fecha, sólo algunos operadores disponen de mecanismos de pago alternativos, si bien la tendencia es que estos mecanismos se generalicen.

* **Respecto de las guías telefónicas.**

En el artículo 67 se recoge que las guías de abonados, independientemente del formato en que se presente la información, deberán limitarse a los datos que sean estrictamente necesarios para identificar a un abonado concreto. Se deja la puerta abierta a que el operador pueda introducir datos adicionales siempre que cuente con el consentimiento inequívoco del abonado.

Se reconoce el derecho del abonado a exigir al operador que excluya sus datos de las guías, a que se omita parcialmente su dirección y a que figuren sus datos en la guía con una marca indicativa de que esos datos no pueden utilizarse para fines de venta directa. El operador viene obligado a atender estos derechos de forma gratuita.

Dada la multiplicidad actual de operadores y el requerimiento establecido en el artículo 14 del Reglamento en el sentido de que debe facilitarse al abonado una guía unificada por provincia, se ha optado por dejar para un desarrollo posterior mediante Orden Ministerial el establecimiento de las condiciones en que deberán elaborarse estas guías y las

condiciones en las que se harán constar los datos en ellas. Esta Orden no ha sido publicada todavía por el Ministerio de Fomento.

De las investigaciones practicadas se ha constatado la no existencia de una guía unificada, estando los operadores pendientes de la publicación de la mencionada Orden Ministerial. No obstante, los abonados pueden ejercer sus derechos de exclusión de las guías, solicitar la omisión parcial de la dirección y pedir que se indique que sus datos no se utilicen para fines de venta directa.

* **Respecto de las llamadas con fines de venta directa.**

En el artículo 68 se regula las llamadas que se realicen a través de las redes de telecomunicaciones con fines de venta directa, distinguiendo entre dos categorías de llamadas. Una primera categoría que engloba todas aquellas llamadas generadas sin intervención humana, es decir por procedimientos automáticos que generen llamadas o envíen faxes. Y una segunda categoría que engloba al resto de llamadas, es decir, las realizadas de forma manual, típicamente operadores de televenta.

La norma prevé que únicamente podrán realizarse llamadas de la primera categoría (llamadas automáticas) a aquellos abonados que hayan manifestado su consentimiento previo. Por el contrario, las llamadas de la segunda categoría (llamadas manuales) podrán realizarse siempre que el abonado no haya manifestado su oposición a las mismas.

De las investigaciones practicadas se ha concluido que ninguno de los operadores analizados realizan llamadas de la primera categoría ni para fines propios ni de terceros. No obstante, y respecto de este tipo de llamadas, sí que manifiestan que en el estado actual de la tecnología, el operador no tiene forma de saber si un tercero utiliza la red del operador para realizar este tipo de llamadas, ya que no es posible saber si el origen de la misma es manual o automático y mucho menos discernir si su contenido es con fines de venta directa o no.

Sí reconocen los operadores, en general, realizar llamadas de la segunda categoría con fines comerciales propios, respetando los deseos de aquellos abonados que solicitan no recibir este tipo de llamadas.

* **Respecto de los servicio de presentación y limitación del identificador de línea llamante y línea conectada.**

En los artículos 69 a 79 se recoge la diferente casuística asociada a estos servicios. El legislador comunitario ha considerado, y así se recoge en la Directiva 97/66/CE, que los servicios de presentación de la identificación de la línea llamante y conectada afectan a la privacidad, ya que muestran información personal sobre el titular de la línea que realiza la llamada en el caso de la identificación de línea llamante y del titular de la línea que recibe la llamada en el caso de la identificación de la línea conectada. Por otro lado, y teniendo en cuenta el derecho de oposición del afectado, principio ya consagrado en las legislaciones de protección de datos, se recogen en los mencionados artículos las diferentes formas en que dicho derecho puede ser ejercido por los afectados de que se trate en cada caso, así como las excepciones al derecho de oposición para la eliminación del identificador de línea llamante cuando la llamada tiene por destino un servicio de urgencia.

Se recoge en el artículo 67 la obligación del operador de informar a sus abonados de la puesta en marcha de los servicios de identificación de línea llamante y conectada con quince días de antelación. Se establece que para los abonados que han solicitado su exclusión de las guías (artículo 67) deba remitirse una comunicación adicional que recoja la especial situación en que se encuentran estos abonados, ya que al excluirse de las guías desean mantener su número de teléfono secreto y estos servicios pueden provocar que dicho número aparezca en las pantallas de los teléfono que envíen llamadas a estos abonados o en los teléfonos a los que estos abonados llamen.

De los artículos mencionados en este apartado, cinco de ellos remiten la concreción de determinados aspectos a normas posteriores. De los cinco, únicamente se ha desarrollado uno mediante la publicación de la Resolución de 2-12-98 de la Secretaría General de Comunicaciones, que atribuye el código *"067"* al servicio de supresión en origen, llamada a llamada, de la identificación de línea llamante.

Los otros cuatro aspectos pendientes de regulación son los siguientes:

* Calendario para el cumplimiento de la obligación recogida en el artículo 74 relativo al filtrado en destino de las llamadas sin identificación. Se atribuye la redacción de dicho calendario al Ministerio de Fomento.

* Resolución de la Secretaría General de Comunicaciones relativa a los servicios de urgencia que dispongan de la posibilidad de eliminar las marcas de supresión de la eliminación del identificador de línea llamante según se recoge en el artículo 75.

* Relación de destinos a los que, con el fin de proteger el derecho a la intimidad de los ciudadanos, no se les habilite de la posibilidad de disponer del servicio de identificación de la línea llamante. Según recoge el artículo 76, corresponde al Ministerio de Fomento la elaboración de dicha relación.

* Relación de países a los que pueda ser enviada información sobre la identidad de la línea llamante en la interconexión internacional. Según se recoge en el artículo 79, compete a la Secretaría General de Comunicaciones la elaboración de dicha relación previo informe de la Agencia de Protección de Datos.

De las actuaciones practicadas sobre los principales operadores en relación a estos artículos se ha constatado que si bien casi todos los operadores prestan los servicios de identificación de línea llamante y conectada, la casuística es diferente en cada uno de ellos.

En el caso del operador dominante, éste presta los mencionados servicios sin que algunas de las restricciones que imponen los artículos mencionados anteriormente se encuentran operativas en la totalidad de las líneas afectadas y sin que el Ministerio de Fomento haya autorizado ninguna exención tal y como recoge el apartado 2 del artículo 64.

Se ha detectado también que algunos de los operadores envían la identificación de línea llamante a terceros países en llamadas internacionales sin que se haya publicado la relación de países a los que puede ser enviada dicha información.

* **Respecto del servicio de desvío automático de llamadas.**

El artículo 80 recoge que los operadores que presten el servicio de desvío automático de llamadas deberán facilitar al abonado, mediante un procedimiento sencillo y gratuito, la posibilidad de poner fin a los desvío que a su terminal efectúen terceros.

De las investigaciones realizadas se ha constatado que diversos operadores, que prestan el servicio de desvío automático de llamadas no disponen de este procedimiento y no han solicitado la correspondiente exención del Ministerio de Fomento tal y como establece el apartado 2 del artículo 64.

* **TERCERO: Procedimientos de "scoring".**

Finalmente, cabe destacar también las inspecciones sectoriales practicadas en relación con los denominados procedimientos de "scoring". Consisten en esencia estos procedimientos en que un operador facilita a otra entidad especializada en información sobre solvencia patrimonial y crédito una relación de sus propios clientes o potenciales clientes, la cual le es posteriormente devuelta por ésta, pero ampliada con una clasificación con información sobre la aptitud crediticia de cada uno de esos clientes, lo cual le sirve al operador para rechazar o no la solicitud de servicio realizada por el potencial cliente. Esta operación de "scoring" puede suponer una cesión inconsentida de datos personales a efectos de la Ley española de Protección de Datos, razón por la que se han abierto dos procedimientos sancionadores a otros tantos operadores, que aún están en fase de tramitación y que concluirán en el próximo año 2000.

2.13.2 Actuaciones de la APD realizadas en virtud de denuncias de los ciudadanos

La Agencia de Protección de Datos ha seguido recibiendo durante el año 1999 un alto porcentaje de denuncias relacionadas con el uso de los datos personales de abonados a los servicios de telecomunicaciones. De entre ellas, las más significativas afectan a las siguientes materias:

* Se han recibido denuncias relativas al procedimiento utilizado por un operador para recabar el consentimiento para el tratamiento de los datos de tráfico. Estas denuncias han sido incorporadas a los procedimientos que ya se encontraban abiertos de oficio, y de los que se ha hablado anteriormente, en el seno de los cuales ya se habían iniciado las correspondientes actuaciones inspectoras.

* Se han recibido también denuncias que hacen referencia a la difusión de datos personales que un importante operador de telefonía realiza a través del enlace de Internet que, con el nombre "*páginas blancas on line*", permite a cualquier usuario conocer el nombre completo, número de teléfono y domicilio, y que además adjunta un plano a través del cual se puede ubicar el emplazamiento exacto de la calle donde está el domicilio del abonado. Este servicio que ofrece el operador, según consideran los denunciantes, vulnera la legislación de protección de datos al incluir en el tratamiento datos que no son adecuados ni pertinentes y sí excesivos para la finalidad legítima de dicho tratamiento, que no es otra que la de facilitar el número de teléfono de un abonado para realizar una comunicación telefónica, siempre que figuren en la guía su nombre y dirección.

Las actuaciones previas relacionadas con este tipo de denuncias han concluido con resoluciones de archivo, por entender la APD que la mera posibilidad de poder consultar la localización geográfica del domicilio de los abonados no supone una ampliación de los datos de acceso público de dichos abonados, dado que en la consulta simplemente aparece el plano de situación con el nombre de la calle y la ubicación del número de inmueble al que corresponde. Los planos de una localidad no suponen en sí mismo una invasión de la intimidad de las personas físicas que en ella residen, por lo que concretar el emplazamiento del dato referente al domicilio de un abonado telefónico, si sólo se limita a eso, no puede considerarse un exceso de información siempre y cuando dicho dato figure en repertorios públicos.

A la hora de dictar estas Resoluciones se tuvieron en consideración las recomendaciones del Grupo Internacional de Protección de Datos en Telecomunicaciones, si bien en los casos aludidos no se producía una identificación física del inmueble, sino una simple aportación de un plano o callejero.

En este sentido, el Grupo Internacional de Protección de Datos en Telecomunicaciones en su reunión de 29 de abril de 1999 en Noruega ha fijado la *"Posición común sobre la protección de datos en bases de datos de imágenes de edificios"*, cuyas conclusiones se exponen en el apartado de esta Memoria correspondiente a las relaciones internacionales.

Efecto jurídico distinto al descrito, que podría vulnerar los derechos protegidos por la legislación sobre protección de

datos, se produciría si, a través de la consulta al servicio "Páginas Blancas On Line" y mediante una sola entrada al nombre de una persona, se pudiera obtener el plano con la ubicación de los distintos inmuebles y domicilios que tal persona pudiera tener en una o varias localidades.

* Otro tipo de denuncias se refieren a la obligatoriedad de facilitar los datos de una cuenta corriente o tarjeta de crédito para conectarse al servicio de acceso a Internet facilitado por un proveedor, cuando el pago del mismo se ha realizado por anticipado con la compra de un kit contra reembolso. En estos casos, el usuario no es informado en ningún momento de dicha obligatoriedad, ni de que se condicione la prestación del servicio a que se faciliten dichos datos financieros.

Estos hechos han supuesto una sanción por infracción del artículo 4.1 de LORTAD, tipificada como grave en el artículo 43.3 d) y sancionada por el art. 44.2 con multa de 10 a 50 millones de pesetas.

En el transcurso del procedimiento quedó acreditado que cuando el usuario del servicio se conecta por primera vez, debe cumplimentar unos datos de carácter obligatorio y otros facultativos. Entre los obligatorios se encuentran datos de la cuenta bancaria o número de tarjeta VISA y, aunque el operador manifestó que los datos financieros se exigen sólo a efectos de renovación, se considera que son excesivos para la finalidad para la que se exigen, dado que el cliente, después de haber transcurrido el tiempo contratado, puede optar por no renovar su contrato y, por tanto, todos los datos que haya dado con esta finalidad de renovación quedan sin efecto.

* Un cuarto grupo de denuncias se producen a raíz de la aparición de nuevos operadores de telecomunicaciones y se refieren al procedimiento utilizado por aquéllos para darse a conocer en el mercado y así captar socios-abonados. Concretamente denuncian la pertinencia de los datos solicitados en los formularios utilizados para la captación de socios y la utilización posterior de los mismos.

Todas estas denuncias han finalizado con resoluciones de archivo, puesto que los operadores a los que se refieren las denuncias han sido adjudicatarios para la gestión indirecta del servicio público de telecomunicaciones por cable en una demarcación territorial por el Ministerio de Fomento, y para poner en conocimiento de los habitantes de esa demarcación su entrada en el mercado, utilizan formularios en los que informan de dicho extremo, incluyendo en los mismos la cláusula informativa exigida por la Ley Orgánica 5/1992, y siendo además voluntaria la cumplimentación o no de los formularios por parte de los afectados.

* También, se han denunciado en la APD aspectos relacionados con las búsquedas inversas en directorios, esto es, obtener la identidad y/o dirección de una persona a partir de su número de teléfono, fax o correo electrónico.

La existencia de este tipo de servicios representa una amenaza para la privacidad. La finalidad de un repertorio con búsqueda inversa es diferente de la de un repertorio tradicional de abonados y si bien el recurso de los directorios inversos puede servir a intereses legítimos en algunos casos especiales de emergencia y seguridad pública, el proporcionar los datos de un usuario a partir de su número de teléfono, sin disponer del consentimiento del usuario, constituye un tratamiento desleal de la información.

En virtud de denuncias recibidas, por las que un operador situado en el extranjero utilizaba este sistema de "búsqueda inversa", la APD se ha dirigido a la Autoridad de Control de dicho país, al amparo de lo establecido en el art. 28.6 de la Directiva, para que le informe sobre si el tratamiento de los datos del denunciante español se adecua a las previsiones de la Directiva.

* Finalmente, cabe señalar una denuncia que hace referencia a hechos relacionados con diferentes artículos del R.D. 1736/98 como son:

* Que el operador no haya accedido a su petición consistente en la presentación de la identificación de la línea llamante (la denunciante se apoya en la Directiva 97/66/CE y en la Disposición Transitoria Novena del RD 1736/98.

* Que el operador no ha accedido a su petición consistente en rechazar las llamadas procedentes de usuarios o abonados que hayan suprimido la presentación de la línea llamante (art. 74 RD 1736/98 y Directiva 97/66/CE).

* Que el operador tampoco ha accedido a su petición consistente en rechazar las llamadas no solicitadas con fines de venta directa (art.68 RD 1736/98 y art. 12 de la Directiva 97/66/CE).

* Que el operador no le ha proporcionado el servicio consistente en la facilidad de identificación de la línea llamante en los mensajes de depósito del servicio contestador, del cual la denunciante es una abonada.

* Que el operador no le ha proporcionado el servicio consistente en establecer un procedimiento para poner fin al desvío automático de llamadas a su terminal por parte de un tercero (art. 10 de la Directiva 97/66/CE y art. 80 del RD 1736/1998.

A la vista de esta denuncia se han iniciado actuaciones previas al objeto de estudiar el alcance de los hechos denunciados, si bien al cierre del año 1999 no se ha iniciado aún ningún procedimiento por parte del Director de la Agencia de Protección de Datos.

2.14 INSPECCIÓN AL SECTOR DE INVESTIGADORES PRIVADOS (DETECTIVES PRIVADOS)

En el año 1999 la Agencia de Protección de Datos inició un plan de oficio con el objeto de analizar los ficheros automatizados y la información manejada por las entidades del Sector de Investigación Privada, cuya actividad se regula en la Ley 23/92, de 30 de julio, de Seguridad Privada y en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, a fin de comprobar el grado de adecuación de dichas entidades a las prescripciones de la Ley Orgánica 5/1992.

En concreto, los objetivos del Plan han sido los siguientes:

- Identificar las fuentes y los procedimientos de recogida de información utilizados en el desempeño de su trabajo, por los profesionales del sector, prestando especial atención al posible acceso o existencia de copia de ficheros tales como: censo, ficheros de solvencia patrimonial o vehículos de la Dirección General de Tráfico.

- Identificar los ficheros automatizados con los que cuentan tales profesionales, comprobando respecto de los automatizados la adecuación a la Ley Orgánica 5/1992.

- Recabar información de los equipos informáticos y de los propios ficheros automatizados, así como de las herramientas utilizadas en la confección de los informes y en el almacenamiento de éstos y de sus expedientes asociados.

- Determinar las posibles cesiones de datos realizadas por las entidades inspeccionadas.

*** Fuentes de información y criterios de selección**

En el proceso de selección de las entidades a inspeccionar correspondientes a cualquier sector de actividad, se persigue obtener una muestra de ellas lo suficientemente representativa que permita después extrapolar las conclusiones obtenidas del trabajo realizado a todas las entidades del sector.

De acuerdo con estas premisas, en el Plan de oficio de las entidades del Sector de investigación Privada no se ha contado con una única fuente de información para obtener datos fiables sobre el estado del sector, sino que se ha acudido a diferentes fuentes al objeto de obtener hechos diferenciales entre las diversas entidades de manera que permitiera obtener la muestra deseada.

A tal fin, se seleccionaron nueve entidades ubicadas en Barcelona, Madrid, Sevilla, Valencia, Valladolid y Palma de Mallorca; la alta concentración de entidades en Madrid y Barcelona, respecto de otras provincias, obligó a realizar la mayoría de las inspecciones en estas ciudades.

* **Resultados de la inspección**

De las investigaciones y comprobaciones realizadas sobre los ficheros inspeccionados, manifestaciones recogidas en las actas de inspección y de la documentación obtenida por la inspección, se desprenden como conclusiones más importantes las siguientes:

- La mayoría de las entidades reciben un gran número de peticiones concernientes a personas jurídicas (en algunos casos de hasta un 80%), siendo las entidades que exclusivamente realizan trabajos puros de investigación privada y no de información comercial, las que reciben mayoritariamente peticiones referentes a personas físicas.

- Entre las fuentes públicas que utilizan las entidades en el desarrollo de sus investigaciones se encuentran los diferentes Registros Públicos existentes: Registro Mercantil, de la Propiedad, de Buques y Naves, de Vehículos de la Dirección General de Tráfico, así como repertorios telefónicos.

- Aquellas entidades que elaboran informes comerciales tienen suscritos contratos con empresas que les facilitan acceso a sus ficheros de información comercial o de solvencia patrimonial, proporcionando dicho acceso a través de INTERNET.

- De las comprobaciones efectuadas en las inspecciones, no se ha acreditado que en el desarrollo de sus investigaciones los detectives privados accedan ilegítimamente a información residente en otros ficheros automatizados con datos de carácter personal.

- Cuatro de las entidades inspeccionadas cuentan con ficheros automatizados donde recogen los datos identificativos de los clientes y de las personas investigadas.

- Una de las entidades tiene automatizado el Libro-Registro contemplado en el Reglamento de Seguridad Privada cuyo contenido y formato ha sido autorizado por la Dirección General de la Policía, recogiendo datos identificativos de los clientes y de las personas investigadas.

- La documentación recabada en las investigaciones y los informes elaborados relativos a las mismas suelen guardarse en expedientes manuales, aunque tres de las entidades guardan copia de dichos informes en los equipos informáticos utilizados para su elaboración.

- De la operativa de algunos detectives y de las manifestaciones realizadas por los mismos, se desprende que no es absolutamente necesario para el desempeño de su trabajo mantener la documentación recabada en sus investigaciones, sino que tanto la documentación como los informes podrían quedar exclusivamente en poder de los clientes al

finalizar la investigación.

- Tres de las entidades investigadas no guardan ninguna documentación recabada para la investigación, aunque sí guardan los informes elaborados por si fuera necesaria su ratificación ante los Tribunales.

- Con relación a las cesiones de datos, en todos los casos, los responsables han manifestado, y no se ha constatado lo contrario en el curso de la inspección, que el único destinatario de los resultados de sus trabajos es el propio cliente que encarga la realización de la investigación. Los detectives privados son conscientes de la obligación del deber de secreto que les impone la legislación vigente relativa a Seguridad Privada, que en el artículo 103 de su Reglamento recoge que los detectives privados están obligados a guardar riguroso secreto de las investigaciones que realicen, no pudiendo facilitar datos sobre las mismas más que a las personas que se las encomienden y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

Por tanto, a tenor de los resultados de la inspección y al margen de las obligaciones que a los Detectives Privados impone su normativa específica, el Director de la Agencia de Protección de Datos tiene previsto emitir durante el año 2000 unas recomendaciones que deberán ser observadas por las entidades del Sector de la Investigación Privada, al objeto de adecuar sus tratamientos automatizados a los principios de la normativa vigente en materia de protección de datos.

2.15 TARJETAS DE IDENTIFICACIÓN PARA JÓVENES

En la memoria del año 1998 se reseñaba el inicio de actuaciones relativas a la implantación de una tarjeta de identificación universitaria promovida por diversas universidades en colaboración con entidades bancarias. Este tipo de tarjeta puede tener una doble finalidad: Por un lado, se trata de un carnet universitario que actúa como documento de identificación y acceso a los terminales de información dentro de la universidad, y de otro, puede tener un carácter financiero como tarjeta de crédito y monedero electrónico, para aquellas personas que así lo soliciten.

El Director de la Agencia de Protección de Datos, durante el año 1999, resolvió las actuaciones anteriores dictando dos Resoluciones de Archivo en virtud del artículo 27.1 de la Ley Orgánica 5/1992, ya que los datos personales son facilitados por la universidad promotora del carnet a una entidad bancaria para la confección de tarjetas universitarias cuya única finalidad es la relacionada con temas universitarios, salvo en aquellos supuestos en que los interesados soliciten expresamente que dicha tarjeta, tenga, además, una finalidad bancaria. En este caso, el interesado presta su consentimiento a la entidad financiera para que utilice sus datos personales para una finalidad diferente a la que se atribuye en principio a la tarjeta como mero carnet universitario.

Durante 1999 se han recibido en la Agencia de Protección de Datos cinco reclamaciones relacionadas con la emisión de carnet de identificación destinados a los jóvenes, procediéndose a la apertura de otras tantas actuaciones de investigación.

De las actuaciones iniciadas cabe destacar las relativas a la presunta vulneración de la LORTAD a consecuencia de la implantación del Carnet Joven "EURO 26", que es un programa puesto en marcha en diversos países de nuestro entorno con el objetivo de ofrecer diferentes bienes y servicios a los jóvenes de entre 14 y 26 años y que, en algunos casos, posibilita funciones adicionales como medio de pago (monedero electrónico y tarjeta de crédito).

En España, la tarjeta esta promovida por el Instituto de la Juventud y por los Organismos equivalencites de las Comunidades Autónomas en colaboración con entidades financieras. Para adherirse al programa es necesario que el joven rellene una ficha, aporte una fotografía y pague la cuota que la Comunidad Autónoma correspondiente haya establecido.

De los expedientes iniciados como consecuencia de las anteriores actuaciones de inspección, es especialmente relevante lo siguiente:

* Posible vulneración de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, en la implantación del programa "EURO26" por una Consejería de Educación, Cultura, Juventud y Deportes, ya que los interesados en obtener el carnet deben rellenar un formulario en las oficinas de las entidades bancarias aportando sus datos personales de: *nombre, apellidos, dirección postal, DNI, teléfono, fecha de nacimiento y sexo.*

De las actuaciones practicadas por parte de la Inspección, se constató que existía un acuerdo para la promoción y comercialización del carnet joven "EURO26" firmado entre dicha Consejería y las entidades bancarias y que el formulario utilizado por las entidades bancarias para recabar los datos personales del interesado lleva incluida cláusula informativa relativa a la Ley Orgánica 5/1992 , por lo que se procedió al archivo de las actuaciones.

* Posible incumplimiento del artículo 5 de la Ley Orgánica 5/1992, por parte de la Administración patrocinadora del carnet Joven Euro < 26, ya que los jóvenes que solicitan el mencionado carnet no son informados de los derechos que les asisten y se condiciona la obtención del carnet a la autorización de transmisión de los datos.

Según la resolución de archivo dictada por el Director de la Agencia de Protección de Datos, el texto incluido en el impreso de solicitud del Carnet Joven Euro < 26 indica expresamente que los datos facilitados van a ser objeto de tratamiento automatizado por parte de la entidad bancaria y de la Administración competente para los fines propios del citado carnet. Por tanto, atendiendo a la cláusula y al contenido de los datos personales que se solicitan, cabe entender

que la información que exige el artículo 5 de la LORTAD puede ser deducida claramente de la naturaleza de los datos solicitdos y de las circunstancias en que se recaban, luego no existe desconocimiento de los afectados respecto a los usos y finalidades que se van a dar a los datos proporcionados. Tampoco existe duda sobre los responsables del tratamiento de dichos datos.

No obstante, se insta al organismo competente para que adopte las medidas necesarias para adecuar el impreso de solicitud del carnet Joven Euro < 26 al contenido exacto de lo prescrito por dicho art. 5, especificando el carácter obligatorio o facultativo de las respuestas, las consecuencias de la falta de respuesta a alguna pregunta y la dirección del responsable del fichero donde ejercitar los derechos de acceso, rectificación y cancelación.

2.16 OTRAS ACTUACIONES DE LA INSPECCIÓN DE DATOS

Dentro de las actuaciones previas efectuadas por la Inspección de Datos durante el año 1999, debemos hacer mención a las encaminadas a constatar la procedencia de los datos personales que una empresa privada incluye en sus ficheros automatizados, con la finalidad de editar diversas publicaciones referentes a temas relativos a la construcción y que contienen los datos personales de los profesionales que intervienen en ésta, tales como arquitectos, aparejadores, ingenieros, promotores o constructores. Las publicaciones son distribuidas por la entidad en distintos soportes, papel, disquete, fax o correo electrónico, de acuerdo con las necesidades de los clientes. Realizadas las correspondientes inspecciones se pudo constatar que los datos personales eran obtenidos por dicha empresa de Organizaciones Colegiales, Ayuntamientos y una Comunidad Autónoma.

Por todo lo expuesto se procedió al inicio del correspondiente procedimiento sancionador a la entidad privada por tratamiento automatizado y cesión de los datos de carácter personal sin el consentimiento de los afectados, lo que podría suponer infracción de los artículos 6.1 y 11.1 de la Ley Orgánica 5/1992, tipificadas como grave y muy grave, respectivamente. Al finalizar el año 1999 dicho procedimiento se encuentra aún en fase de tramitación.

V. SECRETARIA GENERAL

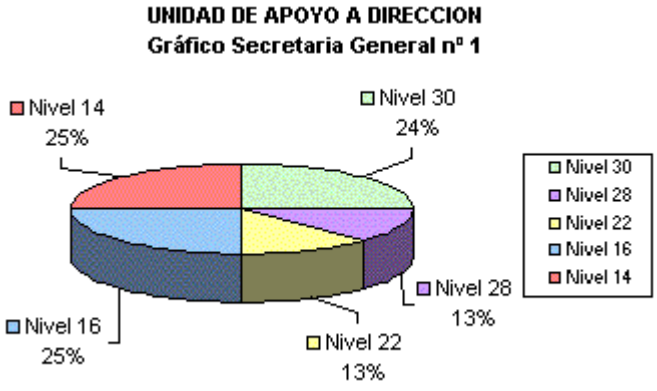
Las principales actividades realizadas por la Secretaría General durante 1999 han ido dirigidas a posibilitar el funcionamiento de la Agencia de Protección de Datos, en sus aspectos materiales, técnicos y de recursos humanos, así como el Área de atención al ciudadano. Para ello se han efectuado las siguientes tareas y funciones en cumplimiento de las competencias que el Real Decreto 428/93 de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, atribuye a la Secretaría General :

1. PLANIFICACIÓN, ORGANIZACIÓN Y GESTIÓN DE RECURSOS HUMANOS.

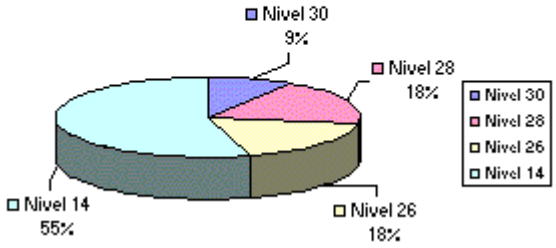
La estructura orgánica de la Agencia de Protección de Datos se configura, de conformidad con lo dispuesto en el artículo 11 del citado Real Decreto 428/93, en los siguientes órganos:

- El Director de la Agencia, asistido por su Secretaría Particular, Unidad de Apoyo y el Jefe del Gabinete Jurídico, que suponen un total de 8 funcionarios.
- El Consejo Consultivo
- El Registro General de Protección de Datos, integrado por 11 funcionarios.
- La Inspección de Datos, constituida por 23 puestos de trabajo de funcionarios, de los que 1 se encuentra vacante.
- La Secretaría General, integrada por 13 funcionarios y 3 laborales.

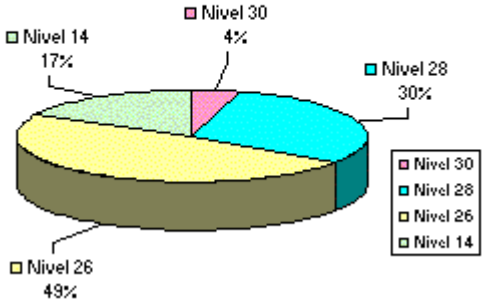
El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General se constituyen como órganos jerárquicamente dependientes del Director de la Agencia.



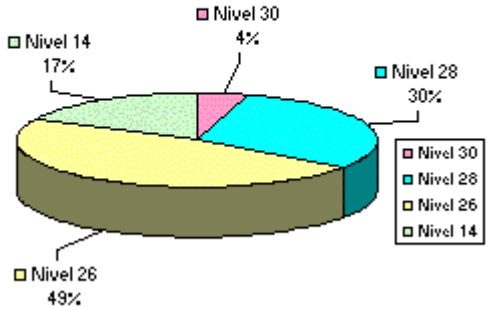
SUBDIRECCION GENERAL DE REGISTRO GENERAL DE PROTECCION DE DATOS
Gráfico Secretaría General nº 2



SUBDIRECCION GENERAL DE INSPECCION DE DATOS
Gráfico Secretaría General nº 3



SUBDIRECCION GENERAL DE INSPECCION DE DATOS
Gráfico Secretaría General nº 4



En materia de Planificación, Organización y Gestión de Recursos Humanos se han realizado las siguientes actuaciones:

* Gestión y Administración del personal funcionario y laboral destinado en la Agencia, y gestión de retribuciones y habilitación del mismo. Entre las actividades realizadas durante el año destaca, además de la gestión y administración ordinaria para el normal funcionamiento de la Agencia, la tramitación de un expediente de incremento de puestos de trabajo del Ente Público ante la Comisión Ejecutiva de la Comisión Interministerial de Retribuciones . Se ha puesto de manifiesto durante 1999 la insuficiencia de la actual Relación de Puestos de Trabajo para el desarrollo de competencias propias de este Ente Público para dar respuesta al gran volumen de actividad que viene experimentando un creciente y constante crecimiento, por lo que se ha considerado indispensable acometer un incremento de la Relación de Puestos de Trabajo que permita atender las crecientes necesidades de la Agencia. El expediente ha sido resuelto a principios del año 2000 otorgando un incremento de 7 puestos de trabajo, lo que constituye algo menos de la mitad de

lo solicitado.

* Realización de las convocatorias, formación e integración de las Comisiones de Valoración, y resolución de procedimientos de provisión de puestos de trabajo por concurso y libre designación, para la cobertura de la Relación de Puestos de Trabajo, compuesta por 55 puestos de trabajo que se proveen por funcionarios y 3 ordenanzas con vínculo laboral. Al finalizar el año 1999 se encontraba cubierta en un 98% en lo que se refiere a personal funcionario y al 100% en cuanto a personal laboral.

* Elaboración del anteproyecto de la Oferta de Empleo Público, en el que se solicita nuevamente la inclusión de las tres plazas de Ordenanza, actualmente cubiertas con personal eventual, a fin de que puedan ser provistas con personal laboral fijo.

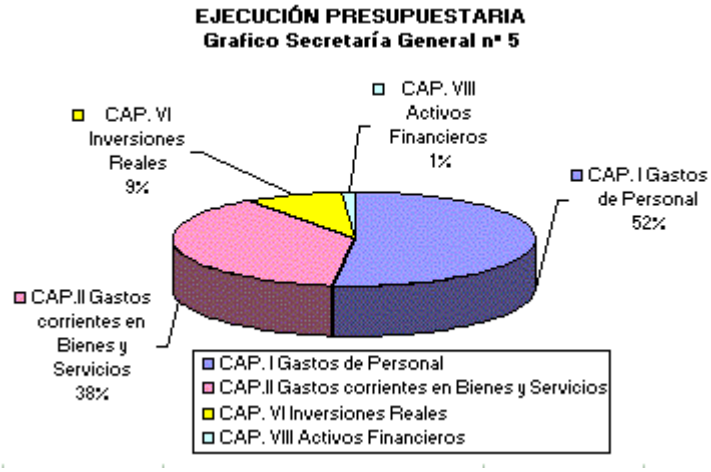
* Ejecución del Plan de Acción Social de la Agencia de Protección de Datos para 1999, así como Aprobación del Proyecto de Plan de Acción Social del Ente Público para 2000, siguiendo las recomendaciones previstas en el Acuerdo de

Administración - Sindicatos sobre condiciones de trabajo en la Función Pública.

2. **GESTIÓN ECONÓMICA Y PRESUPUESTARIA.**

En cumplimento de lo dispuesto en el artículo 34 de la Ley Orgánica 5/92 y en los artículos 30 e), 32, 33, 34, 35 y 36 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia se han llevado a cabo las siguientes tareas y funciones:

* Ejecución y seguimiento presupuestario



* Modificaciones presupuestarias

* La contratación y la gestión presupuestaria y del gasto

* Gestión de los ingresos de la Agencia de Protección de Datos que han tenido su procedencia de transferencias establecidas en los Presupuestos Generales del Estado, venta de disquetes, intereses de cuentas corrientes, así como el pago de las sanciones impuestas por la Agencia en el ejercicio de la potestad sancionadora.

* Contrato de arrendamiento: Se mantiene un contrato de arrendamiento de las plantas 3ª, 4ª, y 5ª del edificio del Paseo de la Castellana nº 41, con una extensión de 1725 metros cuadrados. La duración de dicho contrato expira el 31 de diciembre del año 2000. Se han iniciado actuaciones con la propiedad del edificio para una posible prórroga del contrato de arrendamiento. Al propio tiempo se han mantenido conversaciones y se han dirigido diversos escritos a la Dirección General de Patrimonio y a la Junta Coordinadora de Edificios Administrativos planteando el problema de la futura extinción del contrato de arrendamiento del Ente Público con el ruego de que se realicen todas las gestiones necesarias tendentes a proporcionar a la Agencia un edificio adecuado para el ejercicio de sus funciones. Asimismo se mantiene el contrato de arrendamiento de un pequeño local destinado a almacén y archivo del Ente Público.

* Actualización permanente del inventario de los bienes y derechos que integran el patrimonio de la Agencia.

* Gestión de la Biblioteca de la Agencia: Ha continuado la adquisición de volúmenes y ejemplares para la formación de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales.

3. **OTRAS FUNCIONES Y TAREAS**

_ Notificación de las resoluciones del Director en cumplimiento de lo establecido en el artículo 30, b) del Real decreto 428/1993 de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Total de Notificaciones efectuadas 1.819

- De procedimientos a Administraciones Públicas 139
- De actuaciones previas 566
- De Procedimientos sancionadores 646
- De Tutela de Derechos 468

Estas cifras no tienen porqué coincidir necesariamente con las de expedientes, procedimientos y actuaciones de la Inspección (ver el apartado de la Memoria dedicado a la Inspección de Datos), toda vez que una actuación inspectora habitualmente da lugar a diversas notificaciones por la existencia de una pluralidad de personas que legalmente deben ser notificadas.

_ Registro de Entrada y Salida de documentos en la Agencia

Registros de Entrada 11.920 (incremento del 20.8% respecto 1998)

Registros de Salida 17.206 (incremento del 42.4 % respecto 1998)

Estas cifras son reveladoras del notable incremento de la actividad de la Agencia.

* En el ejercicio de sus competencias, y con el fin de lograr un mejor conocimiento de la ley y tratar en profundidad temas de la mayor actualidad e interés, la Agencia de Protección de Datos ha organizado unas Jornadas sobre "Privacidad, Contratación Electrónica e Internet" en colaboración con el Centro Regional de Extremadura de la UNED, que tuvieron lugar en Mérida los días 1 y 2 de julio de 1999.

En las Jornadas se abordaron los siguientes temas:

* Contratación Electrónica
* Prof. Dr. D. Andrés Recalde. Catedrático de Derecho Mercantil. Universidad de Castellón.
* Seguridad en la Contratación por Internet: Firma Electrónica y Fe Pública.
* Excmo. Sr. D. Juan Bolás Alfonso. Presidente del Consejo General del Notariado.
* Protección de la Propiedad Industrial en Internet.
* Prof. Dr. D. Carlos Lema Devesa. Catedrático de Derecho Mercantil. Universidad Complutense de Madrid
* Legislación Aplicable y Jurisdicción Competente.
* Ilmo. Sr. D. José María Álvarez Cienfuegos Suárez. Magistrado Presidente de la Sala de lo Contencioso-administrativo de la Audiencia Nacional.
* La Protección de la Intimidad.
* Prof. Dr. Francisco Eugenio Díaz. Universidad de Derecho. UNED
* Autorregulación y Códigos Éticos
* Ilmo. Sr. D. Jesús Rubí Navarrete. Adjunto al Director de la Agencia de Protección de Datos.
* Flujo Internacional de Datos.
* Ilmo. Sr. D. Juan Manuel Fernández López **.** Director de la Agencia de Protección de Datos.

* Se ha convocado la **TERCERA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES",** con una dotación de un millón de pesetas, y un accésit dotado de 250.000 pesetas, con la finalidad de profundizar en el estudio del desarrollo del artículo 18.4 de la Constitución. Según las Bases de la Convocatoria el premio se otorgará a la mejor obra científica, original e inédita de autores españoles o extranjeros, que verse sobre la materia de la protección de datos personales informatizados, desde un plano jurídico, ya sea con un enfoque estrictamente teórico o a partir de experiencias concretas basadas en nuestro ordenamiento o en el Derecho Comparado. El Jurado establecido en las Bases de la convocatoria otorgó el Premio a la obra " Protección de los datos de carácter personal relativos a la salud" presentada por la Doctora en Medicina Dª Carmen Sánchez Carazo y el Licenciado en Derecho D. Juan Mª Sánchez Carazo. De la referida obra la Agencia ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional.

La obra premiada aborda las materias y contenidos que se relacionan detalladamente en el apartado de otras actividades de esta memoria.

Se concedió un áccesit, dotado con 250.000 pesetas, a la obra titulada "El Derecho a la autodeterminación informativa. Marco constitucional y europeo", de la que es autora Dª Juana Marí Cardona, Profesora de la Universidad de Barcelona . Se trata de un estudio de interés general de la legislación en materia de protección de datos, que recopila la información existente. Entre los principales temas que aborda cabe destacar el estudio de la configuración constitucional del derecho a la autodeterminación informativa, su desarrollo normativo, las referencias a la Agencia de Protección de Datos o el flujo transfronterizo de datos de carácter personal.

* En cumplimiento del mandato establecido en el artículo 22 del Estatuto de la Agencia la Secretaria General ha actuado como Secretaria del Consejo Consultivo en las 4 reuniones celebradas durante el año 1999. El contenido de las reuniones se concreta en el apartado de la memoria relativo al Consejo Consultivo.

4. **INFORMACIÓN AL CIUDADANO**

La Ley Orgánica 5/92 establece en su artículo 36 apartados d) y e) la función de la Agencia de Protección de Datos de atender las peticiones y reclamaciones formuladas por las personas afectadas y proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de datos de carácter personal. Esta función viene atribuida a la Secretaría General de la Agencia por el artículo 31 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia .

Asimismo en su artículo 4 se dispone que la Agencia de Protección de Datos informará a las personas de los derechos que la Ley les reconoce y a tal efecto podrá promover campañas de difusión, valiéndose de los medios de comunicación social. En cumplimiento de este mandato la Agencia llevó a cabo las siguientes tareas:

4.1. **CAMPAÑA DE PUBLICIDAD EN MEDIOS DE COMUNICACIÓN**

Con la finalidad de difundir la existencia de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal y de las funciones de la Agencia entre los ciudadanos se ha realizado una campaña de información en medios de comunicación, dirigida a concienciar a los ciudadanos de sus derechos frente a una posible vulneración de su intimidad por el tratamiento automatizado de sus datos personales. La campaña institucional ha tenido como destinatarios a los ciudadanos en general y ha consistido en la inserción de anuncios divulgativos en prensa escrita diaria y dominical de máxima difusión en todo el territorio nacional. Esta empresa se ha visto apoyada por una acción informativa consistente en el desarrollo de múltiples actos, ruedas de prensa y entrevistas, dirigidos a los profesionales del mundo de la comunicación, tanto de los medios impresos como de medios audiovisuales y fundamentalmente emisoras de radio. Se ha podido constatar, una vez más, el importante efecto que la campaña ha producido en el número de ciudadanos que se han dirigido a la Agencia no sólo en demanda de mayor información sobre esta materia sino también mediante la presentación de numerosas consultas, demandas de información, reclamaciones o denuncias.

4.2. **CAMPAÑA INFORMATIVA MEDIANTE TRÍPTICOS, MANUALES Y CD ROM**

Además de la campaña de comunicación en periódicos, se ha continuado con la difusión de varios trípticos divulgativos con información general que permita conocer al público los objetivos de la campaña. Su contenido versa sobre información general de la Ley Orgánica, las funciones de la Agencia, ejercicio de los derechos por los ciudadanos, ficheros de morosidad y marketing directo. En estos folletos se trata divulgar de forma simplificada la información elemental en materia de protección de datos. Para su difusión se ha contado, como en años anteriores, con la colaboración del Instituto Nacional de Consumo, Oficinas Municipales de Información al Consumidor, Asociaciones de Consumidores de ámbito Nacional y de ámbito Autonómico y Direcciones Generales de Consumo de las Comunidades Autónomas, así como diferentes asociaciones de consumidores, de vecinos y de colectivos diversos. Asimismo se han entregado a los ciudadanos que se dirigen a la Agencia en demanda de información.

Con el fin de ampliar y complementar el contenido de los trípticos se ha reeditado, introduciendo modificaciones y nuevos modelos, el Manual explicativo del tratamiento automatizado de datos de carácter personal, de la Ley Orgánica 5/92 y de la Agencia de Protección de Datos, dirigido primordialmente a los organismos públicos y privados cuya misión sea la de informar a los ciudadanos de sus derechos en materia de consumo o materias relacionadas con la intimidad y su protección frente al uso indebido de la informática. Se ha entregado también a todos aquellos ciudadanos interesados en la materia.

Asimismo se ha procedido a la reedición y distribución de un Manual sobre Recomendaciones a Usuarios de Internet elaborado por la Agencia. La distribución se ha efectuado fundamentalmente a través de las Oficinas Municipales de Información al Consumidor y otras Organizaciones y Asociaciones de Consumidores, habiéndose hecho también entrega del mismo a los ciudadanos que lo han solicitado.

Igualmente se editado de nuevo un CD ROM el cual, en cumplimiento de la obligación impuesta por el artículo 36 j) de la Ley Orgánica publica el catálogo de los ficheros automatizados de datos de carácter personal inscritos en la el Registro General de Protección de Datos de la Agencia a 3l de mayo de 1999. En el CD Rom se contiene además la siguiente información adicional: estadística del Registro General de Protección de Datos; las memorias de actividad de los años 1994, 1995, 1996, 1997 y 1998; el texto de la conferencia sobre Seguridad, Privacidad y Protección de Datos; el libro de las Jornadas sobre el Derecho Español de la Protección de Datos realizado en octubre en 1996; el trabajo ganador del premio Protección de Datos Personales 1997 y el trabajo ganador del premio Protección de Datos Personales 1998**;** el libro de la XX Conferencia Internacional, así como el manual de Tratamiento de Datos Personales Informatizados y Legislación sobre Protección de Datos.

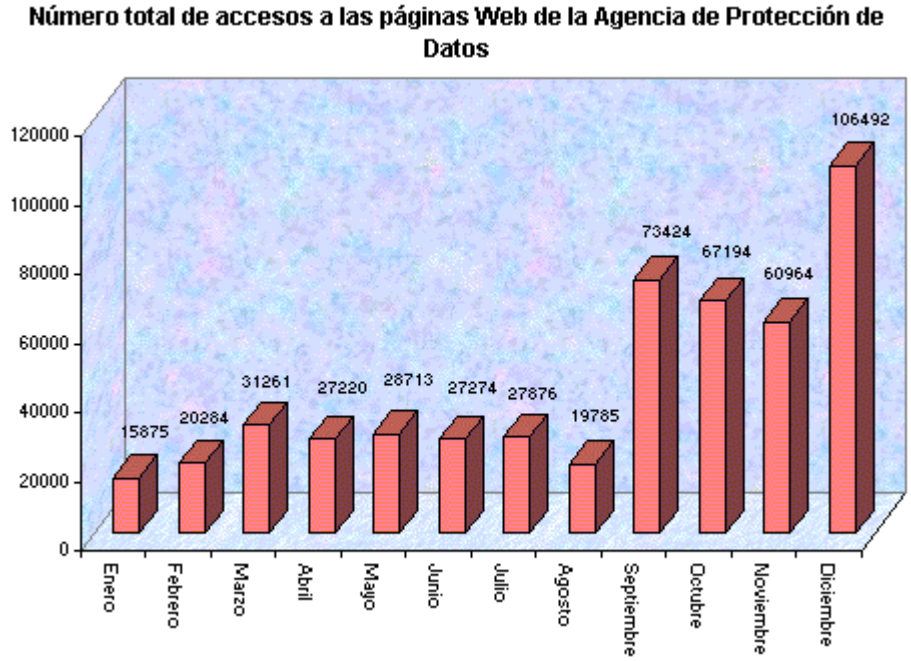
4.3. **INFORMACIÓN A TRAVÉS DE LA PÁGINA WEB DE LA AGENCIA**

Con el fin de lograr una mayor difusión de la existencia y funciones de la Agencia de Protección de Datos, así como de la legislación en materia de protección de datos en general y de los derechos de los ciudadanos en particular, se ha

editado una página web de la Agencia de Protección de Datos con el siguiente contenido:

- Estructura Orgánica de la Agencia de Protección de Datos
- Guía Práctica
- Registro General de Protección de Datos: incluye el catálogo actualizado de ficheros inscritos en el Registro General de Protección de Datos
- Modelos y Formularios, que incluye modelos para el ejercicio de los derechos de los ciudadanos así como para formular denuncias y reclamaciones, y formularios para notificar ficheros de titularidad pública y privada al Registro General de Protección de Datos
- Legislación en materia de protección de datos
- Infracciones
- Recomendaciones sobre Internet

El número de ciudadanos que han accedido a dicha página durante 1999 en cómputo global, fue de un total de 506. 362 accesos. En el gráfico que representa el número de accesos por meses se observa como los accesos se han ido incrementando notablemente a lo largo del año.



5. **EL ÁREA DE ATENCIÓN AL CIUDADANO**

El Área de Atención al Ciudadano desarrolla dentro de la Agencia de Protección de Datos la función de atención personalizada a todos aquellos ciudadanos que o bien acudiendo directamente a las dependencias de la Agencia, o a través del teléfono, o a través del correo ordinario o electrónico, solicitan información sobre la protección de sus datos personales. Por parte del Área se trata de facilitarles la orientación y ayuda que precisen para una mejor defensa de sus derechos, o informarles acerca de los diferentes aspectos que el ordenamiento jurídico de aplicación en esta materia contempla, ordenamiento que durante el periodo al que se circunscribe esta memoria estaba recogido básicamente en la Ley Orgánica 5/1992, Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, si bien en el momento en que la memoria se publique ya habrá entrado en vigor la nueva Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, norma por la que se han tratado de incorporar a nuestro ordenamiento las previsiones contenidas en la Directiva Comunitaria 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

Entrando seguidamente en un detalle estadístico acerca del numero de consultas atendidas a lo largo del año 1999 se indica que, se han contestado 11.500 consultas telefónicas , se han atendido 1.150 consultas presenciales, y se han contestado a un total de 1.739 consultas por escrito. Un primer análisis comparativo de estas cifras implica un posible cambio en la forma de materializarse las consultas, ya que si bien han descendido las consultas telefónicas y presenciales, se observa que se ha incrementado en un 20% las consultas escritas y que dicho incremento se ha debido en parte a la posibilidad de su formalización a través de la página Web de la Agencia.

En efecto, si se compara el número de consultas presentadas a través del correo electrónico durante los años 1998 y 1999, se constata que éstas han pasado de 369 a 654 lo que supone un 77% de incremento Esta cifra implica que

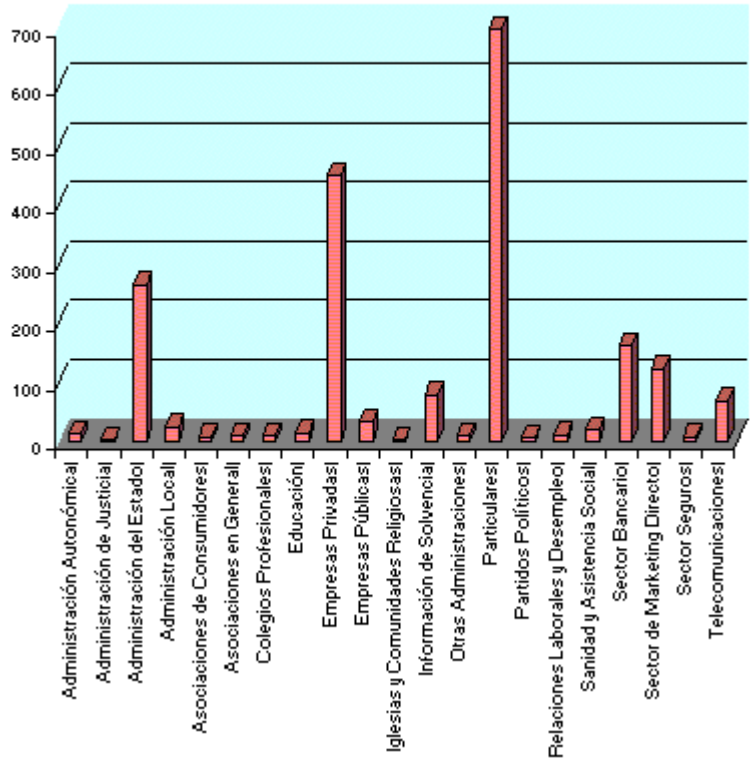
efectivamente se está invirtiendo la forma de acceder a la información por parte de los ciudadanos y ello presumiblemente derivado, entre otros, de dos factores importantes, como son de una parte, la inmediatez del acceso a la información que da el correo electrónico, y de otra, la posibilidad de obtener una respuesta por escrito de una forma rápida a la consulta planteada.

Igualmente se considera importante destacar que, en cómputo global, el acceso por parte de los ciudadanos a la página Web de la Agencia (www.ag-protecciondatos.es), fue de un total de 506.362 accesos, lo que supone un 43% de incremento respecto a 1998.

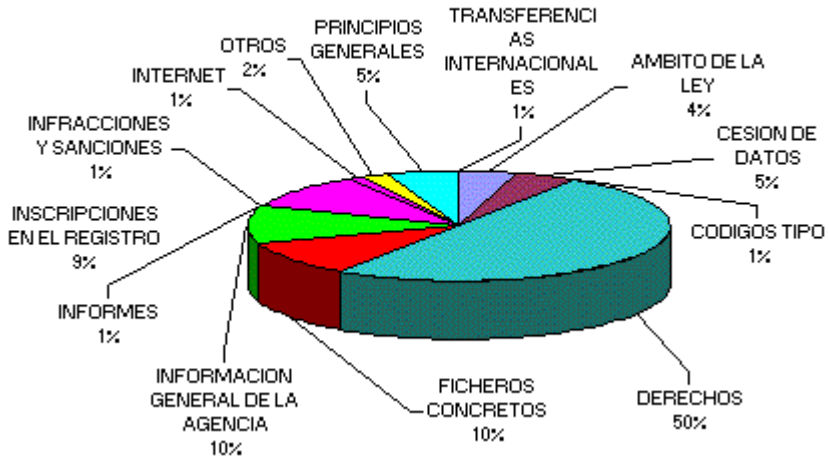
Al igual que en memorias anteriores y dado el interés que las consultas de los ciudadanos pueden plantear a las personas interesadas o destinatarias de la información, y de modo análogo a otras Agencias Europeas, se procede a publicar en esta memoria aquellas consultas que se consideran de mayor importancia, tanto por la frecuencia de la consulta, como por el interés que la cuestión planteada pueda suscitar.

Partiendo de la frecuencia del tipo de preguntas se han clasificado en los cuatro primeros apartados aquellos sectores en los que el ciudadano tiene mas interés y así se contiene el Derecho de información ante la Agencia, los Ficheros de Información de Solvencia Patrimonial y Crédito, los Ficheros de Publicidad, y el ejercicio de los Derechos de Acceso, Rectificación y Cancelación ante los responsables del fichero. A continuación se tratan consultas especiales clasificadas igualmente por sectores en función de su especial singularidad y así se han clasificado por Ámbito de aplicación de la Ley; Ficheros Policiales; Relaciones Laborales; Telecomunicaciones; Datos de Salud; Datos del Censo Electoral; Datos Estadísticos; Cesión de Datos; Colegios Profesionales; Seguros; y, finalmente las consultas derivadas de la entrada en vigor del Reglamento de Medidas de Seguridad

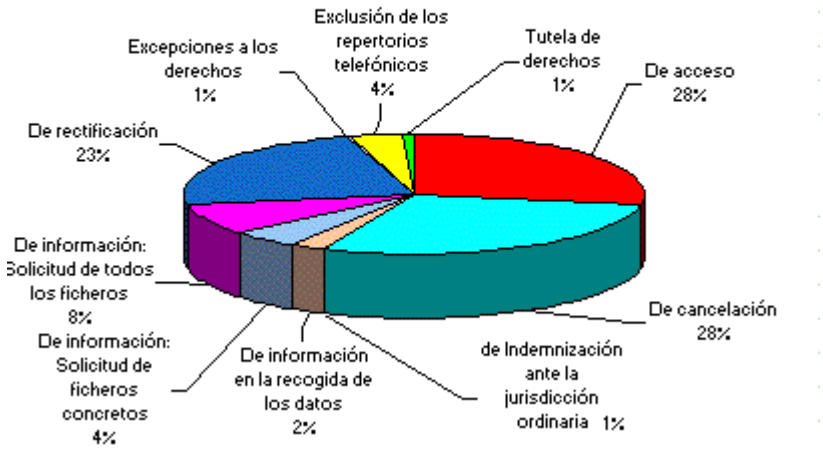
CONSULTA POR SECTORES 1999
Gráfico Secretaría General nº 7



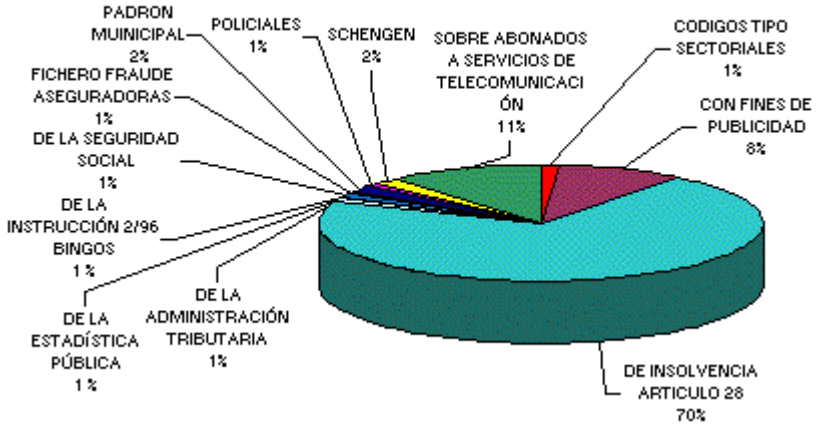
CONSULTAS POR TEMAS 1999
Gráfico Secretaría General nº 8



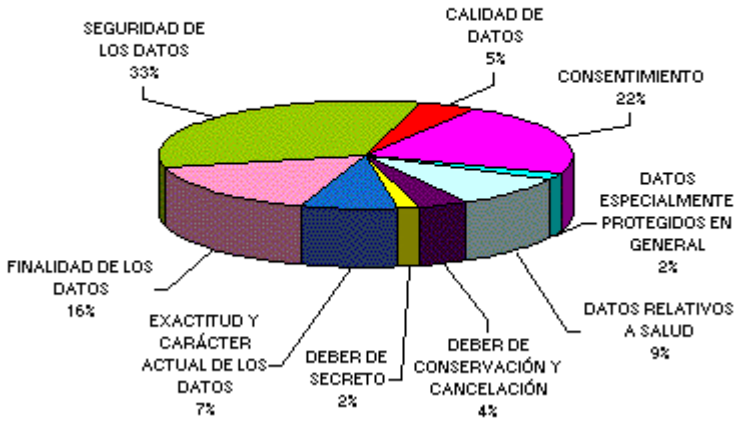
TIPOS DE CONSULTAS SOBRE DERECHOS 1999
Gráfico Secretaría General nº 9

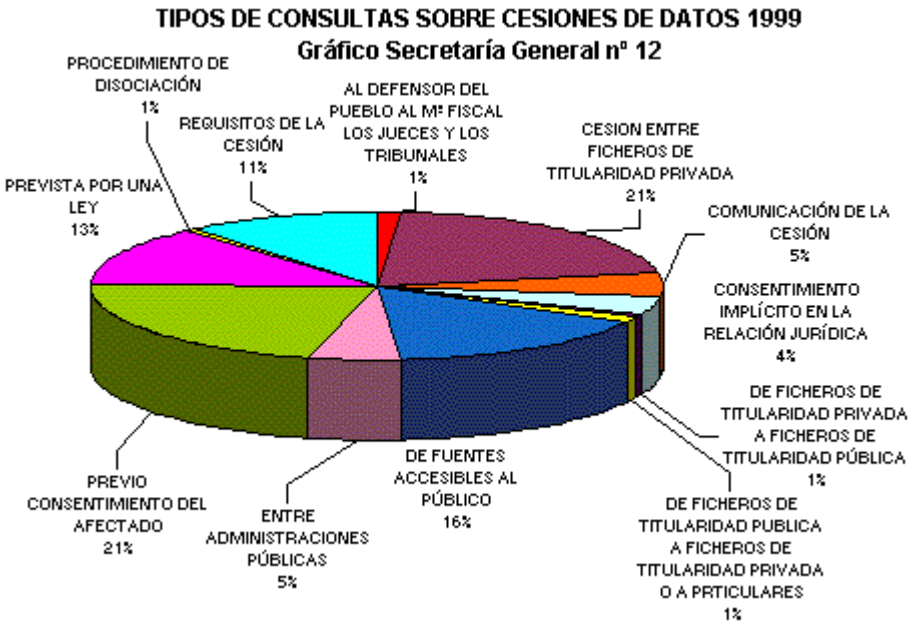


CONSULTAS SOBRE FICHEROS CONCRETOS 1999
Gráfico Secretaría General nº 10



CONSULTAS SOBRE PRINCIPIOS GENERALES 1999
Gráfico Secretaría General nº 11





5.1. **EL ALCANCE DEL DERECHO DE INFORMACIÓN ANTE LA AGENCIA DE PROTECCIÓN DE DATOS**

Bajo este epígrafe se quiere poner de relieve las quejas que por parte de los ciudadanos se plantean cuando desde la Agencia se les informa que no se dispone en ningún caso de datos personales de ningún ciudadano.

El ciudadano, en general, no entiende que cuando se está dirigiendo a la Agencia para que se le indique en que ficheros figuran sus datos, se le informe que en virtud de la legislación vigente en esta materia, la Agencia de Protección de Datos no dispone de los datos de las personas incluidas en los ficheros inscritos, sino tan sólo información relativa a la descripción de dichos ficheros, su finalidad, servicios o unidades ante los que se pueden ejercer los derechos de acceso, rectificación y cancelación, así como los responsables de los mismos; y por lo tanto, no se le puede informar qué empresas tienen sus datos.

Se les informa por la Agencia que tan sólo se puede suministrar la dirección de la oficina designada por el responsable o titular del fichero, de aquellas entidades o personas de las que el ciudadano lo solicite de manera individualizada bien por tener el conocimiento a ciencia cierta de que poseen datos personales suyos, o bien de que presumiblemente los tienen, para que con esta información se pueda dirigir personal y directamente a cada una de las empresas que le remiten información, utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud, acompañando copia de su DNI, solicitando le informen qué datos tienen, cómo los han obtenido y, en su caso, la cancelación o rectificación de los datos en sus ficheros.

5.2. **FICHEROS SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO**

Respecto a las consultas planteadas sobre estos ficheros se indica en primer lugar que al igual que en años anteriores nos encontramos frente al grupo más numeroso de las consultas formuladas por los ciudadanos a esta Agencia, tanto en lo que se refiere al derecho de información sobre la identidad del responsable, como en relación con los derechos de acceso, rectificación y cancelación, y en especial este último, dado que al ciudadano lo que le preocupa fundamentalmente es la forma de no figurar en este tipo de ficheros.

Este tipo de consultas implica una mayor dedicación por parte del Área para intentar explicar al ciudadano que con carácter general el funcionamiento de este tipo de ficheros es legal y que así está previsto en el artículo 28 de la LORTAD, dado que sirve para un mejor funcionamiento del tráfico mercantil basado en el crédito personal en su sentido más amplio, lo que justifica la existencia de este tipo de ficheros.

En este sentido se destaca que la preocupación del ciudadano al estar incluido en un fichero de estas características es de una importancia considerable en la vida financiera de las personas, dado que, como consecuencia de esta inclusión, se puede producir una restricción importante en las posibilidades de acceso a cualquier tipo de crédito. Ello revierte en la demanda de información a la Agencia sobre si esta práctica es conforme o no a derecho, centrándose la información facilitada en dos apartados fundamentalmente que se analizan a continuación, como son, la obligación por parte del responsable del fichero de información de solvencia de notificar al ciudadano afectado la inclusión en el fichero, así como la forma en que se puede formalizar el ejercicio de los derechos de acceso, rectificación y cancelación, distinguiendo que, en estos casos, hay ocasiones en que no se cancelan totalmente los datos sino que se permanece con el saldo pagado o saldo "0".

También se señala que a menudo y al igual que en años anteriores se han recibido consultas como consecuencia de la inclusión de personas jurídicas en estos ficheros. La Agencia de Protección de Datos, en este aspecto, carece de competencia para actuar, y así se informa a las empresas que reclaman o denuncian esta actuación, en el sentido de que la Ley Orgánica 5/1992 Reguladora del Tratamiento Automatizado de Datos de Carácter Personal limita su actuación a las personas físicas identificadas o identificables, quedando fuera de su ámbito de aplicación las personas jurídicas.

5.2.1. ***Información sobre el alcance del deber de comunicación del artículo 28.***

En relación con este asunto se trata de informar que en este tipo de ficheros quiebra el principio general de la Ley consagrado en sus artículos 6 y 11, que exigen el consentimiento del afectado para el tratamiento y la cesión de sus datos personales. Se sustituye la necesidad del consentimiento previo informado por la obligada notificación posterior de los datos más relevantes de dicha inclusión, con un doble objetivo: por una parte, informar al ciudadano de la inclusión, dada la gran trascendencia que la misma tiene para sus derechos; por otra, dar al ciudadano la posibilidad de rectificar y cancelar dichos datos en el caso de que sean erróneos. La primera garantía establecida por la Ley Orgánica, es la obligación de comunicar al afectado su inclusión en esta clase de ficheros, para que, con este conocimiento, el mismo pueda oponerse a su inclusión, solicitando la cancelación o rectificación en su caso.

La información que se proporciona al ciudadano en esta materia se puede resumir en los siguientes puntos:

* La obligación de comunicar la inclusión en estos ficheros se extiende tanto a los supuestos de información sobre solvencia patrimonial y crédito, como a la información relativa al cumplimiento o incumplimiento de obligaciones dinerarias, con independencia del origen de los datos. Esta obligación se ha visto modificada por la Ley orgánica 15/1999, que en su artículo 29 limita la obligación de notificar al ciudadano la inclusión en el fichero de sus datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitadas por el acreedor o por quien actúe por su cuenta o interés. No obstante en el artículo 5.4 se impone la obligación de notificar a los afectados en el plazo de tres meses, desde el momento del registro de sus datos, cuando los mismos no hayan sido recabados del propio afectado.
* La notificación de la inclusión de datos personales en el fichero se efectuará en el plazo máximo de 30 días, informando al afectado de su derecho a recabar información sobre los datos recogidos en el fichero.
* La inclusión en el fichero común de la obligación incumplida, se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan, señalando la fecha de cada uno de ellos.
* Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.
* El responsable del fichero deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y la fecha de entrega o intento de entrega de la misma.
* La notificación se dirigirá a la última dirección conocida del afectado a través de un medio fiable e independiente del responsable del fichero.

5.2.2. ***Ejercicio de los derechos de acceso, rectificación y cancelación en relación con los ficheros de solvencia patrimonial y crédito***

Se han realizado frecuentes consultas sobre las actuaciones necesarias ante la inclusión de datos personales en un fichero de morosidad o impagados cuando no se conoce la identidad concreta del responsable del fichero de impagados al que se deben dirigir.

Se informa que, el derecho de acceso puede ejercerse bien ante el propio fichero de información sobre solvencia o bien ante todas aquellas personas o entidades bancarias o de financiación que tienen acceso o conocimiento de datos relativos a solvencia patrimonial y crédito, que tienen la obligación de informar al afectado sobre toda la información de que la entidad dispone sobre su persona.

Si se conoce el nombre del fichero se puede dirigir a la Agencia bien por teléfono o bien por escrito o utilizando la página Web, para solicitar la dirección del responsable del fichero y poder ejercer el derecho de acceso. En ambos supuestos el responsable del fichero al que se solicitan los datos, debe contestar en el plazo de un mes.

Si como consecuencia del ejercicio del derecho de acceso, se constata que los datos de carácter personal incluidos en este tipo de ficheros resultan inexactos o incompletos, dichos datos deberán ser rectificados o cancelados en su caso.

Para solicitar la rectificación o la cancelación, se informa que podrán dirigirse al acreedor que ha facilitado los datos para que por su parte se realicen las actuaciones correspondientes con el responsable del fichero de solvencia y se rectifiquen o cancelen los datos. Asimismo, puede dirigirse directamente al responsable del fichero de solvencia aportando un principio de prueba suficiente que contradiga esta inclusión, en cuyo caso se trasladará al acreedor para que resuelva. Una vez resuelta por éste, o si transcurridos cinco días desde que se le comunicó no ha resuelto nada, el responsable del fichero procederá a la rectificación o cancelación cautelar del dato.

La Ley Orgánica 15/1999 ha modificado el plazo para hacer efectivos los derechos de rectificación y cancelación, que han pasado de cinco a diez días.

En todo caso el ejercicio de estos derechos es personalísimo lo que justifica que los responsables de estos ficheros exijan a los afectados una acreditación suficiente de su identidad, lo que se cumple habitualmente con la presentación

del DNI.

5.2.3. **Saldo pagado o saldo cero**

En estos supuestos se ha informado que en virtud del artículo 28 de la Ley Orgánica se puede incluir en esta clase de ficheros al deudor siempre que lo comunique el acreedor o su representante legal.

La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, a los que hace relación el mencionado artículo 28, deberá efectuarse cuando exista una deuda **cierta, vencida y exigible**, que haya resultado impagada. El tiempo que se puede permanecer en este tipo de ficheros es de seis años.

Si la deuda ya se ha pagado, pero con retraso, el responsable del fichero de solvencia podrá mantener el dato rectificado y desfavorable hasta un máximo de seis años contados a partir del impago de la deuda. No obstante, la deuda debe estar actualizada, por lo que si ya ha saldado la misma, deberá constar en el fichero pero con saldo cero.

5.3. **PUBLICIDAD DIRECTA**

Este es el tercer sector que continua teniendo un número importante de consultas y quejas por parte de los ciudadanos. La petición más frecuente manifestada ante la Agencia es el deseo de no recibir información comercial. Se han recibido quejas frecuentes y solicitudes de información en relación con la publicidad nominativa no solicitada y remitida por empresas con las que el afectado carece de relación previa.

En estos casos la queja mas común es debida a que no se entiende que una vez recibida la publicidad tengan que ser los ciudadanos los que directa y personalmente deben dirigirse a las empresa que les envían la misma para que les cancelen sus datos, considerando que debería ser la Agencia la que tutelase directamente sus derechos sin necesidad de su intervención. Se les informa que el ejercicio de los derechos reconocidos en la Ley Orgánica se debe llevar a cabo directamente por sus titulares ante cada uno de los responsables de los ficheros automatizados conforme determinan los artículos 14 y 15 de la Ley Orgánica, por lo que deben dirigirse a cada una de las empresas que le remiten publicidad solicitando información sobre qué datos tienen y cómo los han obtenido y, en su caso, la cancelación de los datos en sus ficheros. En el supuesto de no satisfacerse este derecho por el responsable del fichero podrá el ciudadano solicitar la intervención de la Agencia para tutelar su derecho.

Asimismo, y en esta materia, se les informa que los datos personales pueden obtenerse, entre otras fuentes, de los repertorios telefónicos ya que estos tienen la consideración de fuente accesible al público, por lo que pueden recabarse, tratarse y cederse sin el consentimiento de las personas afectadas.

El artículo 26 de la Ley Orgánica, a la vez que reconoce la facultad de las empresas que presten servicios de telecomunicación de utilizar los datos sobre sus abonados y determina que los números de los teléfonos y demás servicios de telecomunicación, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, tanto en formato papel como electrónico (paginas blancas, Servicios Electrónicos de Telecomunicación etc.,.), reconoce el derecho al afectado de exigir su exclusión, en el caso de que no desee aparecer en dichos repertorios.

Hay que destacar que datos como los que proporcionan los referidos repertorios pueden ser utilizados legalmente por empresas de publicidad. Este servicio contiene el nombre completo y dirección de los abonados. Debe ser el afectado el que manifieste su oposición o exclusión, y esta negativa tendrá como resultado una importante disminución de la publicidad nominativa que recibe.

Se recomienda que en consecuencia se ejercite el derecho de exclusión de los repertorios de abonados de Telefónica y otras empresas del sector de la telefonía, que tienen el carácter de fuente accesible al público, y de acuerdo con el artículo 29, pueden ser utilizados con fines de publicidad.

Una vez ejercido el derecho de que se trate ante el responsable del fichero sin que éste actúe adecuadamente, el afectado se podrá dirigir a la Agencia solicitando la tutela de sus derechos. Todo ello sin perjuicio de las correspondientes actuaciones si se estima que el origen de los datos era ilegal.

5.3.1. ***Publicidad directa a través de Internet***

Dentro del apartado merece especial mención la publicidad directa enviada a través de Internet, en la que las direcciones se obtienen a través de los accesos realizados por los usuarios a las diferentes páginas Web, o en cualesquiera otros servicios disponibles en la red: correo electrónico, listas de distribución, grupos de noticias, foros de discusión . A este respecto, hay que tener en cuenta las Recomendaciones sobre Internet que ha publicado la Agencia y que se vienen facilitando a todos los ciudadanos que plantean alguna consulta sobre este aspecto.

Se informa que la dirección de correo es la forma más común de registrar la "identidad" de una persona en Internet. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección se utiliza en múltiples lugares de la red y puede ser conseguida fácilmente sin conocimiento del afectado. Sin embargo, su aspecto más preocupante radica en que sirva de base para la confección de perfiles personales (temas de interés, inclinaciones políticas, orientaciones sexuales, etc.) a partir de la pertenencia a listas de distribución, o basándose en la participación en grupos de discusión, corriendo el riesgo de ser etiquetados por la pertenencia a los mismos.

El envío de publicidad no solicitada a través del correo electrónico requiere, lógicamente, el conocimiento de la dirección de correo electrónico del receptor del mensaje. Adicionalmente, una dirección de correo electrónico puede tener asociada información de carácter personal, tal como la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa que se dedique a la publicidad directa. Las formas más habituales de obtener direcciones de correo sin el conocimiento del usuario son:

* Listas de distribución y grupos de noticias.
* Captura de direcciones en directorios de correo electrónico.
* Venta, alquiler o intercambio de direcciones de correo por parte de los proveedores de acceso.
* Entrega de la dirección de correo, por parte de los programas navegadores, al conectar a los servidores Web.
* Recepción de mensajes de correo requiriendo contestación a una dirección determinada y pidiendo la máxima difusión de los mismos.

La Agencia recomienda a este respecto que cuando se incluya la dirección de correo electrónico en un directorio o lista de distribución, se considere la posibilidad de que la misma pueda ser recogida por terceros para enviar mensajes publicitarios no deseados. También conviene conocer la política de alquiler, venta o intercambio de datos que han adoptado tanto el proveedor de acceso a Internet como los administradores de los directorios y listas de distribución donde esté incluido.

Si no se quiere dar difusión a la dirección de correo electrónico, es necesario configurar el navegador para que no deje su dirección de correo en los servidores Web a los que accede.

Por último conviene destacar que se han producido un número considerable de peticiones tanto de las Recomendaciones de Internet, como del Código Etico de protección de datos en Internet inscrito en la Agencia.

5.4. **DERECHOS DE ACCESO, RECTIFICACION Y CANCELACION**

Se quiere reflejar este apartado independientemente, dado que es precisamente una de las materias principales del Área en cumplimiento de lo dispuesto en el artículo 36 de la Ley Orgánica.

En primer lugar conviene señalar que este tipo de consultas son las que en cómputo global han supuesto el mayor número de las presentadas por escrito ante la Agencia ya que durante 1999 se han presentado 445 consultas sobre el derecho de acceso, 461 consultas sobre derecho de cancelación y 375 sobre derecho de rectificación, que sumadas ascienden a un total de 1281. En este punto conviene precisar que la suma de consultas por derechos no coincide con el total porque una misma consulta puede planear consultas sobre distintos derechos y sobre diferentes temas.

Con carácter general se recoge a continuación la información que se facilita cuando se plantean estas consultas. Se viene a indicar que la Ley Orgánica reconoce una serie de derechos a los ciudadanos, como son el derecho de acceso, rectificación y cancelación de sus datos personales. El ejercicio de los mismos es personal, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables/titulares de los ficheros automatizados, lo que significa que pueden dirigirse a cada una de las empresas u organismos públicos, de los que saben o presumen que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación). Deberán dirigirse directamente al responsable del fichero utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud, para el ejercicio de sus derechos, acompañando copia de su D.N.I. para acreditar su personalidad.

Se informa que si en el plazo de un mes para el derecho de acceso y de cinco días (diez días en la nueva Ley Orgánica 15/1999) para los derechos de rectificación y cancelación desde la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, se podrán dirigir a la Agencia con copia de la solicitud cursada, para que ésta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de sus derechos.

Junto con la información anterior se acompañan al ciudadano los modelos confeccionados por la Agencia para el ejercicio de estos derechos.

5.5. **ÁMBITO DE APLICACIÓN DE LA LORTAD**

Se han producido con relativa frecuencia, consultas de ciudadanos en relación con el ámbito de aplicación de la Ley Orgánica, en concreto 140, de las que se destacan cuatro dada su especial singularidad. Se refieren, la primera, a la inclusión en un fichero de información de solvencia patrimonial y crédito de datos relativos a una deuda derivada de un contrato de Leasing; la segunda al registro en una base de datos de aquellos datos referidos al gerente de una empresa; la tercera a la forma de obtener mediante operaciones automáticas el Número de Identificación Fiscal; y, la cuarta a la exclusión del ámbito de aplicación de la Ley en los casos de tratarse de datos de empresa.

5.5.1. ***Datos derivados de un contrato de Leasing***

En este caso se informó al ciudadano que a la vista de que la deuda que motiva la inclusión de sus datos en el fichero derivaba de un crédito obtenido en una operación de Leasing mobiliario, había que precisar previamente que la disposición adicional 7ª.1 de la LEY 26/1988 de 29 de julio, de Disciplina e Intervención de las entidades de crédito dispone que: "*Tendrán la consideración de operaciones de arrendamiento financiero aquellos contratos que tengan por objeto exclusivo la cesión del uso de bienes muebles o inmuebles, adquiridos para dicha finalidad según las especificaciones*

del futuro usuario, a cambio de una contraprestación consistente en el abono periódico de las cuotas a que se refiere el número 2 de esta disposición. Los bienes objeto de cesión habrán de quedar afectados por el usuario únicamente a sus explotaciones agrícolas, pesqueras, industriales, comerciales, artesanales, de servicios o profesionales. El contrato de arrendamiento financiero incluirá necesariamente una opción de compra, a su término, en favor del usuario".

En consecuencia, debía entenderse que la operación de Leasing que dió lugar al impago que se anotó en el fichero de información de solvencia tan sólo podía derivarse de una actividad empresarial, o bien de una actividad ejercida como profesional liberal, por lo que en principio los datos se refieren a esta actividad y no a la propia intimidad de la persona física en cuanto tal, no siendo de aplicación, en consecuencia, lo previsto en la Ley Orgánica 5/1992 que, de acuerdo con lo establecido en su artículo 1, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. Este criterio deberá ser revisado con la entrada en vigor de la Ley Orgánica 15/1999 dada la ampliación de su objeto que se contiene en su artículo 1.

5.5.2. ***Inclusión de datos correspondientes a administradores, gerentes etc. de las empresas***

Se planteaba si un fichero de una empresa que contiene los datos de sociedades y empresas clientes con el nombre y apellidos de su gerente o persona de contacto dentro de la empresa, se considera como un fichero que contiene datos de carácter personal y por tanto debe inscribirse en el Registro General de Protección de Datos.

La información facilitada consistió en indicar que la Constitución Española delimita el ámbito de protección de la Ley, al establecer en el artículo 18.4 que: La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. De forma idéntica, el artículo primero de la LORTAD establece como objeto la protección de los citados derechos de las personas físicas.

De dichos preceptos se deduce claramente que la protección de la "privacidad" conferida por la LORTAD no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran exigirse en el caso de que el uso de información relativa a las empresas les cause algún perjuicio.

El fundamento de la delimitación de este ámbito de aplicación reside en que si la protección de los datos personales se refiere a la intimidad personal y familiar, no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, en principio no puede ser aplicable a esas personas la protección, ni siquiera cuando su actividad se identifique plenamente con la de una persona física determinada, habida cuenta que el ámbito personal que se protege debe entenderse distinto del empresarial.

En consecuencia, si los datos que se van a utilizar para enviar la documentación se corresponden con los de los Administradores, Gerentes o cualquier otro cargo de la Sociedad que conste en el Registro Mercantil, en principio dichos datos no se consideran como de personas físicas y quedarán fuera del ámbito de aplicación de la Ley Orgánica 5/1992. Ahora bien, si se utilizan los datos de cualquier otra persona de la empresa fuera de estos cargos, sí habría que considerarlo dentro del ámbito de aplicación y en consecuencia la base de datos que se utilizase con estos datos debería ser notificada a la Agencia para su inscripción en el Registro de Protección de Datos.

Este criterio deberá ser revisado con la entrada en vigor de la Ley Orgánica 15/99, cuyo artículo 1º define un ámbito más amplio que el de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, al señalar que *"la presente ley orgánica 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"*. Con esta nueva redacción, en la que se amplía el objeto de la ley, se deberá entender que si los datos que se van a utilizar para enviar documentación o publicidad se corresponden con los nombres de los administradores, gerentes, así como el de cualquier persona de La empresa será necesario, en todo caso, recabar su consentimiento. Así lo establece el artículo 6.1 de la Ley Orgánica 15/99, conforme al cual el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

5.5.3. ***Obtención del N.I.F.***

En esta consulta se plantea que a través de una página Web e indicando el DNI se calculaba, previa la realización de unas operaciones automáticas, el numero de identificación fiscal.

En este caso se informó que la Agencia de Protección de Datos tiene por principal tarea el velar por el cumplimiento de la Ley Orgánica 5/1992, norma que tiene por objeto en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

De conformidad con lo previsto en el artículo 2 de dicha Ley la misma será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores públicos y privados y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

Un vez señalado el objeto y el ámbito de aplicación se concluyó que de la consulta planteada no se desprendía ni que

se traten en ningún caso datos personales de nadie, ya que no son identificados o identificables, ni que se recojan informatizadamente en ningún fichero, sino que lo único que se realiza es un cálculo para la conversión de un número en otro, por lo que en principio quedaría fuera del ámbito de aplicación de la Ley.

5.5.4. ***Exclusión por persona jurídica***

Con cierta frecuencia las empresas han enviado escritos de reclamación o denuncia solicitando el amparo y protección de la Agencia respecto de los datos de las propias empresas, señalando que en todos estos casos se ha informado, con carácter general, que la Agencia de Protección de Datos no tiene competencia sobre la cuestión formulada, ya que la legislación vigente en la materia, en concreto la Ley Orgánica 5/1992, únicamente afecta a los datos relativos a personas físicas, y no a personas jurídicas y así lo regula en su artículo 1. " *La presente Ley Orgánica 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".*

5.6. **FICHEROS POLICIALES**

Dentro de este apartado y aunque este año las consultas referidas a este tipo de ficheros no han sido tan frecuentes, sí se quiere destacar una de las realizadas, habida cuenta que en ella se estaba planteando hasta que punto se pueden tratar datos como las huellas dactilares, fotografías y datos antropométricos y físicos de las personas investigadas.

El ciudadano en su escrito venía a plantear su disconformidad con el tratamiento de determinados datos personales suyos por parte de Fuerzas y Cuerpos de Seguridad.

Se le informó, en primer término, que el artículo 20 de la Ley Orgánica 5/1992 permite a las Fuerzas y Cuerpos de Seguridad del Estado el recabar y tratar datos de carácter personal sin el consentimiento de las personas afectadas siempre que sea para la represión de infracciones penales, debiendo ser cancelados dichos datos cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento.

Se le puso igualmente de relieve que, la Ley no distingue en estos casos que datos personales pueden ser recabados y tratados y cuáles no, por lo que en consecuencia habrá que atender a la definición de datos de carácter personal que la propia Ley dentro de su artículo 3 contempla, y así los define como "cualquier información concerniente a personas físicas identificadas o identificables". Esta definición anterior queda completada de una forma más amplia en el Real Decreto 1332/1994, de 20 de junio que desarrolla determinados artículos de la Ley Orgánica 5/1992, estableciendo en su artículo 1, apartado 4 que, dato de carácter personal será: "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable".

Por otra parte, parece desprenderse de la consulta que, la investigación policial versa sobre un presunto delito de falsificación en documento público, señalándole que el Código Penal lo regula en su articulo 392 estableciendo que: "El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses."

A la vista de la regulación anterior y del contenido de la consulta, se deduce que se estaba investigando un presunto delito de falsedad en documento público, y en este sentido dentro de las actuaciones de dicha investigación, utilizó las que la propia Ley Orgánica le permite en su artículo 20, recogiendo de las personas investigadas, entre las que se encontraba la persona que plantea la consulta, sus datos personales, entre los que pueden quedar incluidos ya que no se excluyen en las definiciones anteriores, las huellas dactilares, fotografías y datos antropométricos y físicos. Se informó que de dicha actuación en principio y tal y como se planteó no se desprendía que existiese una vulneración a la Ley Orgánica.

No obstante se le reiteró que podía ejercitar el derecho de cancelación de sus datos y si dicho derecho se le denegase total o parcialmente sin motivación podrá ponerlo en conocimiento de esta Agencia de conformidad con lo previsto en el articulo 21 de la LORTAD, a los efectos de que se tutelen sus derechos.

5.6.1. ***Acceso y cancelación de datos en los ficheros del Sistema de Información de Schengen***

Han existido durante 1999, al igual que en 1998, una serie de consultas sobre la forma de acceder y cancelar datos personales del Sistema de Información de Schengen.

Se ha informado que el acuerdo de adhesión del Reino de España al Convenio de aplicación del acuerdo de Schengen de 14 de junio de 1985, regula esta materia. En concreto en el Título IV, sobre el Sistema de información de Schengen establece en su Capítulo III la protección de los datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen. Así el artículo 109 del citado Convenio reconoce:

1. El derecho de toda persona a acceder a los datos que se refieran a ella y estén introducidos en el Sistema de Información de Schengen se ejercerá respetando el Derecho de la Parte contratante ante la que se hubiere alegado tal derecho. Si el Derecho nacional así lo prevé, la autoridad nacional de control prevista en el apartado 1 del artículo 114 decidirá si se facilita información y con arreglo a qué modalidades. Una Parte contratante que no haya realizado la descripción no podrá facilitar información relativa a dichos datos, a no ser que previamente hubiere dado a la Parte contratante informadora la ocasión de adoptar una posición.

2. No se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada en la descripción o para la protección de los derechos y libertades de terceros. Se denegará en todos los casos durante el período de descripción con vistas a una vigilancia discreta.

Por su parte, el Artículo 110 del mismo Convenio establece que toda persona podrá hacer rectificar datos que contengan errores de hecho que se refieran a ella o hacer suprimir datos que contengan errores de derecho que se refieran a ella. Por último, en el artículo 114 se establece que:

1. Cada Parte contratante designará a una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre el fichero de la parte nacional del Sistema de Información de Schengen y de comprobar que el tratamiento y la utilización de los datos introducidos en el Sistema de Información de Schengen no atentan contra los derechos de la persona de que se trate. A tal fin, la autoridad de control tendrá acceso al fichero de la parte nacional del Sistema de Información de Schengen.

2. Toda persona tendrá derecho a solicitar a las autoridades de control que comprueben los datos referentes a ella integrados en el Sistema de Información de Schengen, así como el uso que se haga de dichos datos. Este derecho estará regulado por el Derecho nacional de la Parte contratante ante la que se presente la solicitud. Si los datos hubieran sido integrados por otra Parte contratante, el control se realizará en estrecha colaboración con la autoridad de control de dicha Parte contratante.

La legislación nacional vigente en España en materia de protección de datos es la Ley Orgánica 5/92. Esta ley reconoce una serie de derechos a los ciudadanos, como son el derecho de acceso, rectificación y cancelación de sus datos personales. El ejercicio de los mismos es personal, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables de los ficheros automatizados, lo que significa que el solicitante debe dirigirse al organismo público responsable del fichero, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación). También se pueden ejercer estos derechos a través de representantes legales debidamente acreditados y apoderados.

Para la resolución del problema planteado, es necesario dirigirse en primer lugar a la Secretaría de Estado de Seguridad del Ministerio de Interior, responsable del fichero en España, exponiendo el problema. En la petición se debe hacer referencia al ejercicio de los derechos de acceso, rectificación y cancelación en relación con el fichero NSIS/ SIRENE**.** Este fichero tiene por finalidad la gestión nacional para el sistema de información de Schengen.

En el caso de que la petición sea desatendida, podrá entonces dirigirse el afectado, o su representante legal a la Agencia de Protección de Datos, que es la autoridad de control sobre este fichero en España. Si en el plazo de un mes para el derecho de acceso y de cinco días para los derechos de rectificación y cancelación desde la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, nuevamente también podrá dirigirse a la Agencia con copia de la solicitud cursada, para que ésta, a su vez, se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de sus derechos.

5.7. **RELACIONES LABORALES**

El ámbito de las relaciones laborales implica a un entramado complejo de sujetos: el empresario, el trabajador, las asociaciones de empresarios, los sindicatos o las Administraciones Públicas. En los ficheros automatizados de personal de las empresas está contenida una gran cantidad de información relativa a los trabajadores, que incluye, tanto datos relativos a la vida profesional de los mismos, titulación, puestos desempeñados, retribuciones, como otros relativos a la vida familiar como el estado civil o el número de hijos. También y sin abandonar la vida estrictamente laboral, nos encontramos ante otros datos especialmente protegidos como los datos de salud contenidos en las bajas laborales, enfermedades profesionales, etc. o, incluso, datos relativos a ideología, como la afiliación sindical para el descuento de las cuotas sindicales.

En este apartado se recogen las consultas relativas a la utilización de los datos de carácter personal en el ámbito de las relaciones de trabajo dependientes, señalando que durante 1999 ha destacado la preocupación por parte de los empleados en el sentido de hasta que punto el empresario puede acceder a la información contenida en los ordenadores personales puestos a disposición de los trabajadores.

5.7.1. ***Acceso por parte del empresario a los correos electrónicos de sus trabajadores***

En este sentido se han planteado varias consultas relativas a si sería legal que una empresa estableciese, respecto de sus empleados, un control para acceder, leer, copiar o divulgar los e-mail, archivos electrónicos, u otras grabaciones de ordenador, creadas, recibidas o almacenadas a través del uso que sus trabajadores hacen de los ordenadores de la empresa.

En contestación a esta consulta se indicó, en primer lugar que, dejando a salvo que con carácter general la Constitución Española garantiza en su artículo 18.3 el secreto de las comunicaciones y en especial las postales, telegráficas y telefónicas salvo resolución judicial, el Tribunal Constitucional en su sentencia de 22 abril 1993 dictada en Recurso de amparo núm. 190/1991, excluye del ámbito de la intimidad, constitucionalmente amparado, a "los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada".

En este mismo sentido se informó que el artículo 20 del Estatuto de los Trabajadores regula la dirección y control de la actividad laboral por parte de la empresa estableciendo que :

" 1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue.

2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe....."

De conformidad con esta regulación se indica que, las actuaciones por parte del empresario en el ámbito laboral pueden limitar los derechos fundamentales de los trabajadores. El empresario tiene, en principio, la potestad de controlar el cumplimiento de las obligaciones laborales, así como el uso profesional de los instrumentos de trabajo, como el uso del ordenador y de Internet y, en consecuencia, este uso debe quedar afectado a la propia actividad laboral del trabajador.

El problema estribaría en determinar hasta donde llegan las facultades de dirección del empresario para que el derecho fundamental reconocido en el artículo 18.3 CE no sufra una merma de su contenido esencial, sin que, por otra parte, el derecho al trabajo, consagrado en el articulo 35 CE, pueda verse en peligro al eliminarse uno de los componentes esenciales de la relación laboral, cual es el derecho de vigilancia y control que corresponde al empresario. Todo ello en el bien entendido de que la celebración de un contrato de trabajo no puede implicar la privación al trabajador de sus derechos constitucionales sino sólo, en su caso, una modulación en virtud de las obligaciones asumidas contractualmente.

Centrando el objeto de esta información a la consulta planteada sobre si el empresario podría en el ejercicio de su facultad de control y vigilancia, acceder, leer, copiar o divulgar los e-mail, archivos informáticos, etc. recibidos o remitidos por sus empleados, se entiende que habrá que partir de dos consideraciones previas:

De un lado habrá que tener en cuenta que el titular del derecho al secreto de las comunicaciones es el que efectúa la comunicación, y no el propietario del ordenador desde el que se remite o recibe el correo electrónico.

De otro lado habrá que ponderar el conocimiento previo que por parte del trabajador se tiene respecto del posible control del correo electrónico que puede ser ejercido normalmente por el empresario.

Partiendo de estas consideraciones se entiende que la posible solución a esta cuestión va a depender de la circunstancias que rodean cada supuesto, valorando entre otros, los siguientes factores, si el correo electrónico se recibió o se envío, por ejemplo, en un descanso interjornada; si se trata de un supuesto en que el objeto de la prestación del trabajador sea de un modo muy específico la recepción o envío de correos electrónicos; cuál ha sido la motivación del empleador en el control de un concreto correo etc.

A la vista de todo lo anteriormente señalado se concluye, en principio y de modo general, que siempre que el e-mail, archivo informático, etc. o cualquier otra comunicación formen parte de la actividad laboral del trabajador y se realicen en tiempo de trabajo pueden ser analizadas y supervisadas por el empresario dado que entrarían dentro de la potestad de control que puede ejercer legalmente.

5.7.2. ***Grabación de imágenes de los trabajadores y acceso a las mismas a través de una página Web de la empresa***

En este caso se solicita información sobre si se produce un atentado contra el derecho a la intimidad y a la propia imagen, al difundir públicamente la actividad que una persona realiza en el ámbito laboral, ya que una empresa en su página web, incluye las imágenes captadas por una cámara (webcam) instalada en el lugar de trabajo durante toda la jornada, preguntando también si la empresa podría hacer tal cosa sin el consentimiento de los trabajadores, se le pone de manifiesto lo siguiente:

En primer lugar se dio la información, al igual que en el caso anterior, de todo lo referente a la regulación del articulo 20 del Estatuto de los Trabajadores y de la interpretación que ha realizado el Tribunal Constitucional.

Se informó que, el empresario tiene en principio la potestad de controlar el cumplimiento de las obligaciones laborales, así como el uso profesional de los instrumentos de trabajo, como el uso del ordenador y de Internet y en consecuencia este uso debe quedar afectado a la propia actividad laboral del trabajador, por lo que en principio la grabación de imágenes de dicha actividad laboral entraría dentro de la potestad de control.

Ahora bien, es necesario resaltar que si la actuación no se limita sólo a una simple grabación y almacenamiento en vídeo sino que, además, se está tratando digitalmente la imagen, como parece que sería en el presente supuesto en que se incluiría dicha grabación en una pagina Web, ello exigiría dos consideraciones. Así, en primer lugar, la de considerar esta actuación como la de un tratamiento automatizado de datos y, en consecuencia implicaría la creación de un fichero de datos por parte del empresario y su inscripción en el Registro de Protección de Datos de esta Agencia previamente a la recogida y grabación de las imágenes. Y en segundo lugar, la necesidad del consentimiento de los

trabajadores para poder ceder su imágenes fuera del propio ámbito laboral correspondiente a la empresa, ya que al introducir las imágenes en una página Web y poderse consultar por terceras personas o entidades, dicha actuación estaría traspasando las fronteras del ámbito de la propia empresa y en consecuencia existiría una cesión de datos personales en forma de imágenes, que de conformidad con la Ley orgánica 5/1992 necesitaría del consentimiento de las personas afectadas para que pudiera llevarse a efecto.

5.8. **SECTOR DE TELECOMUNICACIONES**

Aquí hay que comenzar indicando que, al igual que en los sectores anteriores, año tras año se plantean consultas tipo que obedecen a la preocupación más general de los ciudadanos. Se pone de relieve que en el sector de telecomunicaciones esta preocupación obedece fundamentalmente a la utilización de los datos personales que de ellos figuran en los repertorios telefónicos. En este sentido se refleja, a continuación, en primer término este tipo de consultas y posteriormente se destaca la contestación dada ante una consulta referida a la normativa aplicable al servicio de buzón de voz y a la facturación telefónica.

5.8.1. ***Utilización de los repertorios telefónicos***

Los ciudadanos consultan sobre si los datos personales incluidos en los Directorios Telefónicos de acceso público pueden usarse para finalidades de marketing o análogas. En este sentido el artículo 26 de la Ley Orgánica 5/92 establece que los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado. Concretamente, en el fichero Servicios Electrónicos de Telecomunicación (actualmente páginas blancas), aparecen el nombre y apellidos completo (no sólo las iniciales) así como la dirección, y, salvo que el afectado se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general. En relación con la publicidad nominal el artículo 29 relativo a los Ficheros con fines de publicidad establece que:

"1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos figuren en documentos accesibles al público o cuando hayan sido facilitados por los propios afectados u obtenidos con su consentimiento.

2. Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud."

En estos casos se sugiere al ciudadano que, si no desea recibir publicidad, puede ejercer el derecho de exclusión de sus datos de los repertorios telefónicos, al amparo del citado artículo 26.

Este mismo derecho de exclusión viene regulado en el artículo 67 del Reglamento por el que se desarrolla el Titulo III de la Ley General de Telecomunicaciones (Real Decreto 1736/1998) que establece lo siguiente:

Artículo 67. Guías de servicios de telecomunicaciones disponibles al público.

1. Los datos personales que figuren en las guías de abonados de los servicios a los que se refiere el artículo 62 que sean accesibles al público o que puedan obtenerse a través de servicios de información, ya sean impresas o electrónicas, deberán limitarse a los que sean estrictamente necesarios para identificar a un abonado concreto. Por Orden del Ministro de Fomento, se determinarán las condiciones para hacer constar dichos datos.

No obstante lo dispuesto en el párrafo anterior, los operadores encargados de la elaboración de las guías podrán publicar otros datos personales de los abonados siempre que éstos hayan dado su consentimiento inequívoco.

A estos efectos, se entenderá que existe consentimiento inequívoco de un abonado, cuando éste se dirija al operador por escrito solicitándole que amplíe sus datos personales que figuran en la guía. También se producirá cuando el operador solicite al abonado su consentimiento y éste le responda en el plazo de un mes dando su aceptación. Si en dicho plazo el abonado no hubiese dado su consentimiento expreso, se entenderá que no acepta que se publiquen en la guía correspondiente otros datos que no sean los que se establecen en el párrafo primero de este apartado.

2. Los abonados podrán exigir a los operadores que se les excluya de las guías, que se indique que sus datos personales no puedan utilizarse para fines de venta directa o que se omita parcialmente su dirección. Los operadores requeridos deberán cumplir lo dispuesto en este apartado, sin coste alguno para los abonados.

Los abonados que soliciten su exclusión de las guías, tendrán derecho a recibir la información adicional a la que se refiere el párrafo segundo del apartado 3 del artículo 69."

5.8.2. **Supresión en origen de la línea llamante. Código 067.**

En el mes de julio de 1998 se publicó una norma que afecta directamente a la protección de la privacidad en el marco de las comunicaciones telefónicas. Concretamente nos referimos al Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación

de las redes de telecomunicaciones, aprobado por Real Decreto 1736/1998, de 31 de julio, que establece en su artículo 70 que los operadores que presten servicios avanzados de telefonía con la facilidad de identificación de la línea llamante deberán ofrecer la posibilidad de que el usuario que origine las llamadas pueda suprimir en cada una de ellas dicha identificación y mediante un procedimiento sencillo y gratuito.

En este sentido la Resolución de 2 de diciembre de 1998 de la Secretaría de Estado de Comunicaciones del Ministerio de Fomento, publicada en el BOE de 30 de diciembre, establece el código 067 para el servicio de supresión en origen, llamada a llamada, de la identificación de línea llamante.

En consecuencia, el establecimiento del referido código 067 permitirá soslayar la posible lesión contra la intimidad que supone la identificación del número llamante ya que existe un procedimiento previsto para suprimir en origen dicha identificación.

5.8.3. ***Servicio buzón de voz y facturación telefónica***

Se plantean varias consultas sobre la normativa aplicable a la protección de datos que vaya referida al servicio de buzón de voz que prestan las empresas telefónicas, y, de otra parte, al tiempo en que puede ser almacenada la información sobre las llamadas que un abonado realiza desde su teléfono,

En primer lugar se señala que, con carácter general, la Ley Orgánica 5/1992 establece en su artículo 4 que los datos de carácter personal serán cancelados cuando hallan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

Por otro lado el Titulo V del Reglamento que desarrolla la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones aprobado por Real Decreto 1736/1998, de 31 de julio (BOE 5-9-98) viene a regular en detalle lo dispuesto en el artículo 50 de dicha Ley que prevé, en este ámbito, la protección de los datos personales. En concreto, el artículo 65 del Reglamento, establece, en su apartado 1, que los operadores deberán destruir los datos de carácter personal sobre el tráfico relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto termine la misma, sin perjuicio de los dispuesto en los apartados siguientes.

A la vista de esta regulación, en términos generales se entiende, en principio, que, el mensaje grabado en el buzón de voz puede ser un dato de carácter personal, de conformidad con la definición contenida en el apartado 5 del referido artículo 65, por lo que una vez recibido por su destinatario y borrado por este de su buzón, habrá que considerar que el operador de telefonía no podría almacenarlo de ninguna forma, ya que ello podría contravenir lo dispuesto en la regulación anterior.

Por lo que se refiere a los datos relativos a la facturación se indica que, el mismo artículo 65 del Reglamento del Servicio Universal regula en su apartado 2 que, por los operadores de telefonía, podrán ser tratados exclusivamente con objeto de realizar la facturación y los pagos de las interconexiones, los datos que incluyan :

a) el número o la identificación del abonado
b) la dirección del abonado y el tipo de equipo terminal empleado en las llamadas.
c) el número total de unidades que deben facturarse durante el ejercicio contable
d) el número de abonado que recibe la llamada
e) el tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos.
f) la fecha de la llamada o del servicio
g) Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.

Sigue regulando dicho precepto que los datos referidos podrán tratarse y almacenarse únicamente por el plazo durante el que pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores deberán destruir los datos de carácter personal en los términos del apartado 1 de dicho precepto.

A la vista de lo anterior se desprende que, en una relación comercial de desarrollo normal entre los abonados al servicio telefónico y los operadores telefónicos, una vez abonada la factura correspondiente al período de la prestación del servicio de telefonía y transcurrido el plazo de impugnación de la misma, se deberían destruir por los operadores los datos señalados anteriormente.

5.9. **DATOS DE SALUD**

Sobre los datos de salud hay que señalar que, con carácter general, las consultas planteadas son referidas al derecho de acceso a las historias clínicas e inscripción de los ficheros utilizados por el personal medico y sanitario. A modo de resumen se resalta una de las consultas planteadas en las que se recoge ampliamente la información suministrada a los ciudadanos sobre estos datos.

En primer lugar se indica que los datos de salud son un tipo de datos a los que la Ley Orgánica 5/1992 considera como especialmente protegidos y así los contempla en su artículo 7 al establecer que este tipo de datos solo podrán ser recogidos y tratados automatizadamente con el consentimiento expreso de las personas afectadas, o cuando por razones de interés general así lo disponga una ley.

No obstante lo anterior y aun cuando una persona que acude a la consulta de un médico sabe o presume de antemano que se le va a preguntar por una serie de datos suyos referentes sobre todo a su salud, igualmente deberá ser informada previamente por el personal médico o profesional correspondiente, del contenido del artículo 5 de la Ley Orgánica que viene a establecer que las personas a las que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

"a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos en forma claramente legible, las advertencias a que se refiere el apartado anterior.

No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban."

A la vista de lo anterior se entiende en principio que, el tratamiento automatizado será posible siempre que se haya informado del mismo a los afectados.

También se informa que respecto a los datos de salud y de conformidad con lo previsto en el articulo 4 del Reglamento de Medidas de Seguridad aprobado por Real Decreto 994/1999, se deberán adoptar además de las medidas de nivel básico y medio, las calificadas de nivel alto, en definitiva todas las medidas contempladas en los capítulos II, III y IV de dicho Reglamento.

Por último se indica que cualquier fichero de datos de carácter personal deberá ser notificado previamente a la Agencia de Protección de Datos para su inscripción formal en el Registro General de Protección de Datos utilizando el modelo de inscripción que fue objeto de publicación en el BOE nº 149 de 23 de junio de 1994.

Seguidamente y dentro de este apartado se resaltan tres consultas que se consideran interesantes

5.9.1. ***Datos genéticos***

Se planteó una consulta a través del correo electrónico en la que por motivos de un trabajo de investigación universitaria se interesaba conocer si la intimidad genética es objeto de algún tipo de protección especial en España, bien a nivel normativo o de política de la Agencia de Protección de Datos

Se puso de manifiesto, en primer lugar, que, con carácter general, el artículo 18.1 de la Constitución española garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, habiendo sido desarrollado este derecho fundamental por la Ley Orgánica 1/1982, de 5 de mayo, con incidencia en lo relativo a la genética de las personas en la medida en que forma parte de su intimidad.

En segundo lugar se indicó que, si los datos genéticos personales son recogidos y tratados en soporte informáticos, entonces sería de aplicación la Ley orgánica 5/1992 reguladora del tratamiento informatizado de los datos de carácter personal, norma esta dictada en desarrollo de lo dispuesto en el articulo 18.4 de la Constitución.

Ciñendo la consulta únicamente a este ultimo punto, que es sobre el que tendría competencia la Agencia de Protección de Datos, se indicó que los datos genéticos en la medida en que puedan afectar a datos de salud, sí serían objeto de una protección especial, dado que así viene regulado en el articulo 7.3 de la Ley Orgánica que expresamente establece: "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente".

5.9.2. ***Datos de historias clínicas***

En este caso se presentó una consulta solicitando información en relación con los aspectos de confidencialidad e inviolabilidad de los datos contenidos en la historia clínica.

Aquí se vino a considerar en primer término la necesidad de tener en cuenta que la Ley Orgánica limita su ámbito de aplicación a los datos personales automatizados, por lo que las respuestas se refieren tan sólo a los datos de la historia clínica que se encuentren informatizados en los instituciones y centros sanitarios no pudiéndose aplicar las respuestas de esta consulta a los historiales clínicos en soporte papel.

En términos generales se informó que el artículo 61 de la Ley General de Sanidad establece que:

En cada Área de Salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse, al menos, dentro de los límites de cada institución asistencial.

Estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Los poderes públicos adoptarán las medidas precisas para garantizar dichos derechos y deberes.

Existen además numerosas normas sanitarias que exigen la creación y conservación del historial clínico siempre que se produzca la intervención de las Administraciones Sanitarias con diversos fines. El mantenimiento de la información viene obligado también por las normas penales y civiles para los supuestos de responsabilidad por posibles negligencias médicas.

5.9.3. ***Datos de prevención de riesgos laborales***

Se han recibido consultas por la que se plantean si, una empresa que dispone de ficheros automatizados de uso interno y acceso restringido, para una mejor gestión de los recursos humanos, en los que introduce datos relativos a la salud y formación de los empleados, debe notificar estos ficheros a la Agencia de Protección de Datos, así como si debe tener el consentimiento expreso de las personas sobre las que se guarda la información.

En primer lugar se indicó que, el artículo 7 de la Ley Orgánica 5/1992 establece que, los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

Por otro lado conviene destacar que el artículo 22 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales, establece que el empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo, siempre que el trabajador preste su consentimiento, salvo que dicho reconocimiento sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores.

Ahora bien, no obstante lo anterior, la misma norma prevé igualmente que dicho reconocimiento se realizará respetando el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud, estableciendo, en este sentido, que el acceso a la información médica de carácter personal se limitará al personal médico y autoridades sanitarias que lleven a cabo la vigilancia de la salud, sin que pueda facilitarse dicha información al empresario o a otras personas, sin consentimiento expreso del trabajador.

En consecuencia y a la vista de la regulación anterior se informa que, si el trabajador no consiente expresamente en que sus datos personales de salud sean facilitados al empresario, éste sólo podrá ser informado de las conclusiones que se deriven de los reconocimientos en relación con la aptitud del trabajador para el desempeño de su puesto, pero en ningún caso estará habilitado para el tratamiento informático de ningún dato de salud que no se refiera a dichas conclusiones.

Finalmente, este tipo de ficheros que evidentemente contienen datos de carácter personal y además datos de salud, deben inscribirse en el Registro de Protección de Datos de esta Agencia, de conformidad con lo previsto en el artículo 24 de la Ley Orgánica, siéndole además de aplicación el Reglamento de Medidas de Seguridad de Ficheros Automatizados aprobado por Real Decreto 994/1999.

5.10. **DATOS DEL CENSO ELECTORAL**

Han existido durante 1999 varias consultas referidas a la utilización del Censo Electoral por los diferentes partidos y formaciones políticas. Es por ello que se entiende útil el plasmar aquí dos de las contestaciones que se han dado a los ciudadanos durante este año informándoles sobre la legalidad de la utilización del censo en los términos planteados.

5.10.1. ***Utilización de los datos del censo electoral exclusivamente para la campaña electoral. Cancelación posterior***

En esta consulta se solicita información sobre la cancelación de los datos obtenidos a partir del Censo Electoral por una formación política.

En contestación a la misma se le puso de manifiesto al ciudadano lo siguiente:

1º.- El artículo 32 de la Ley Orgánica 5/1985, de 19 de junio que regula el Régimen electoral general, modificada por la Ley Orgánica 3/1995, de 23 de marzo prevé que la inscripción en el censo es obligatoria.

2º.- Por otra parte, el artículo 41 de dicha norma regula el acceso a los datos censales, estableciendo en su apartado 5 que: *" Los representantes de cada candidatura podrán obtener el día siguiente a la proclamación de candidaturas una copia del censo del distrito correspondiente ordenado por mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente ley. Alternativamente los representantes*

generales podrán obtener en las mismas condiciones, una copia del censo vigente de los distritos donde su partido, federación o coalición presente candidaturas..."

3º.- De conformidad con lo establecido en la normativa anterior, se desprende, en principio, que el envío de la publicidad electoral que se le realice por parte de las formaciones políticas que se presentan a las elecciones es conforme a derecho, habida cuenta que dicho envío entraría dentro de las actividades lícitas que por parte de dichas formaciones se pueden llevar a cabo para la captación de votos.

Ahora bien es necesario puntualizar que la norma anterior autoriza a los partidos políticos que presentan sus candidaturas a obtener la información referida, pero su uso se limita a la campaña electoral y a la comprobación de la transparencia de los comicios que se celebran, por lo que una vez terminada la campaña y en el supuesto de haber tratado automatizadamente los datos de los electores, éstos deberían de cancelarse de conformidad con lo establecido en el artículo 4.5 de la Ley Orgánica, al haber desaparecido la finalidad del tratamiento.

5.10.2. ***Propaganda electoral enviada por un partido político a un domicilio que no es la residencia habitual del ciudadano***

En este segundo caso, se plantea una queja por un ciudadano, sobre la publicidad electoral que le han enviando a un domicilio que no constituye su residencia habitual, como consecuencia de celebración de las elecciones municipales y europeas.

En este caso y después de informarle de la regulación que con carácter general se contiene en la Ley Orgánica 5/1985, de 19 de junio que regula el Régimen electoral general, y señalar al igual que en la consulta anterior, que el envío de publicidad electoral que se le realice por parte de las formaciones políticas que se presentan a las elecciones es conforme a derecho, se le matizó lo siguiente:

Dado que la propaganda electoral se le ha enviado por parte del partido político a una dirección que no constituye su residencia habitual y que en consecuencia no figura en el censo electoral, hay que señalar que la legislación vigente en materia de protección de datos (Ley Orgánica 5/1992), reconoce una serie de derechos a los ciudadanos, como son el derecho de acceso, rectificación y cancelación de sus datos personales. El ejercicio de los mismos es personal, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables/titulares de los ficheros automatizados, lo que significa que el ciudadano podrá dirigirse a la referida formación política, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación).

Si en el plazo de un mes para el derecho de acceso y de 5 días para los derechos de rectificación y cancelación desde la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, el ciudadano podrá dirigirse a la Agencia con copia de la solicitud cursada, para que ésta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de sus derechos.

5.11. **DATOS ESTADISTICOS**

En relación con la petición o recogida de datos estadísticos se ha realizado en el año 1999 una consulta que se ha considerado conveniente reflejarla en la memoria dado que por el ámbito al que afecta, que es el universitario, puede ser de interés.

Se solicitó información sobre la siguiente consulta: Al ir a hacer la matrícula para el nuevo curso en una Universidad, el ciudadano que consulta se encuentra con la necesidad ineludible de rellenar un impreso, llamado hoja de recogida de datos estadísticos, en el que le hacen preguntas acerca de su nivel de estudios, los niveles de sus padres, sus situaciones de trabajo, tipo de residencia y si tiene o no minusvalías. Al preguntar por la razón de la obligatoriedad de tal trámite, le dicen que se debe a lo establecido en la ley 12/1989. La duda que le surge es la siguiente: ¿Por qué, si se trata sólo de una estadística le obligan a identificarse con nombre, apellidos y número de carnet de identidad?.

En contestación a la consulta, se le informó que, en principio, al indicársele por la Universidad que la recogida de los datos personales tiene su base en la Ley 12/1989 Reguladora de la Función Estadística Pública, dicho tratamiento quedará específicamente regulado por dicha norma. A la vista de la misma, y de conformidad con lo dispuesto en su artículo 10, los servicios estadísticos podrán solicitar datos de todas las personas físicas y jurídicas, nacionales y extranjeras, residentes en España, y estas, tanto si su colaboración es obligatoria como voluntaria, deben contestar de forma veraz, exacta, completa y dentro del plazo a las preguntas ordenadas en la debida forma por parte de los servicios estadísticos.

Ahora bien, también se le indicó que, de conformidad con lo dispuesto en el artículo 11 de la misma norma, cuando los servicios estadísticos soliciten datos, deberán proporcionar a los interesados información suficiente sobre la naturaleza, características y finalidad de la estadística, advirtiendo, además, de si es o no obligatoria la colaboración, de la protección que les dispensa el secreto estadístico, y de las sanciones en que, en su caso, puedan incurrir por no colaborar o por facilitar datos falsos, inexactos, incompletos o fuera de plazo.

Finalmente se le informó que, según el artículo 11.2 de dicha Ley, en todo caso, serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los interesados los datos susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general,

cuantas circunstancias puedan afectar a la intimidad personal o familiar.

5.12. **CESION DE DATOS**

Durante 1999 han sido frecuentes las consultas que sobre el principio de la cesión de datos se han planteado por los ciudadanos, ya que es común la preocupación de hasta qué punto se pueden ceder datos personales sin consentimiento de las personas afectadas. Se ha venido informando con carácter general de la necesidad evidente del consentimiento. En aquellos casos en que concurre una de las excepciones contempladas legalmente (art.11.2) se trata de dar una información lo mas completa posible para que el ciudadano sepa que, en determinados supuestos si se pueden ceder sus datos sin su consentimiento.

Este apartado está desarrollado estadísticamente con todo detalle en el gráfico nº 9.

Aquí y por entenderse que es uno de los asuntos que junto con los ficheros de solvencia y los ficheros de publicidad puede ser de mayor interés, se van a reflejar tres de las consultas que han sido objeto de informe. En primer lugar se destaca una consulta sobre una cláusula de cesión de datos contenida en una libreta de ahorros de una entidad bancaria. En segundo lugar se contempla la legalidad de la cesión de datos a la Inspección de Trabajo por una Compañía de Seguros respecto de sus Agentes y por último la posibilidad de si un Centro escolar puede ceder datos personales de los alumnos a la Asociación de Padres.

5.12.1. ***Cláusula prevista para la cesión de datos en una Libreta de Ahorros.***

Se plantea por un ciudadano la legalidad de una cláusula que debe suscribir para la apertura de una libreta de ahorros.

La cláusula, referente al tratamiento automatizado de datos personales, viene a establecer, de un lado, la información de la posibilidad del tratamiento automatizado de los datos personales en un fichero automatizado titularidad del propio Banco, y de otro, obliga a prestar el consentimiento expreso por parte del cliente, autorizando la cesión de sus datos a terceros que formen parte del grupo de empresas del Banco, con la exclusiva finalidad de poderle enviar informaciones publicitarias sobre productos, servicios, ofertas o promociones especiales.

En primer lugar se informó que con carácter general la Ley Orgánica 5/1992 reguladora del tratamiento automatizado de los datos de carácter personal establece el derecho de información en la recogida de los datos y así el articulo 5 regula:

"Artículo 5. Derecho de información en la recogida de datos

1. Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".

Igualmente se indicó que los artículos 6 y 11 de dicho texto legal regulan la necesidad del consentimiento de las personas afectadas por los datos tanto para el tratamiento informático de los mismos como para su cesión a terceros. En este sentido conviene transcribir el contenido completo de dichos artículos. Así, el artículo 6 establece lo siguiente

Artículo 6. Consentimiento del afectado

1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el *ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.*

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos."

Por lo que se refiere concretamente a la cesión de datos, ésta se encuentra detalladamente regulada en el artículo 11 de la Ley Orgánica que establece lo siguiente:

"Artículo 11. Cesión de datos

1.Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2.El consentimiento exigido en el apartado anterior no será preciso

a)Cuando una Ley prevea otra cosa.

b)Cuando se trate de datos recogidos de fuentes accesibles al público.

c)Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

d)Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

3.Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o sino constase con claridad la finalidad de la cesión que consiente.

4.El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.

5.El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.

6.Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."

A la vista de la regulación anterior se indicó que, en principio la cláusula que se contiene en el contrato de apertura de la Libreta de Ahorros cumple con la obligación de informar previamente a la formalización del contrato de que sus datos van a ser tratados y cedidos a empresas del grupo, informándole además que si se firma el contrato se estaría aceptando la misma en esas condiciones.

Ahora bien, una vez firmado el contrato y atendiendo a que de conformidad con lo previsto en el articulo 11.4 el consentimiento puede ser revocado, nada le impediría que, con posterioridad a la apertura de la cuenta, se dirigiese a la entidad bancaria indicándoles que revoca sus consentimiento a los efectos de la cesión de sus datos a las empresas del grupo.

5.12.2. ***Cesión de datos a la Inspección de Trabajo por parte de una Compañía Aseguradora***

Se solicita información sobre si sería posible la cesión de datos de los agentes, subagentes o intermediarios que trabajen para una Compañía Aseguradora a la Inspección de Trabajo y a su vez de la Inspección de Trabajo a la Tesorería General de la Seguridad Social.

Se le indicó que la Dirección General de la Inspección de Trabajo tiene inscrito en el Registro General de Protección de Datos un fichero cuya finalidad es la gestión de documentación generada en las inspecciones provinciales y realización de las actas de infracción levantadas a los trabajadores.

Igualmente la Dirección General de la Tesorería General de la Seguridad Social tiene inscrito en el Registro General de Protección de Datos el fichero "RECAUDACIÓN", cuya finalidad es la gestión integrada de los datos de cotización y recaudación a la seguridad social.

Respecto a la cesión de datos, se le informó que la actuación de la Inspección de Trabajo, en principio, parece tener su fundamento en la realización de una investigación sobre la falta de cotización de los agentes de seguros, dado que dicha conducta puede constituir una infracción a lo dispuesto en la Ley 8/1988, de 7 de abril, sobre infracciones y sanciones en el orden social. Dicha actuación está amparada en la Ley 42/1997, de 14 de noviembre, ordenadora de la

Inspección de Trabajo y Seguridad Social, que prevé como uno de sus cometidos en el artículo 3.1 el de vigilar y exigir el cumplimiento de la normas legales en estas materias.

Entre las facultades que la Ley 42/1997 reconoce a los Inspectores de Trabajo y Seguridad Social, en el desempeño de sus competencias, está previsto dentro del artículo 5, apartado 3.1, la de requerir información, solo o ante testigos, al empresario o al personal de la empresas sobre cualquier asunto relativo a la aplicación de las disposiciones legales.

El artículo 11.2 a) de la LORTAD establece como una de las excepciones al consentimiento previo del afectado para que la cesión de datos pueda tener lugar, el supuesto de que una ley prevea otra cosa. A la vista de este precepto, no se desprende que la empresa de seguros al comunicar los datos de los agentes de seguros a la Inspección de Trabajo esté cometiendo ninguna infracción, habida cuenta que si es requerida por la Inspección a estos efectos tiene obligación legal de facilitar dicha información.

Por lo que se refiere a la posible cesión de datos de la Inspección de Trabajo a la Tesorería General de la Seguridad Social, se informa igualmente que la Ley General de la Seguridad Social prevé en su artículo 36 apartado 4 que, los funcionarios públicos, están obligados a colaborar con la Administración de la Seguridad Social para suministrar toda clase de información objeto o no de tratamiento automatizado, siempre que sea útil para la recaudación de sus recursos.

En ambos casos, pues, la cesión de datos personales sin el consentimiento del afectado, estaría amparada por una ley que expresamente lo prevé.

5.12.3. ***Cesión de datos a las Asociaciones de Padres de Alumnos***

Se planteó una consulta por la que se interesaba conocer si un centro educativo podía o debía facilitar a la Asociación de Padres de Alumnos del Centro, los datos personales de los alumnos cuyos padres no son socios de la Asociación.

En este caso se informó en primer lugar que el supuesto planteado era una cesión de datos y en virtud de la legislación vigente, en concreto en el art. 11 de la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (en adelante LORTAD), se establece en el apartado primero que, los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

No obstante, en el apartado segundo se establece una serie de excepciones a esa necesidad de consentimiento como son, entre otros, :

a) Cuando una Ley prevea otra cosa.

Por otro lado el Real Decreto 1533/1986 de 11 de julio de 1986, que regula las Asociaciones de Padres de Alumnos, establece en su artículo 5 apartado e) el procedimiento de admisión de los asociados señalando que, l*a admisión será en todo caso voluntaria y previa solicitud de inscripción, no pudiendo exigirse más requisitos que el de ser padre o tutor del alumno matriculado en el Centro, abonar, en su caso, las correspondientes cuotas y aceptar expresamente los correspondientes estatutos".*

A la vista de estos preceptos se puso de relieve que, en principio el centro educativo no puede facilitar a la Asociación los datos personales de los alumnos cuyos padres no son socios de la misma, no estando este caso recogido entre las excepciones del art. 11.2 de la Ley Orgánica, y siendo por tanto necesario el consentimiento de los padres para que el centro educativo pudiera ceder esos datos.

5.12.4. ***Cesión de datos entre ficheros de titularidad privada***

Se formula una consulta sobre si al amparo de la Ley Orgánica estaría permitido que un expresidente de una comunidad de vecinos utilice el listado de propietarios de la comunidad para el envío de publicidad de sus empresas.

En este caso se informa de la regla general en esta materia relativa a los principios de calidad de datos y cesión de datos contenidos en los artículos 4.2 y 11 de la Ley Orgánica

Artículo 4. Calidad de los datos

Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

Artículo 11. Cesión de datos.

Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

Se concluye señalando que de conformidad con las disposiciones anteriores, el expresidente de la comunidad de vecinos no puede utilizar el listado de la comunidad de vecinos para el envió de publicidad de sus empresas, sin tener el consentimiento de cada uno de ellos, dado que en caso contrario se estaría actuando de una forma contraria a lo previsto en la Ley, incurriendo en la infracción correspondiente.

5.12.5. ***Cesión de datos del Padrón Municipal a otras Administraciones Públicas***

En este supuesto se planteó una consulta sobre si los datos contenidos en el padrón municipal pueden ser cedidos a otras Administraciones Publicas para usos distintos a los estadísticos o censales, poniéndole de manifiesto lo siguiente:

De un lado, la Ley Orgánica 5/92 regula en su artículo 19 la cesión de datos entre Administraciones Públicas estableciendo que:

"*1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso."*

Por otra parte, la nueva redacción del artículo 16 de la Ley de Bases de Régimen Local determina en su apartado tercero, que los datos del padrón se cederán a otras Administraciones Públicas que lo soliciten sin el consentimiento del afectado, sólo cuando les sean necesarios para el ejercicio de sus respectivas competencias y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

A la vista de estos preceptos y del contenido de la consulta, en principio parece desprenderse que siempre que se trate de competencias similares, y limitado a datos de nombre, apellidos y domicilio, la cesión de datos del padrón a otra Administración Pública será conforme a derecho.

Igualmente se indica que, los funcionarios que intervengan en el tratamiento de los datos del padrón tienen la obligación de guardar secreto profesional, de conformidad con el artículo 10 de la LORTAD.

5.13. **COLEGIOS PROFESIONALES**

Las consultas planteadas sobre el sector de Colegios Profesionales han versado fundamentalmente sobre el carácter de fuentes accesibles al público de las listas de los colegiados y en este sentido se quiere resaltar una consulta por la que se solicitaba información sobre si es legal que un colegio profesional publique en su página Web y sin ningún tipo de restricción de acceso, el nombre, apellidos, dirección y teléfono de sus colegiados sin solicitar el consentimiento expreso de todos y cada uno de ellos.

En primer lugar se puso de manifiesto que, conforme dispone el artículo 11 de la Ley Orgánica 5/1992, los datos de carácter personal objeto de tratamiento sólo podrán ser cedidos, para el cumplimiento de fines directamente relacionados con las funciones del cedente y el cesionario, previo consentimiento del interesado, salvo cuando una disposición con rango de Ley prevea otra cosa o si dichos datos se encuentren recogidos en fuentes accesibles al público.

El artículo 1.3 del Reglamento del desarrollo de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, aprobado por el Real Decreto 1332/1994, de 20 de junio, define los datos accesibles al publico como : "los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo ."

En consecuencia, en el caso de que el Colegio Profesional publique una lista de colegiados para consulta del público en general, independientemente del soporte en que dicha lista se publique que puede ser papel, página Web etc., los datos contenidos en la misma serán susceptibles de utilización conforme a lo establecido en los artículos 6.2 y 11.2 b) de la Ley Orgánica, en el bien entendido de que esos datos serán, únicamente, los referentes al nombre, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

En caso contrario, será preciso, conforme prevé el ya citado artículo 11.1 de la Ley Orgánica, el consentimiento previo de los interesados

5.14. **SEGUROS**

Del total de consultas planteadas en este sector se quiere resaltar una en concreto planteada sobre la legalidad de la cesión de determinados datos personales entre la entidad bancaria que concede un préstamo hipotecario y la entidad aseguradora que procede a suscribir una póliza de seguro de vida para garantizar el pago del préstamo.

En este caso se hizo referencia al contenido de la instrucción 2/1995 de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal, que en su norma segunda establece:

1.La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las entidades de crédito a través de cuestionarios u otros impresos

deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.

2.Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora. Las entidades de crédito no podrán incluir los datos de salud en sus ficheros informatizados o en aquellos en los que almacenen datos de forma convencional.

Por su parte, la norma tercera establece que las entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la entidad de crédito como agente o tomador del contrato de seguro.

5.15. **REGLAMENTO DE MEDIDAS DE SEGURIDAD**

Finalmente se quiere destacar el impacto que ha tenido la entrada en vigor del Real Decreto 994/1999 de 13 de junio por el que se aprobaba el Reglamento de Medidas de Seguridad, lo que se analiza únicamente desde el prisma de la información solicitada tanto por empresas como particulares interesándose por el tipo de medidas a adoptar, sobre la obligación de inscripción de ficheros, sobre la redacción del documento de seguridad, y en definitiva sobre todo lo que implica la adopción de las medidas de seguridad amparadas por dicho Reglamento. Esta incidencia ha sido mayor durante el mes de diciembre en el que como consecuencia de la finalización del plazo para adoptar las medidas de nivel básico, las consultas se intensificaron de manera notable.

Cabe destacar, que la entrada en vigor del Reglamento de Medidas de Seguridad ha provocado un importante número de consultas sobre la obligatoriedad y requisitos para inscribir los ficheros de titularidad pública y privada que contengan datos de carácter personal en el Registro General de Protección de Datos, como paso previo a la adopción de las pertinentes medidas de seguridad.

A modo de resumen y comparativamente con respecto al año 1998 se observa que las consultas escritas relativas a información sobre inscripción de ficheros fue de un total de 48 consultas, mientras que en 1999 han sido de 336. Igualmente las consultas por escrito relativas a la adopción de medidas de seguridad fueron en el año 1998 de 8 y en 1999 han sido de 58. También se destaca que como consecuencia de estas medidas durante los meses de noviembre y diciembre fue constante la atención telefónica incrementándose en más de un 50% ya que se pasó de una media de 450 llamadas a 1.200 llamadas.

La información ha versado únicamente sobre los aspectos formales de la declaración informando que el criterio determinante para proceder a la inscripción de un fichero es el tratamiento automatizado de los datos relativos a personas físicas; por lo que si se dispone de cualquier fichero informatizado que contenga datos de esta clase deberán proceder a la notificación del fichero en el Registro General de Protección de Datos de la Agencia.

A éste efecto se han remitido fotocopia del modelo normalizado publicado en el Boletín Oficial del Estado.

También se ha informado de la posibilidad de obtener el citado formulario de las páginas Web de la Agencia en Internet señalando, que tanto el formulario como la inscripción es gratuita, y en cuanto a la remisión, ha de realizarse por correo.

Igualmente se ha informado que, de conformidad con el Reglamento aprobado por Real Decreto 994/1999 de 11 de junio (BOE 25-6-1999), deberán de adoptar en sus ficheros el nivel de seguridad básico, medio o alto en función del tipo de datos que manejen (art. 4) y redactar el documento de seguridad regulado en el articulo 8 del referido Reglamento, no teniendo la obligación de presentarlo en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido. Al propio tiempo se le informa que la Agencia no ha elaborado ningún modelo de este documento de seguridad.

VI. CÓDIGOS TIPO

1.- Introducción.

El artículo 32 de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPD), prevé, como ya hacía la Ley Orgánica 5/92 (LORTAD), la posibilidad de formular códigos tipo a los responsables de ficheros, a través de acuerdos sectoriales o mediante decisiones de empresa o convenios administrativos, en los que se establezcan:

1. Condiciones de organización
2. Régimen de funcionamiento
3. Procedimientos aplicables
4. Normas de seguridad del entorno, programas o equipos
5. Obligaciones de los implicados en el tratamiento y uso de la información personal
6. Garantías para el ejercicio de los derechos de las personas
7. Medidas a adoptar por el incumplimiento del código

Estos códigos tienen el carácter de códigos deontológicos o de buena práctica profesional, y deben ser depositados en el Registro General de Protección de Datos (RGPD), donde se procederá a su inscripción, siempre que se ajusten a las disposiciones legales y reglamentarias sobre la materia, o se denegará, en caso contrario. En este último supuesto, previamente, los solicitantes son requeridos para que efectúen las correcciones necesarias.

2.- Análisis normativo

La LORTAD y próximamente la LPD constituye la norma básica reguladora de las garantías y la protección de las libertades públicas y los derechos fundamentales y, especialmente, del honor y la intimidad personal, respecto del tratamiento de datos, tenga o no carácter automatizado.

Su regulación, de carácter imperativo, contempla, no obstante, la posibilidad de que los responsables de los ficheros y tratamientos pueden ampliar o adecuar a las peculiaridades del sector en el que operan las previsiones normativas sobre protección de datos personales, abriendo así el camino a la autorregulación en esta materia.

Esta posibilidad encuentra fundamento en la regulación que respecto de los códigos tipos prevee el art. 32 de la LPD:

De acuerdo con este precepto los códigos tipo son códigos deontológicos o de buena práctica profesional formulados por los responsables del tratamiento de datos personales para facilitar el ejercicio de los derechos de las personas en el cumplimiento de las normas reguladoras de protección de datos personales.

Pese a la brevedad de su regulación normativa, ya que la LPD dedica a esta figura sólo un artículo, el tratamiento de los códigos tipo presenta un abanico de cuestiones que es preciso abordar y que hacen referencia a los sujetos habilitados para adaptarlos, a su contenido y a los criterios y procedimientos de evaluación de los mismos. Este conjunto de cuestiones son las que se analizarán a continuación, haciendo referencia tanto a las previsiones contenidas en 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 (la Directiva), como a la LORTAD y de la recientemente aprobada LPD.

Respecto de los sujetos habilitados para la adopción de códigos tipo tanto la LORTAD como la LPD contienen diferencias relevantes respecto de la Directiva comunitaria.

Esta última parece circunscribir la posibilidad de adopción de códigos tipo sólo respecto de aquéllos que tengan carácter sectorial, excluyendo implícitamente que puedan tener como ámbito propio el de una sola empresa. Así se desprende del art. 27 de la Directiva, cuyo apartado 1 hace referencia a que "los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las peculiaridades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva". Por su parte, el apartado 2 del mismo precepto reitera esta configuración sectorial de los códigos tipo en la regulación comunitaria, al referir únicamente a las "asociaciones profesionales" y a "las demás organizaciones representantes de otras categorías de responsables de tratamientos", como sujetos habilitados para adoptarlos.

A diferencia de la Directiva, la LORTAD, admitiendo la posibilidad de realizar códigos tipo de carácter sectorial, ampliaba las posibilidades de adopción de esta figura al permitir en su art. 31 que pudieran ser formulados por "decisiones de empresa", expresión que debe interpretarse en el sentido de que el código tipo tenga como ámbito de aplicación el de un solo operador económico independiente. Esta posibilidad admitida por la norma española no ha resultado, además, una mera posibilidad teórica, sino que ha tenido traducción práctica al haber sido precisamente el primero de los códigos tipo inscritos en el Registro General de Protección de Datos el correspondiente a una sola empresa y no a un sector profesional o empresarial. Es el caso concreto del código tipo elaborado por Telefónica de España S.A., inscrito en el Registro en la temprana fecha de 1994, muy próxima a la entrada en vigor de la LORTAD.

Sin embargo, la normativa española, que contempla, cómo se ha expuesto, posibilidades más amplias que la Directiva en esta materia, resulta más restrictiva que la disposición comunitaria a la hora de permitir la formulación de códigos tipo atendiendo al carácter público o privado del responsable del fichero.

En efecto, la LORTAD sólo admitió la posibilidad de que los códigos tipo pudieran formularse por responsables de ficheros de titularidad privada quedando, así, excluida la hipótesis de que la autorregulación alcanzara el ámbito de las Administraciones Públicas en sus diversas modalidades organizativas. Por el contrario, la Directiva, al no incluir referencia expresa alguna al carácter público o privado del responsable del fichero admite, al menos implícitamente, la alternativa de que los códigos tipo alcancen al tratamiento de datos por parte de tales Administraciones.

Por su parte, la LPD ha venido acertadamente a superar las restricciones de uno u otro orden de que adolecían la Directiva y la LORTAD.

La regulación contenida en su art. 32 permite que la formulación de los códigos tipo pueda adaptarse flexiblemente a las necesidades de una sola empresa o de la totalidad o parte de un sector empresarial o profesional y lo hace sin distinción del carácter público o privado del responsable del fichero, al disponer en su apartado 1 que "mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo ...".

La posibilidad de que puedan elaborarse códigos de conducta por las Administraciones Públicas debe, asimismo,

considerarse de interés en orden a facilitar el conocimiento de la normativa reguladora de la protección de datos personales, armonizar sus actuaciones en esta materia y favorecer su cumplimiento. Máxime si se tiene en cuenta que las citadas Administraciones son operadores que tratan un volumen ingente de datos personales de los ciudadanos. En particular, la formulación de códigos tipo por los responsables de ficheros de titularidad pública puede resultar apropiada respecto de Administraciones como las Locales que, por su dispersión geográfica y diversidad de tamaño, pueden encontrarse en dificultades para el cumplimiento adecuado de la normativa de protección de datos. Asimismo, los códigos tipo podrían constituir un instrumento que facilitara tal objetivo en el ámbito de las Corporaciones de Derecho Público en las que se combina el ejercicio de funciones públicas delegadas con actividades de índole privada.

A modo de resumen, y sin ánimo de codificar lo que la norma contempla con un carácter abierto, el contenido de los códigos tipo puede tener por objeto ampliar o facilitar el cumplimiento de las obligaciones establecidas en la normativa de protección de datos personales, incrementar las garantías de los ciudadanos, reforzar las estructuras organizativas y técnicas en el tratamiento de aquéllos y, en particular, las medidas de seguridad, o contemplar procedimientos específicos para la tutela de los principios y derechos exigibles en esta materia.

La amplitud con la que la LPD trata el contenido hipotético de un código tipo se encuentra directamente relacionada con una cuestión capital en relación con dicha figura, como es la de los criterios que han de utilizarse para su evaluación.

La evaluación de un código tipo es el proceso de análisis del valor añadido o plus de efectividad que su aprobación supone respecto de los principios fundamentales de protección de datos establecidos normativamente.

La evaluación de los códigos tipo debe estar presidida por un criterio de flexibilidad que permita apreciar las circunstancias concurrentes en cada caso concreto. De acuerdo con este criterio no cabe excluir, "a priori", qué códigos tipo de carácter eminentemente informativo, por reiterar los principios básicos de protección de datos personales, puedan ser admitidos pese a que quepa argumentar que el valor añadido que incorporan respecto de las normas imperativas de protección de datos es limitado.

Ello dependerá del sector de actividad al que se refiera el código tipo pudiendo darse la circunstancia de que, en algunos de ellos, dada la novedad de la propia normativa, la producción de un efecto pedagógico que facilite su cumplimiento, pueda admitirse como un plus de efectividad. No obstante, este criterio de flexibilidad no debe tampoco permitir entender que, en cualquier caso, la mera reproducción de los preceptos legales sea suficiente para que el código tipo pueda ser inscrito en el Registro General de Protección de Datos. El análisis, por tanto, debe realizarse caso a caso con una valoración específica de las características del sector en el ámbito de la protección de datos.

En el ámbito comunitario la evaluación de los códigos tipo ha sido objeto de atención por parte del Grupo previsto en el Artículo 29 de la Directiva (el Grupo)1. El Grupo ha elaborado varios documentos que hacen referencia a esta cuestión.

Cronológicamente, el primer documento es el denominado "Primeras orientaciones sobre las transferencias de datos personales a terceros países - Posibles formas de evaluar su adecuación". Se trata de un documento de debate adoptado por el Grupo el 26 de junio de 1997.

Con posterioridad, en el año 1998, se han elaborado otros dos: El Documento de Trabajo "Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?, adoptado por el Grupo el 14 de enero, y el documento "Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo", aprobado el 10 de septiembre de aquel año.

El documento de 26 de junio de 1997, de carácter breve, se limita a explicitar los principios de contenido cuya inclusión en un código tipo se sugiere por el Grupo. El documento distingue entre principios básicos y principios adicionales. Los primeros comprenden todas las categorías básicas de la normativa de protección de datos en los siguientes términos.

Principio de limitación de objetivos: Los datos deberán tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el art. 13 de la Directiva.

Principio de proporcionalidad y de calidad de los datos: Los datos deberán ser exactos y, cuando sea necesario, estar actualizados. Los datos deberán ser adecuados, relevantes y no excesivos en relación al objetivo por el que se han transferido o por el que han sido nuevamente tratados.

Principio de transparencia: Deberá informarse a los interesados acerca de objetivo del tratamiento y de la identidad del responsable del tratamiento en el país tercero, y de cualquier otra cuestión siempre que resulte necesario para garantizar la equidad. Las únicas excepciones permitidas deberán corresponder a los arts. 11 (2) y 13 de la Directiva.

Principio de seguridad: El responsable del tratamiento deberá adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no deberá tratar los datos salvo por instrucción del responsable del tratamiento.

Derechos de acceso, rectificación y oposición.- El interesado deberá tener derecho a obtener una copia de todos los

datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado deberá también ser capaz de oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deberán estar en línea con el art. 13 de la Directiva.

Restricciones respecto a transferencias sucesivas a otros países terceros: Unicamente deberán permitirse transferencias sucesivas de datos personales del país tercero de destino a otro país tercero en el caso de que este último país tercero garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deberán estar en línea con el art. 26 de la Directiva.

Por su parte, los principios adicionales hacen referencia a tipos específicos de tratamientos de naturaleza diversa. Por un lado, atendiendo a la propia naturaleza de los datos, se incluyen principios aplicables a los datos "sensibles" -especialmente protegidos en la terminología de la LPD-, entre los que destaca la exigencia de consentimiento explícito por parte del afectado.

El documento de 26 de junio de 1997, es la pieza básica en lo que afecta al contenido de los códigos tipo y constituye el punto de referencia de los documentos posteriores que se remiten al mismo.

Por su parte, el documento de 14 de enero de 1998, más extenso que el anterior, enfoca la evaluación de los códigos tipo desde una perspectiva distinta. En efecto, mientras que el primero aborda exclusivamente el contenido del código, el segundo contiene una metodología de evaluación al margen de aquél, al que, sin embargo, se remite.

El primer criterio de evaluación afecta a una de las cuestiones tratadas anteriormente, como es la representatividad del sector. Este criterio de evaluación debe entenderse en la lógica de la Directiva que, como se señaló, circunscribe el ámbito de los códigos tipo a los de carácter sectorial. Nos encontramos, por tanto, ante un criterio de evaluación que, en el ámbito de la normativa española resultaría utilizable cuando se trate de códigos con tal carácter. Sin embargo, podría ser prescindible en nuestro derecho interno en los casos en que el código tipo se circunscriba a una sola empresa. Ello, no obstante, el resto de los criterios de evaluación contenidos en el documento serían también de utilidad en este último supuesto, como más adelante se verá.

Por lo demás, el criterio de evaluación basado en la representatividad del sector responde al interés de que la fuerza de la asociación permita hacer efectivo el cumplimiento del código, por su mayor capacidad para imponer sanciones a los miembros incumplidores.

Junto a este criterio básico, el documento incluye otros secundarios relacionados también con la mayor o menor representatividad del sector. Así, se estima que la fragmentación en la representatividad del sector puede producir confusión y opacidad en los consumidores, dificultar la investigación de los incumplimientos o la resolución de las denuncias que se planteen, en particular en sectores como el del marketing directo en el que, siendo habitual la transferencia de datos personales, unas empresas pueden estar sometidas al código y otras no.

Al margen de lo expuesto, el documento de 14 de enero de 1998 desarrolla una metodología de evaluación del código tipo distinguiendo entre la que tiene en cuenta el contenido del código y la que se centra en el análisis de su eficacia.

En el primer aspecto, el documento se remite esencialmente a los principios de contenido del de 26 de junio de 1997 considerando que tal evaluación tienen un carácter puramente objetivo. Sin embargo, añade alguna apreciación que no se refiere estrictamente al contenido, sino a otros aspectos vinculados al procedimiento de elaboración, a su transparencia y a la exigencia de niveles de protección adecuados respecto de empresas no acogidas al código. En este sentido, se valora positivamente la intervención de los afectados cuyos datos se tratan o de las asociaciones de consumidores en el proceso de elaboración del código, por la mayor probabilidad de que esta intervención permita un reflejo fiel de los principios garantes de la protección de datos; se destaca la sencillez, claridad y comprensión del lenguaje como un elemento esencial; y se estima apropiado que no se produzcan transferencias de datos a aquellas empresas ajenas al sector autorregulado o que no se sometan a la autorregulación, salvo que adopten medidas de protección adecuadas.

En este orden de cosas el documento delimita tres criterios que han de servir de guía para realizarla, consistentes en lograr un buen nivel de obediencia general, apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento y una reparación adecuada, en caso de incumplimiento. Para cada uno de ellos el documento incluye un "cuestionario" de preguntas que faciliten la evaluación.

La existencia de un buen nivel de obediencia general aparece relacionada con cuestiones tales como la difusión del código dentro del sector, la auditoría del nivel de cumplimiento y la existencia de un régimen sancionador, incluida la valoración que el incumplimiento del código pueda suponer para el infractor en orden a continuar desarrollando su actividad en el sector.

En lo que respecta al régimen sancionador y, aunque sea al socaire del análisis de los criterios de evaluación del código ético, es de interés formular algunas precisiones básicas.

La primera de ellas hace referencia a una cuestión estructural como es la de en qué medida la elaboración de un código ético puede o no condicionar la aplicación de las normas imperativas de protección de datos. La respuesta no puede ser más que una. Las normas de protección frente a tratamientos ilícitos de los datos personales, al ser dictadas en desarrollo de derechos fundamentales y tutelar el interés público son de aplicación plena y directa cualquiera que sea el contenido de un código tipo. En consecuencia si se produce una infracción de aquéllas procederá la actuación

inmediata de la autoridad de protección de datos.

La segunda afecta a la duda que pudiera suscitarse respecto a si el incumplimiento del contenido de un código tipo que, amplía la protección de datos personales más allá de las exigencias normativas, puede ser objeto de intervención por parte de tales autoridades. El incumplimiento de exigencias adicionales no permitiría actuar a las autoridades de protección de datos por cuanto, al menos en la LPD, dicho incumplimiento no estaría tipificado como infracción ni podría, por ello, sancionarse. Todo ello sin perjuicio de la intervención propia de los órganos de control que el propio código pueda establecer.

Por último, el documento de 10 de septiembre de 1998 ha sido elaborado desde una perspectiva radicalmente distinta de los comentados, refiriéndose exclusivamente a los procedimientos que deben seguirse para la presentación y evaluación de códigos de conducta comunitarios ante el Grupo regulado en el art. 29 de la Directiva. Este documento, tras recoger las definiciones básicas de Directiva, Grupo de Trabajo y código de conducta, regula las tres fases procedimentales previstas: Presentación y admisión, elaboración del dictamen por el Grupo de Trabajo y aprobación del mismo y notificación a los interesados.

3.- Experiencias prácticas

En lo que se refiere a la experiencia práctica sobre códigos de conducta, los supuestos en que se ha producido han sido los siguientes:

CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS EN TELEFONICA DE ESPAÑA

Solicitante: TELEFONICA DE ESPAÑA S.A.

Presentación e inscripción:1994

Objeto y ámbito de aplicación

Este código es desarrollado por Telefónica, que lo adopta mediante una decisión de empresa, con el fin de ceñirse en su gestión a la más estricta legalidad. Se desarrolla por medio de una normativa interna, que articula las prescripciones de la LORTAD en los diversos procesos de gestión empresarial de forma unitaria y homogénea.

El código se establece como una normativa de obligado cumplimiento para todas las Unidades de la Empresa y, en particular, para aquéllas que intervienen en la recogida, tratamiento y entrega de los datos de carácter personal obrantes en ficheros automatizados de Telefónica, así como para los directivos titulares de las Unidades designadas como responsables operativas de dichos ficheros.

CODIGO ETICO DE PROTECCION DE DATOS PERSONALES DE LAS EMPRESAS DE SERVICIOS COMERCIALES

Solicitante: ASOCIACIÓN MULTISECTORIAL DE LA INFORMACIÓN (ASEDIE)

Presentación e inscripción en 1999, sustituye al Código Ético de Protección de Datos Personales de las Empresas de Información Comercial, que había sido inscrito en 1995.

Objeto y ámbito de aplicación:

ASEDIE, consciente de la importancia de la labor de sus miembros, reconoce la necesidad para el sector de elaborar este Código Etico, con el fin de prevenir las violaciones de la privacidad de las personas que pudieran resultar del tratamiento de los datos personales.

El código se aplica a las relaciones que mantienen las empresas asociadas a ASEDIE con los comerciales o profesionales sobre los que se elaboran informes comerciales, con los usuarios de los mismos, así como a las relaciones que dichos asociados pueden mantener entre sí y con terceras personas, empresas, entidades u organismos relacionados de forma directa o indirecta con el ejercicio de la actividad de información comercial.

"REGLAMENTO DEL FICHERO HISTORICO DE SINIESTRALIDAD DE CONDUCTORES"

Solicitante: UNION ESPAÑOLA DE ENTIDADES ASEGURADORAS Y REASEGURADORAS (UNESPA)

Presentación:1998

Objeto y ámbito de aplicación:

El Fichero Histórico de Siniestralidad de Conductores, se fundamenta jurídicamente en el artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados que permite a las entidades aseguradoras establecer ficheros comunes tanto para la colaboración estadística como en la prevención del fraude en la selección de riesgos y en la liquidación de siniestros. El reglamento de regulación de este fichero pretende la adecuación a la LORTAD, especialmente en todo lo previsto en cuanto a garantizar los derechos de las personas cuyos datos son tratados en el mismo,

formulándolo como código tipo.

Se constituye desde la Comisión Técnica de Seguro de Automóviles de UNESPA, titular del fichero, y es de aplicación en todas las entidades aseguradoras adheridas a este fichero.

Este código tipo no ha sido inscrito, habiendose archivado, por no cumplirse los requisitos requeridos en cuanto a la comunicación al interesado de la inclusión de sus datos en este fichero.

Sin embargo, según la nueva redacción del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados, no se requerirá el consentimiento previo del interesado para la inclusión de sus datos en ficheros comunes, cuando la finalidad de estos sea prevenir el fraude en el seguro.

Teniendo en cuenta esta nueva situación, es posible que se presente un nuevo Código en el próximo año.

"CODIGO ETICO DE PROTECCION DE DATOS PERSONALES EN INTERNET"

Solicitante: FEDERACION ESPAÑOLA DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECEMD)

Presentación e inscripción:1998

Objeto y ámbito de aplicación:

Este código surge a través de la Asociación Española de Comercio Electrónico (AECE), actualmente FECEMD, que reconoce la necesidad de regular unas normas de compromiso voluntario por parte de las empresas que operan en Internet, con el fin de proteger la intimidad de las personas en el tratamiento automatizado de los datos de carácter personal en Internet.

Pueden adherirse al Código todas aquellas empresas que comercializan productos o servicios en Internet y tratan datos personales.

El código dedica un capítulo a establecer unos principios adicionales aplicables a las actividades on-line dirigidas principalmente a menores, los cuales en comparación con los adultos, pueden no entender la naturaleza de la información que se les pide o los usos a los cuales se puede destinar la información.

"CODIGO ETICO DE PROTECCION DE DATOS PERSONALES DE LA ASOCIACION DE PUBLICIDAD DIRECTA Y BASES DE DATOS PD&BD"

Solicitante: ASOCIACION DE PUBLICIDAD DIRECTA Y BASES DE DATOS PD&BD

Presentación en 1999. Ha quedado archivado por desistimiento de la Asociación.

Objeto y ámbito de aplicación:

Tiene por objeto la regulación del uso de las tecnologías de la información y singularmente de la informática, en su aplicación al tratamiento informatizado de los datos personales por parte de las empresas miembro de la PD&BD, desarrollando en este código términos establecidos en la LORTAD.

Quedan sujetas a este Código cualesquiera actividades de tratamiento automatizado de datos personales, ya sea de naturaleza principal o accesoria e incluso las previas o posteriores al tratamiento automatizado propiamente dicho, realizadas por los asociados a la PD&BD.

"CODIGO ETICO DE PUBLICIDAD EN INTERNET"

Solicitante: ASOCIACION DE AUTOCONTROL DE LA PUBLICIDAD AAP

Presentación e inscripción en 1999

Objeto y ámbito de aplicación:

Este código tiene por objeto cubrir el vacío que sobre conductas publicitarias, en general, existe en el entorno de Internet estableciendo unas normas mínimas sobre la publicidad en Internet, partiendo del principio de control en origen, que son adoptadas de forma voluntaria por los sectores integrados en la AAP.

Al establecer el principio de control en origen, se siguen las recomendaciones que las instituciones comunitarias europesa propugnan en el Libro Verde sobre la Comunicación Comercial, y se asegura la efectividad a la hora de establecer los mecanismos que aseguran el cumplimiento del Codigo.

En el ámbito deontológico, este Código Ético tiene vocación de complementariedad con el establecido por la Federación Española de Comercio Electrónico y Marketing Directo.

MEMORIA DE 1999 - ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES DE LOS DISTINTOS PAÍSES EN MATERIA DE PROTECCIÓN DE DATOS.

1. UNIÓN EUROPEA. GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES CREADO POR LA DIRECTIVA 95/46/CE

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo aprobaron la Directiva 95/46/CE 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 (designada en lo sucesivo "la Directiva"). El artículo 29 de la Directiva creó el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Este grupo tiene, entre otras funciones, la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal en la Comunidad y en terceros países.

El Grupo de Trabajo se compone de representantes de las autoridades nacionales independientes encargadas de la protección de datos y un representante de la Comisión. Asimismo, incluirá en el futuro un representante de la autoridad responsable de las cuestiones relacionadas con la protección de datos dentro de las instituciones europeas, a partir de la fecha en que entre en vigor el Reglamento regulador de dicha institución, que se encuentra en la actualidad en fase de discusión, habiendo sido ya sometido por el Gobierno Español al parecer de la Agencia de Protección de datos una versión preliminar del mismo. Por último, pueden asistir a las reuniones del Grupo, en calidad de observadores, representantes de las Autoridades de Control existentes en los Estados signatarios del Convenio sobre el Espacio Económico Europeo, no integrantes de la Unión Europea (Noruega, Islandia y Liechtenstein).

Al compartir la experiencia de las autoridades nacionales, el Grupo de Trabajo impulsa la aprobación de una estrategia coherente para la aplicación de los principios generales enunciados en la Directiva, aconsejando a la Comisión en aquellas cuestiones que se encuentran relacionadas con la protección de datos.

Por otra parte, una de las funciones principales del Grupo de Trabajo es la de formular dictámenes sobre el nivel de protección en la Unión y en los terceros países, y en emitir recomendaciones sobre cualquier cuestión referente a la protección de las personas con respecto al tratamiento de datos de carácter personal, pudiendo instarse por las propias Autoridades integrantes del Grupo la formación de grupos de estudio de determinadas cuestiones.

El Grupo de Trabajo se reunió por primera vez el 17 de enero de 1996, iniciándose su actividad a instancia de las propias autoridades nacionales responsables de la protección de datos, aún cuando la Directiva no se encontraba aún en vigor.

La Agencia de Protección de Datos española forma parte de este Grupo de Trabajo, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Como fruto de este trabajo y en el ejercicio de las competencias atribuidas por la Directiva el Grupo de Trabajo del Artículo 29 ha elaborado los siguientes documentos durante 19991:

1.- Dictamen 1/99, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos Adoptado por el Grupo de trabajo el 26 de enero de 1999 (DG XV D 5092/98/final WP 15).

2.- Documento de trabajo: Tratamiento de datos personales en Internet. Aprobado por el Grupo de Trabajo el 23 de febrero de 1999 (DG XV D 5013/99/final WP 16)

3**.-** Recomendación 1/99, sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware* , aprobada por el Grupo de Trabajo el 23 de febrero de 1999 (DG XV D 5093/98/final WP 17)

4.- Recomendación 2/99, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de Mayo de 1999 (DG XV D 5005/99/final WP 18)

5.- Dictamen 2/99, relativo a la idoneidad de los "Principios internacionales de puerto de seguro" que hizo públicos el Departamento estadounidense de Comercio el 19 de abril de 1999, adoptado el 3 de mayo de 1999 (DG XV D 5047/99/inal WP 19)

6.- Dictamen 3/99 relativo a la Información del sector público y protección de datos personales. Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea Titulado La información del sector público: un recurso clave para Europa" COM(1998) 585, Aprobado el 3 de mayo de 1999 (WP 20).

7.- Dictamen 4/99, relativo a las "preguntas más frecuentes" que hará públicas el Ministerio de Comercio de los EE. UU. en relación con la propuesta de principios de puerto seguro, aprobado el 7 junio de 1999 (DG XV D 5066/99/final WP 21).

8.- Dictamen 5/99, sobre el nivel de protección de los datos personales en Suiza, adoptado el 7 de junio de 1999 (DG XV D 5054/99/final WP 22).

9.- Documento de trabajo sobre el estado del debate entre la Comisión Europea y el Gobierno de los Estados Unidos acerca de los "Principios internacionales de puerto seguro", aprobado el 7 de julio de 1999 (DG XV D 5075/99/final WP 23)

10.- Dictamen 6/99, sobre el nivel de protección de los datos personales en Hungría, aprobado el 7 de septiembre de 1999 (DG XV D 5070/99/final WP 24)

11.- Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobado el 7 de septiembre de 1999 (DG XV D 5085/99/final WP 25).

12.- Dictamen 4/99, relativo a la Inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales, aprobado el 7 de septiembre de 1999 (DG XV D 5143/99/final WP 26).

13.- Dictamen 7/99, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE.UU, aprobado el 3 de diciembre de 1999 (DG XV D 5146/99/final WP 27).

Al propio tiempo, a lo largo de 1999, el Grupo de Trabajo ha analizado la existencia de un nivel adecuado de protección en otros terceros Estados, así como la evolución de las reuniones entre los representantes de la Comisión y otras Entidades y Asociaciones con vista a la aprobación de modelos contractuales de transferencia internacional de datos y la adopción de Códigos Tipo en el seno de diversos sectores de actividad, siguiendo los criterios establecidos en los diversos documentos que fueron aprobados a lo largo de 1998, a los que ya se hizo referencia en la Memoria Anual de la Agencia de Protección de datos correspondiente a ese año. Asimismo, el Grupo de Trabajo ha centrado buena parte de sus reuniones en el análisis de los nuevos acontecimientos producidos, esencialmente a nivel legislativo, en los Estados miembros.

Como puede comprobarse, de lo indicado hasta ahora se desprende la necesidad de referirnos separadamente a los distintos campos de actividad del Grupo de Trabajo, haciendo en primer lugar una, siquiera somera, referencia a los problemas derivados de la transposición de la Directiva, refiriéndonos posteriormente a aquellas materias en que la producción del Grupo de Trabajo ha revestido una mayor relevancia: el análisis de la concurrencia de un nivel adecuado de protección en terceros Estados y el estudio de diversas cuestiones relacionadas con el fenómeno de Internet.

1.1.- LA TRANSPOSICIÓN DE LA DIRECTIVA

Cada vez que se ha reunido, el Grupo ha venido efectuando un seguimiento constante del grado de transposición de la Directiva 95/46 por parte de los Estados miembros.

En este sentido, se ha tratado de instar a aquellos Estados que no habían cumplido con la transposición en el plazo establecido al efecto (que concluyó el 24 de octubre de 1998) para que adoptaran las medidas necesarias a la mayor brevedad. Así, está previsto que en los primeros meses del año 2000 se adopte por el Grupo una recomendación, dirigida a los Estados miembros que no han cumplido debidamente con el deber de transposición lo adopten en el plazo más breve posible.

Por otro lado, el Grupo de Trabajo trata de vigilar que las tareas de transposición no incrementen las diferencias existentes en la actualidad entre las diversas legislaciones de la Unión Europea en materia de protección de datos personales, lo que haría inviable el deseo de eliminar los obstáculos a la circulación de datos personales. Con ello se trata de hacer posible que, como señala el considerando octavo de la Directiva, el nivel de protección de los derechos y libertades de las personas, en lo que se refiere al tratamiento de dichos datos, sea equivalente en todos los Estados miembros.

En cuanto al cumplimiento del plazo fijado para la transposición de la Directiva, la mayoría de los Estados miembros han incumplido el citado plazo, aun a pesar de haberse iniciado en tiempo y forma la tramitación parlamentaria de las normas de transposición. Ello se ha debido en parte a que las tareas de transposición no se agotan con las adaptación de la normativa interna a la Directiva 95/46/CE, sino que a ello debe añadirse, las necesarias incorporación al derecho interno la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones. Además, en algunos países, como Suecia, ha sido necesaria una modificación constitucional para poder adoptar la Directiva.

Al final de 1999, y dejando a un lado los supuestos de España, Austria y Reino Unido, en que, pese a no haber entrado en vigor, ya ha sido promulgada una Ley que transpone las previsiones de la Directiva al derecho interno, no habían concluido los trabajos de transposición en Dinamarca, Alemania, Francia, Irlanda, Luxemburgo y Países Bajos, lo que puede motivar una denuncia a estos Estados por parte de la Comisión durante el año 2000.

1.2.- ANÁLISIS DE LA EXISTENCIA DE UN NIVEL ADECUADO DE PROTECCIÓN EN TERCEROS ESTADOS

1.2.1.- Introducción

Es necesario, antes de entrar en el análisis de los supuestos concretos objeto de estudio en el año 1999, tomar en cuenta los criterios sentados por el propio Grupo de Trabajo para la apreciación de la existencia de un nivel adecuado de protección de datos en Estados no miembros de la Unión Europea, contenidos fundamentalmente en el documento

de trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998 (DG XV D/5025/98 WP 12).

El objetivo de la protección de datos es ofrecer asistencia a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU (1990). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince Estados de la Comunidad.

Es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas. En Europa las legislaciones han incluido en general las normas de procedimiento como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos relativos al procedimiento están plasmados en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones.

Fuera del ámbito comunitario es menos común encontrar estos medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos. Los signatarios del Convenio 108 deben incorporar los principios de la protección de datos en su legislación, pero no se requieren mecanismos complementarios tales como una autoridad de control. Las directrices de la OCDE sólo exigen que "se tengan en cuenta" en la legislación nacional y no prevén procedimientos para garantizar que las directrices deriven en una protección efectiva de las personas físicas.

Por otro lado, las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento y de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. El grado de riesgo que, en el caso de una transferencia internacional, supone para el interesado será un factor importante para determinar los requisitos concretos de un caso determinado.

1.2.2.- Principios fundamentales de la protección de datos

Principio de limitación de objetivos (finalidad) - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por alguna de las razones expuestas en el artículo 13 de la Directiva.

Principio de proporcionalidad y de calidad de los datos - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

Principio de transparencia (información en la recogida de los datos) - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2, 3 y 13 de la Directiva.

Principio de seguridad - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

Derechos de acceso, rectificación y oposición - el interesado debe tener derecho a obtener una copia de todos los datos relativos a su persona, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento sus datos personales. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

Restricciones respecto a transferencias sucesivas a otros terceros países -únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.

Además, deben aplicarse otros principios adicionales a tipos específicos de tratamiento como a los **datos sensibles, la publicidad directa -** con la posibilidad de negarse a transferencias de datos cuyo fin sea la publicidad directa, o la **decisión individual automatizada -** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

1.2.3.- Objetivos de un sistema de protección de datos

Los objetivos de un sistema de protección de datos son básicamente tres:

a) Asegurar un **nivel satisfactorio de cumplimiento** de las normas. Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

b) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello, es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

c) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

1.2.4.- Aplicación práctica de estos criterios durante 1999.

Tomando estos datos en consideración, el procedimiento seguido por el Grupo de Trabajo consiste en un estudio preliminar de la legislación existente en el Estado objeto de análisis (referida no solo a la protección de datos sino a cualesquiera otras cuestiones que puedan encontrarse relacionadas con esta materia, como por ejemplo, el régimen de las telecomunicaciones), llevado a cabo, generalmente por los servicios de la Comisión Europea. Este estudio es sometido al Grupo, a fin de que manifieste su parecer, planteando las cuestiones que resulten discutibles o dudosas. Las cuestiones son planteadas a las autoridades del tercer Estado por la Presidencia del Grupo, pudiendo, en caso de estimarse necesario, plantear cuestiones adicionales en una reunión del Grupo con las citadas autoridades. Cumplidos estos trámites, el Grupo de Trabajo, en caso de apreciar la existencia de un nivel adecuado de protección, aprueba un dictamen en ese sentido, sometiendo la cuestión al Comité regulado por el artículo 31 de la Directiva, de cara a la adopción de una decisión definitiva sobre la cuestión por parte de la Comisión Europea.

Siguiendo este procedimiento se han aprobado a lo largo de 1999 sendos dictámenes favorables a la consideración de Suiza y Hungría como Estados que conceden un nivel adecuado de protección, fundándose tales consideraciones en el hecho de que la protección de datos de carácter personal aparece reconocida como derecho fundamental en sus textos constitucionales, en que ambos Estados son signatarios del Convenio 108 del Consejo de Europa, en la existencia de sendas leyes nacionales reguladoras de la protección de datos de carácter personal, que establecen un régimen sustancialmente similar al recogido en la Directiva y en la existencia en ambos casos de una Autoridad independiente de control.

Asimismo, durante 1999 se ha iniciado el análisis del régimen existente en otros terceros Estados, tales como Eslovaquia, Eslovenia o Polonia y los territorios extracomunitarios británicos de la Isla de Man, Guernsey y Jersey, siendo probable que, en algunos de estos supuestos, se adopte una resolución definitiva a lo largo del próximo año.

1.2.5.- Estudio especial del nivel de protección en los Estados Unidos. Los llamados "Principios de Puerto Seguro".

Sin embargo, como puede fácilmente deducirse de la lista de los documentos elaborados por el Grupo de Trabajo, la mayor parte de los esfuerzos desarrollados por el Grupo durante 1999, y previsiblemente durante el año 2000, se centrarán en el análisis de la existencia de un nivel adecuado de protección de datos en los Estados Unidos de América.

Frente al estudio de otros Estados, en los que el punto de partida para el análisis de la cuestión ha sido el estudio de una legislación de protección de datos aplicable en todo el territorio del estado, el problema de partida para el análisis de la cuestión en los Estados Unidos se centra en el hecho de que no existe, dado el marcado carácter autorregulador del comercio en dicho país, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos.

En efecto, la protección de la intimidad y de los datos en Estados Unidos se enmarca en un complejo entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial. En este sentido, el Grupo de trabajo ha considerado que este conjunto de leyes sectoriales muy segmentadas y la autorregulación voluntaria no son suficientes para proporcionar protección adecuada en todos los casos a los datos personales transferidos desde la Unión Europea.

A fin de superar los problemas derivados de esta dispersión normativa, el Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, los operadores debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.

El texto de los principios se dividía en siete apartados, dedicados a las materias más importantes recogidas en los Acuerdos y normas fundamentales sobre protección de datos, así como a la aplicación de los principios.

Por otra parte, durante el desarrollo de las negociaciones, los principios se vieron complementados por una serie de "preguntas más frecuentes" (FAQ), en que se daba explicación a los principios, modificando en muchos de los supuestos el contenido que parecía derivarse de los mismos. El Grupo de Trabajo exigió, a la vista de estas FAQ que se otorgara a las mismas el mismo grado de obligatoriedad que a los principios, constituyendo aquéllas y éstos un único cuerpo normativo.

Partiendo de esta configuración, el Grupo de Trabajo manifestó en su Dictamen 1/99, la posibilidad del establecimiento en EE.UU. de un modelo de norma consensuada de protección en forma de conjunto de principios de "puerto seguro" ofrecidos a todos los agentes económicos y a los operadores de EE.UU, como planteamiento útil que quizá debería complementarse con soluciones contractuales en algunos casos específicos, siempre y cuando dichos principios tuvieran un carácter obligatorio para aquellos operadores que decidieran adherirse a los mismo, estableciéndose un mecanismo de control y sanción en caso de incumplimiento de los principios y un mecanismo que evitara la transmisión de los datos por parte de las empresas que recibieran los datos al amparo de su adhesión. Asimismo se consideró preciso que se estableciera un procedimiento que asegurara el desenvolvimiento de los derechos de acceso, rectificación, cancelación y oposición por parte de los nacionales de los Estados miembros de la Unión Europea cuyos datos fueran transferidos, asegurándose el pleno desarrollo de esos derechos y la resolución de las quejas que pudieran plantearse ante autoridades independientes que, en su caso, impondrían el abono de las correspondientes indemnizaciones a los afectados.

Por último, se indicó que cualquier conjunto aceptable de principios de "puerto seguro" debería, como requisito mínimo, incluir todos los principios establecidos en las directrices sobre protección de la intimidad ("Privacy guidelines") de la OCDE de 1980, adoptadas entre otros países por Estados Unidos.

A lo largo de 1999, y a partir de la opinión manifestada en el Dictamen citado, se sometieron al parecer del Grupo de Trabajo cuatro versiones de los citados principios de "puerto seguro", dictándose otros tantos documentos por parte del Grupo, en que se manifestaron aquellos aspectos de los mismos que se consideraron insuficientes frente al nivel de protección mínimo requerido para que pudiera considerarse posible recomendar una decisión afirmativa a la Comisión Europea.

En estas opiniones se ha puesto de manifiesto la existencia de diversos problemas que dificultan la posibilidad de llegar a una opinión definitiva sobre esta cuestión, y que pueden resumirse en los siguientes:

1.- Dificultad en la comprensión de los principios, como consecuencia de la aparición de las FAQ que, en muchos casos excepcionan el régimen general contenido en los principios, remitiéndose a normas sectoriales norteamericanas o a otras FAQ, lo que imposibilita un adecuado conocimiento del verdadero nivel de protección de datos otorgado en cada caso concreto.

2.- Ausencia de un mecanismo ágil y adecuado para la satisfacción de los perjuicios causados a los nacionales de los Estados miembros de la Unión Europea como consecuencia de un incumplimiento por parte de las empresas adheridas al Puerto Seguro de los principios contenidos en el mismo

3.- Inexistencia de mecanismos que aseguren, en la práctica, el cumplimiento de los principios, garantizando la imposición de sanciones a las entidades adheridas que los incumplan.

4.- Falta de mecanismos previstos para evitar que, una vez producida la transferencia a los Estados Unidos, los datos sigan protegidos por un nivel de protección adecuado, siendo posible que los mismos sean cedidos a otras terceras entidades en cualquier lugar del mundo.

5.- Imposibilidad de conocimiento por parte de los nacionales Estados miembros de la Unión Europea y de las propias autoridades de control de las empresas adheridas al "puerto seguro" y de las medidas adoptadas en caso de incumplimiento.

6.- Falta de adecuación de alguno de los principios con los criterios derivados de las directrices de la OCDE y, aún en mayor medida, de las normas europeas de protección de datos.

7.- Falta de mecanismos de verificación por parte de las autoridades federales de los Estados Unidos, a fin de comprobar el cumplimiento de los principios por parte de las empresas adheridas. Estos mecanismos se reemplazan por un sistema de "autoverificación".

Como consecuencia de lo que se ha venido exponiendo, en el último dictamen aprobado durante el año 1999 (dictamen 7/99, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE.UU), aprobado el 3 de diciembre de 1999, el Grupo de Trabajo consideró que los acuerdos de «puerto seguro» propuestos, tal como quedan reflejados en las versiones actuales de los diversos documentos, continúan siendo insatisfactorios, invitando a la Comisión a que inste a la parte estadounidense a realizar una serie de mejoras clave, en particular las siguientes:

- Especificar el alcance del «puerto seguro» y, en especial, eliminar todo posible malentendido referido a que las entidades de EE.UU. pueden optar por basarse en los principios de «puerto seguro» en circunstancias en las que es de aplicación la propia Directiva.

- Facilitar acuerdos más fiables que permitan identificar con seguridad a los participantes en el «puerto seguro» y evitar el riesgo de continuar otorgándoles los beneficios del «puerto seguro» cuando, por un motivo u otro, hayan sido eliminados de la lista.

- Afirmar sin ningún asomo de duda que todos los participantes en el «puerto seguro» están sujetos a la jurisdicción de un organismo público con las facultades apropiadas para controlar su aplicación.

- Establecer la norma de que los organismos de resolución de conflictos del sector privado deben remitir las quejas no resueltas a uno de estos organismos públicos.

- Eliminar las generalizaciones y ambigüedades de las excepciones y exenciones permitidas, de manera que las excepciones sean precisamente eso, es decir, que se apliquen solamente cuando sea necesario y en la medida requerida, y que no sean invitaciones generales para hacer caso omiso de los principios. Esto cobra especial importancia en relación con el derecho de acceso.

- Reforzar el principio de opción, que es el elemento decisivo del enfoque de los EE.UU.

Por último, el Grupo de Trabajo destaca la importancia de continuar e incluso acelerar el trabajo sobre las cláusulas de los contratos tipo, con el objeto de tomar una o varias decisiones en virtud del apartado 4 del artículo 26 de la Directiva, lo que constituye una parte importante de la simplificación y transparencia de las salvaguardias necesarias para la transmisión a zonas en las que no hay otros medios de garantizar la protección adecuada.

En este sentido, debe recordarse que, como ya se ha indicado en otro lugar de esta Memoria, la Agencia de Protección de Datos ha continuado durante 1999 autorizando aquellas transferencias de datos que se han verificado mediante la celebración de contratos entre exportador e importador no situado en un Estado que concediera un nivel adecuado de protección de datos, en virtud de cláusulas que han sido consideradas como adecuadas. La celebración de estos contratos ha permitido que, a lo largo de 1999, se produjera la libre transferencia de datos a los Estados Unidos, entre otros, sin que ello menoscabara las garantías que la Directiva y la Ley española consagran a favor de las personas a que los datos se refieren.

Las negociaciones relativas a los principios de "puerto seguro" continuarán a lo largo del año 2000, si bien es previsible que, dado el estado en que se encuentra esta materia al final de 1999, no se alcance un acuerdo definitivo antes de 31 de marzo de 2000, fecha prevista por la Comisión Europea y las autoridades Norteamericanas para la finalización del Acuerdo.

1.3.- ACTUACIÓN DEL GRUPO DE TRABAJO EN RELACIÓN CON INTERNET

Ya en 1997 (Recomendación 3/97: Anonimato en Internet) y en 1998 (Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma Abierta de Perfiles (OPS)) el Grupo del Artículo 29 mostró su preocupación por determinados aspectos relacionados con el tratamiento de datos personales en Internet.

No obstante, dada la cada vez mayor penetración de Internet en todos los ámbitos de la Sociedad de la Información, en 1999 el Grupo estimó la conveniencia de formar un subgrupo especializado (Grupo Operativo de Internet) con miembros de las distintas autoridades de control provenientes tanto del campo del Derecho como de las Tecnologías de la Información para proceder a un estudio sistemático de aquellos temas o categorías de tratamientos en Internet que tuvieran una mayor incidencia sobre la intimidad de las personas.

Fruto del trabajo de este Grupo Operativo, durante 1999 se elaboraron tres documentos, que fueron remitidos al plenario del Grupo para su discusión y que fueron posteriormente aprobados. Dichos documentos son:

- Tratamiento de datos personales en Internet

- Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware

- Recomendación 3/99 sobre la conservación de los datos de tráfico por los proveedores de servicios de Internet a efectos de cumplimiento de la legislación

A continuación, analizaremos estos textos:

1.3.1.- Documento de trabajo sobre el tratamiento de datos personales en Internet (aprobado por el Grupo de Trabajo el 23 de febrero de 1999).

El documento tiene por objeto poner simplemente de manifiesto la problemática derivada del fenómeno Internet, aclarando su estrecha vinculación con la protección de datos de carácter personal. Así, en su apartado primero, el documento viene a poner de manifiesto los distintos aspectos que configuran la problemática derivada de la irrupción de Internet, indicando que dicha irrupción supone un nuevo desafío por los siguientes motivos:

1.- La utilización de la infraestructura suele estar directamente basada en el tratamiento de datos personales, como ocurre con determinadas direcciones de protocolo Internet.

2.- Los servicios proporcionados a través de esa infraestructura ofrecen nuevas posibilidades especialmente las relativas a la distribución de información que incluya datos personales (por ej. Listas de direcciones, grupos de discusión, acceso a bases de datos, etc.).

3.- Los instrumentos técnicos son nuevos, por ejemplo el *software* de navegación, y evolucionan a un ritmo muy rápido.

4.- Muchos actores son también nuevos para las nuevas actividades comerciales en línea que implican el tratamiento de datos personales y los límites tradicionales entre las diferentes profesiones se encuentran en un proceso de redefinición igualmente rápido.

5.- Uno de los usos de Internet que plantea mayores desafíos es hacer negocios en línea: el comercio electrónico consiste en vender directamente y de forma privada de las empresas a los consumidores sin ningún tipo de intermediario, utilizando nuevos métodos de selección y nuevos medios de pago.

6.- La dimensión global está inmediatamente presente.

Tras esta exposición, y recordando los distintos foros internacionales en que la cuestión ha sido especialmente analizada en la vertiente tocante a la protección de datos, el documento señala que el tratamiento de los datos personales en Internet debe respetar los principios de protección de datos al igual que en el mundo convencial (off-line). Esto no constituye una limitación de la utilización de Internet, sino que, por el contrario, forma parte de los requisitos fundamentales destinados a garantizar la confianza de los usuarios en el funcionamiento de Internet y los servicios que se facilitan mediante esa red. La protección de datos en Internet es, por tanto, una condición indispensable par el desarrollo del comercio electrónico.

Del mismo modo, el Documento recuerda que, como consecuencia de lo ya indicado, el tratamiento de los datos a través de Internet se encuentra sujeto a la Directiva 95/46/CE, que hace referencia a cualquier tipo de tratamiento de datos personales dentro de su campo de acción, con independencia de los medios técnicos utilizados, y a la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, dado que Internet es una red de ordenadores abierta a todo el mundo y, por ello, forma parte del sector público de telecomunicaciones.

Concluye el documento indicando que el Grupo Operativo Internet, creado en el seno del Grupo de Trabajo, va a seguir trabajando de manera más general sobre la aplicación de las dos directivas al tratamiento de datos personales en Internet y presentará propuestas sobre la forma de llevar a la práctica sus disposiciones de manera homogénea, por ejemplo en relación con los servicios de correo electrónico y los datos sobre el tráfico en Internet.

1.3.2. - Requisitos del software y hardware en internet (recomendación 1/99, adoptada el 23 de febrero de 1999).

Si las recomendaciones anteriores del Grupo de Trabajo (especialmente la Recomendación 3/97, sobre anonimato en Internet) centraban su preocupación en la necesidad de que el usuario no se viera compelido a la revelación de sus datos al servirse de las distintas posibilidades que le ofrece la red, la Recomendación 1/99 toma como referente el hecho de que, en muchas ocasiones, el interesado no tiene conocimiento de que determinados datos referidos al mismo pueden ser captados como consecuencia del software y hardware empleado para la navegación. Se plantean en especial los problemas derivados de los datos almacenados en el navegador y de la existencia de cookies.

Así lo indican los antecedentes de la propia recomendación, cuando se recuerda que el Grupo de Trabajo está especialmente preocupado por los riegos inherentes al tratamiento de los datos personales sobre personas que desconocen por completo tal tratamiento.

A partir de esta consideración, la Recomendación insta a los diseñadores de software y hardware a tomar en consideración y respetar los principios de las directivas 95/46/CE y 997/66/CE con objeto de incrementar la intimidad de los usuarios de Internet, partiendo del respeto a los principios de consentimiento informado, finalidad y del derecho del interesado a decidir sobre el tratamiento de sus propios datos.

Resumiendo el contenido de la Recomendación, más depurada desde el punto de vista de aplicación de la legalidad vigente en materia de protección de datos, deben ponerse de manifiesto las siguientes conclusiones

1.- Una condición para el tratamiento legítimo de los datos personales es que se informe al interesado y se le tenga al corriente del tratamiento en cuestión (principio de consentimiento informado), por lo que se insta a la industria informática a trabajar en productos que respeten la vida privada y se ajusten a la normativa europea en materia de protección de datos.

2.-Tomando en consideración el derecho de información, vinculado al consentimiento, los productos (*software y hardware*) de Internet deberían proporcionar a los usuarios de la red información sobre los datos que pretenden recopilar, almacenar o transmitir y el fin para el que son necesarios. Esto significa, por ejemplo, que:

En el caso de un navegador, al establecer una conexión con un servidor web se informa al usuario de qué información se pretende transferir y con qué objetivo.

En el caso de existencia de "hipervínculos" que envía un sitio web a un usuario por el medio que sea, el navegador del

usuario debería indicárselos en su totalidad.

En caso de "cookies", debería informarse al usuario cuando está previsto que el software de Internet reciba, almacene o envíe una "cookie".

3.- Los productos (*software y hardware*) de Internet deberían asimismo permitir al usuario de los datos un fácil acceso a cualquier dato recopilado que le concierna personalmente, garantizando el desenvolvimiento de los derechos de acceso, rectificación y cancelación.

Habida cuenta de lo anterior, se establecen dos consecuencias:

1.- La configuración de los productos informáticos (*hardware y software*) no debería, por defecto, permitir la recopilación, almacenado o envío de información persistente del cliente.

2.- Los productos Internet (*hardware y software*) deberían permitir al interesado decidir libremente en cuanto al tratamiento de sus datos personales ofreciéndole instrumentos de fácil manejo para filtrar (es decir rechazar o modificar) la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados (incluidos los perfiles, el dominio o la identidad del servidor Internet, el tipo y duración de la información recopilada, almacenada o enviada y así sucesivamente). Esto supone que:

- el software navegador debería proporcionar opciones para que el usuario pueda configurar el navegador, especificando el tipo de información que debería o no debería recopilar y transmitir.

- en el caso de las "cookies", el usuario debería contar siempre con la opción de aceptar o rechazar el envío o almacenamiento de una "cookie" en su totalidad

1.3.3.- Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación (aprobado el 7 de septiembre de 1999).

La tercera de las recomendaciones directamente relacionadas con Internet se centra en el problema de la conservación de los datos de facturación por parte de los proveedores de este tipo de servicios, tomando en consideración el hecho de que los mismos tienen la condición de proveedores de servicios de telecomunicaciones.

La recomendación recuerda que, como norma general, los datos sobre tráfico deben destruirse o hacerse anónimos en cuanto termine la comunicación (apartado 1 del artículo 6 de la Directiva 97/66/CE). Ello se debe al carácter confidencial de los datos sobre tráfico que permiten obtener perfiles individuales de comunicación incluyendo fuentes de información y ubicación geográfica del usuario y a los posibles efectos perniciosos sobre la intimidad resultantes de la recopilación, difusión o uso posterior de dichos datos. En el apartado 2 del artículo 6 se incluye un excepción relativa al tratamiento de datos sobre tráfico a los efectos de la facturación de los usuarios y de los pagos de las interconexiones, pero únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Por último, el apartado 1 del artículo 14 permite a los Estados miembros limitar el alcance de las obligaciones y derechos que se establecen en el artículo 6 cuando dichas limitaciones constituyan una medida necesaria para la salvaguardia de la seguridad nacional y la prevención, investigación, detección y represión de infracciones penales tal como se indica en el apartado 1 del artículo 13 de la Directiva 95/46/CE.

De estas disposiciones se deduce que los operadores de telecomunicaciones y los proveedores de servicio Internet no pueden recopilar y almacenar datos amparándose en la necesidad de controlar el cumplimiento de la legislación, a menos que así se les exija legalmente, de conformidad con los motivos y condiciones antes mencionados.

Por otra parte, se pone de manifiesto que el período de conservación de los datos sobre facturación y tráfico difiere ampliamente en los distintos estados miembros, llegando en algunos supuestos, como el caso de Francia, a 10 años (coincidentes con el período de prescripción del derecho a reclamar el pago de la factura telefónica). Del mismo modo, se pone de manifiesto que tampoco es homogénea la práctica habitual de los proveedores de servicio Internet: parece que los pequeños proveedores conservan los datos sobre tráfico durante periodos muy breves (unas horas) debido a falta de capacidad de almacenamiento, mientras que los proveedores más importantes, que pueden permitirse disponer de capacidad de almacenamiento, pueden conservar los datos sobre tráfico durante unos meses (pero todo depende de su política de facturación: por tiempo de conexión o por periodos fijos).

Todas estas divergencias podrían plantear obstáculos en el mercado interior para la prestación transfronteriza de servicios de telecomunicación e Internet, dada la existencia de plazos divergentes entre la legislación nacional del operador y la propia del usuario de los servicios, lo que podría generar dudas a aquél acerca del tiempo en que debe conservar los datos de facturación.

Ante esta situación, el Grupo considera que los medios más eficaces para evitar riesgos inaceptables a la intimidad y reconocer simultáneamente la necesidad de una ejecución eficaz de la ley es que, en principio, los datos sobre tráfico no deberán conservarse a efectos exclusivos de control y que las legislaciones nacionales no deberían obligar a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicios Internet a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación.

En este mismo sentido, el Grupo recomienda que la Comisión Europea proponga medidas apropiadas para una mayor armonización del plazo durante el cual se permite a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicio Internet conservar los datos sobre tráfico para facturación y pago de interconexiones. El Grupo considera que este plazo deberá ser suficiente para permitir a los consumidores impugnar la factura, pero lo más breve posible para no sobrecargar a los operadores y proveedores de servicios y para respetar los principios de proporcionalidad y especificidad como componentes del derecho a la intimidad, debiendo este plazo ser conforme con los mayores niveles de protección observados en los Estados miembros.

1.3.4.- Conclusiones.

Las principales conclusiones de los documentos adoptados se pueden resumir en los siguientes puntos:

- No existe un vacío legal en Internet. Tanto la Directiva 95/46/CE y la Directiva 97/66/CE como las Leyes nacionales aprobadas a consecuencia de la transposición de las mismas, son aplicables a Internet, lo que implica que tanto los principios de protección de datos como los derechos de los ciudadanos en relación con la protección de sus datos personales son exigibles cuando los tratamientos se realizan en Internet.

- Hay que informar explícitamente al usuario de Internet de qué datos se le están recabando, ya sea de forma explícita o implícita, dándole la oportunidad de oponerse al tratamiento de los mismos.

- Los datos sobre tráfico no deberían conservarse a efectos exclusivos de control de cumplimiento de la ley por los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicio de Internet, no debiendo establecerse obligaciones legales sobre la conservación de estos datos de tráfico durante un plazo de tiempo superior al necesario para cubrir las necesidades sobre reclamaciones respecto de la facturación.

Está previsto que el Grupo Operativo continúe sus trabajos a lo largo del año 2000 para, de esta manera, poder disponer de un documento general que aborde todos los aspectos en los que el tratamiento de datos personales en Internet es relevante. Dicho documento, que será sometido al plenario del Grupo del Artículo 29, se estima que servirá como referencia para hacer llegar a los distintos estamentos de la Unión Europea la opinión de las autoridades de control sobre esta materia. Además, constituirá una herramienta muy útil en el ámbito nacional como directriz para abordar de forma armonizada los distintos problemas que puedan plantearse.

2.- CONSEJO DE EUROPA

En 1981 se firmó el Convenio 108 para la protección de los individuos en relación con el tratamiento automatizado de datos. Este Convenio permitía, en principio, el libre flujo de datos personales entre los Estados que son parte del mismo, flujo que sólo podría impedirse en los supuestos en que dichos Estados dejen de ser parte del Convenio o en caso de que la protección datos en el país en cuestión, aún habiendo sido firmado el Convenio, no sea equivalente o en caso de que los datos se transfieran a un tercer Estado que no sea signatario del Convenio.

El Convenio crea un Comité Consultivo (T-PD), compuesto por los representantes de los Estados que son parte en el mismo. Este Comité es el encargado de la interpretación de las normas, cuidando asimismo del cumplimiento del Convenio. Además, el Comité ha estudiado la cuestión de las cláusulas contractuales, como instrumento para facilitar las transferencias internacionales entre los Estados Parte del Convenio y los que no lo son, analizando la cuestión junto con representantes de la Unión Europea y la Cámara Internacional de Comercio

Desde 1981 el desarrollo de la sociedad de la información se ha producido ental medida que en la actualidad el ordenador es un instrumento muy extendido que permite tanto a un individuo como a una organización el tratamiento de los datos. En este contexto, el individuo se convierte en un agente activo de la sociedad de la información, mientras que por otra parte, su privacidad se ve sometida a un número de interferencias cada vez mayores por los numerosos sistemas de información tanto públicos como privados.

Los principios contenidos en el Convenio deben adaptarse e interpretarse en función de los diferentes sectores implicados en la actividad. La actividad del Consejo de Europa con este fin se ha desarrollado mediante la aprobación de diversas recomendaciones, dado que su procedimiento de adopción es sencillo y se adaptan mejor a las circunstancias cambiantes de la protección de datos. Se ha considerado que las recomendaciones, a pesar de carecer de obligatoriedad, son una referencia obligada para los Estados.

Con el fin de elaborar estas recomendaciones el Comité de Ministros creó en 1976 un Comité de Expertos sobre protección de datos, que se convirtió después en el Grupo de Proyectos sobre protección de datos (CJ-PD). Este Comité se compone de expertos de los todos los Estados Miembros del Consejo de Europa, los cuales desempeñan tareas de responsabilidad en relación con la protección de datos en sus respectivos países. Asimismo asisten como observadores a las reuniones del CJ-PD representantes de Estados Unidos, Canadá, Japón, la Santa Sede, Australia, la OCDE, UNIDROIT, la Cámara Internacional de Comercio, la Organización Internacional del Trabajo y otras Organizaciones Internacionales.

Durante estos años el CJ-PD no sólo ha elaborado una serie de Recomendaciones, sino que también ha publicado estudios sobre temas específicos en el ámbito de la protección de datos.

La Agencia de Protección de Datos española forma parte de este Comité, participando activamente en los diferentes

debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Durante 1999, el Grupo concluyó los trabajos relacionados con la Recomendación sobre la vida privada en Internet, adoptada definitivamente como "Recomendación R (99) 5 para la protección de los individuos en lo que respecta a la recogida y tratamiento de datos de carácter personal en las autopistas de la información", por el Comité de Ministros en su reunión de 23 de febrero de 1999. Además, el Grupo ha concluido los trabajos para la elaboración de una recomendación sobre la protección de datos de carácter personal recogidos y procesados para fines relacionados con el sector asegurador.

Por otra parte, se han adoptado diversos documentos relacionados con el control de los servicios de seguridad interna, así como con la colaboración entre los Estados Miembros del Consejo de Europa en materia criminal, analizándose la utilización de datos para usos policiales, con el fin de evaluar los nuevos desarrollos en este ámbito. Por último, se han continuado los trabajos ya iniciados sobre las tarjetas inteligentes y la vigilancia electrónica.

Para el año 2000, el Grupo tiene previsto centrar sus esfuerzos en el terreno de la vigilancia electrónica y la utilización de tarjetas inteligentes, adoptando, en su caso, las correspondientes recomendaciones. Asimismo, se prevé efectuar un informe multidisciplinar relacionado con la utilización de datos genéticos para fines de investigación criminal, en colaboración con otros grupos de expertos del Consejo de Europa.

En la memoria de 1998 ya se dio cuenta del contenido de la Recomendación R (99) 5, siendo el contenido final de la misma similar al allí estudiado, lo que hace innecesario reiterar su contenido en esta Memoria. Por ello, nos referiremos a continuación al Proyecto de Recomendación relativa al tratamiento de datos en el sector asegurador, cuyo texto fue adoptado por el CJ-PD, quedando pendiente para el año 2000 la elaboración de su Exposición de Motivos explicativa para su elevación al Comité de Ministros.

2.1.- EL PROYECTO DE RECOMENDACIÓN PARA LA PROTECCIÓN DE DATOS RECOGIDOS Y TRATADOS PARA FINES RELACIONADOS CON EL SECTOR DEL SEGURO.

2.1.1.- Ámbito de aplicación:

La Recomendación será de aplicación a la recogida y tratamiento de datos para finalidades relacionadas con seguros, quedando excluidas las actividades relacionadas con la seguridad social, sin perjuicio de que los Estados puedan extender la aplicación de la Recomendación a dichas actividades. Asimismo se prevé la posibilidad de extender los efectos de la recomendación a datos no automatizados y a personas jurídicas.

2.1.2.- Fines para los que pueden ser recogidos y tratados los datos:

Tal y como se indica en el apartado 4.4 de la Recomendación, los datos podrán ser objeto de tratamiento con la finalidad de la preparación y celebración de un contrato, la cuantificación de las primas, el pago de indemnizaciones, el reaseguro, el coaseguro, la prevención del fraude, la resolución de quejas, el cumplimiento de otras obligaciones legales o contractuales, la prospección de nuevos mercados, la gestión interna y la realización de actividades actuariales. En todo caso, los datos no podrán ser utilizados para fines incompatibles con los que motivaron su recogida.

2.1.3.- Tratamiento de datos sensibles:

Su tratamiento se encuentra prohibido a menos que el afectado, o su representante si carece de capacidad, hubieran dado su consentimiento, si se efectúa para el cumplimiento de una función relacionada con el interés público o si se permite por la Ley, dada la naturaleza de la actividad y previa la adopción de las debidas garantías de seguridad.

Del mismo modo, el tratamiento de datos relacionado con actividades criminales será posible en los supuestos en que así lo permita la Ley interna y los datos tengan por objeto evitar actividades de fraude por parte del afectado.

2.1.4.- Deber de información al afectado y consentimiento al tratamiento:

La persona cuyos datos son objeto de tratamiento deberá ser informada, antes de dicho tratamiento, si los datos se recogen de él o, en caso contrario, antes de ser comunicados a un tercero, de las categorías de datos recogidos, las finalidades del tratamiento, la identificación del responsable del tratamiento, el modo de ejercicio de los derechos de acceso y rectificación, las categorías de personas destinatarias de los datos, el carácter obligatorio o facultativo de facilitarlos o, en su caso, las consecuencias derivadas de no hacerlo.

Esta obligación sólo se verá exceptuada si el interesado ha sido previamente informado, si la Ley interna lo permite o si el hacerlo encierra un esfuerzo desproporcionado.

Por su parte, el consentimiento deberá ser libre, específico, informado, inequívoco y, en caso de datos sensibles, expreso. Además deberá ser dado por el propio afectado salvo que carezca de capacidad legal para ello, en cuyo caso, corresponderá otorgarlo a su representante legal.

2.1.5.- Tratamientos por terceros por cuenta del responsable:

En este caso, la relación entre el responsable y el encargado del tratamiento deberá estar regida por un contrato u otro instrumento vinculante para el encargado, que sólo podrá actuar dentro de los límites que establezca el responsable

del tratamiento o la Ley interna. Además, la recomendación prevé que el encargado deberá ofrecer medidas de seguridad adecuadas, tanto desde el punto de vista técnico como desde el organizativo que permitan, entre otras cosas, asegurar que el tratamiento sólo se desarrolla en el marco de las instrucciones del responsable.

2.1.6.- Cesiones de datos:

Los datos sólo podrán ser utilizados para las finalidades anteriormente descritas. Cualquier otro uso requerirá que la Ley lo prevea expresamente o que el afectado haya prestado su consentimiento, que deberá ser expreso si se trata de datos especialmente sensibles.

No obstante se permite la utilización para fines de marketing directo si el interesado no se opone a ello. Del mismo modo, será posible el tratamiento para el cumplimiento de fines legítimos del asegurador si no prevalece sobre ellos el interés del asegurado.

2.1.7.- Decisiones basadas en el tratamiento:

Si bien se prevé que, con carácter general, no será posible la adopción de decisiones basadas exclusivamente en los datos tratados, se permite la adopción de las mismas cuando los datos hayan sido facilitados por el afectado con la intención de celebrar un contrato de seguro, en orden a establecer sus términos.

2.1.8.- Derecho de acceso:

En caso de que así lo soliciten, los afectados tienen derecho a conocer, de forma inteligible, los datos que han sido tratados, las finalidades para las que se tratan, los destinatarios de dichos datos y las fuentes de donde se obtuvieron en caso de que no sean el propio interesado. Este derecho sólo podrá restringirse en caso de prevención, investigación o persecución de delitos o en garantía de derechos de terceros, y sólo mientras no desaparezca esta causa.

Por otra parte, los afectados tienen derecho a obtener la rectificación, bloqueo o cancelación de los datos que sean inadecuados, irrelevantes o excesivos respecto a la finalidad que motiva su tratamiento, debiendo informarse de estas circunstancias a los terceros a los que hayan sido cedidos los datos.

2.1.9.- Medidas de seguridad:

La recomendación detalla las medidas técnicas y organizativas que deberán adoptarse para proteger los datos objeto de tratamiento, siempre de acuerdo con los criterios que se establezcan por las legislaciones nacionales de los Estados miembros.

2.1.10.- Transferencias internacionales:

Regirán los principios generales del Convenio 108. Ello supone que, con carácter general, será libre la transferencia a otros países signatarios del citado Convenio que ofrezcan un nivel de protección equivalente al previsto en el mismo. En caso de terceros estados no signatarios sólo será posible la transferencia cuando el interesado lo haya consentido o si se ofrecieran garantías adecuadas, incluidas las de naturaleza contractual en su caso.

2.1.11.- Otras previsiones:

Los datos deberán ser eliminados cuando dejen de ser necesarios para el cumplimiento de los fines que motivaron su recogida, incluido el caso en que se rechace la celebración del contrato por parte de la compañía aseguradora, a menos que se conserven para fines estadísticos y previa la necesaria disociación.

Las legislaciones nacionales adoptarán medidas a fin de regular las compensaciones e indemnizaciones que sean procedentes como consecuencia del incumplimiento de la Recomendación.

Los Estados miembros encomendarán a sus autoridades nacionales de control el velar por el cumplimiento de lo dispuesto en la Recomendación.

3.- SISTEMA DE INFORMACIÓN SCHENGEN.

El objetivo del Convenio de Aplicación del Acuerdo de Schengen es permitir la supresión de los controles en las fronteras comunes en la circulación de personas entre los Estados miembros (en la actualidad Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos y Portugal), manteniendo en el interior de dicho territorio un nivel de seguridad al menos igual al que ya existía. Hay que destacar que durante el año 2000 se iniciará el proceso por el cual los países nórdicos (Noruega, Suecia, Finlandia, Dinamarca e Islandia) cumplirán con todas las condiciones para suscribir el Convenio, con lo que presumiblemente a principios del año 2001 el número de países donde se aplicará el Convenio será de quince.

Entre las medidas compensatorias previstas en el Convenio que persiguen este objetivo, se encuentran la armonización de la política en materia de expedición de visados, una política común en materia de determinación del Estado responsable del examen de la solicitud de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico ilegal de estupefacientes, la armonización del nivel de control de las fronteras exteriores del terri-

torio Schengen y la creación del Sistema de Información Schengen (SIS).

El principal objeto del SIS es, con la ayuda de la información que se transmite en el sistema, preservar el orden y la seguridad públicos, incluida la seguridad del Estado, así como la aplicación de las disposiciones previstas en el Convenio relativas a la circulación de personas en los territorios de los países que conforman el territorio Schengen. El SIS consta de una parte nacional (NSIS) en cada uno de los países que aplican el Convenio y de una unidad de apoyo técnico central ubicada en Estrasburgo (CSIS), estableciéndose de esta forma una conexión entre todos los Estados miembros que permite a los usuarios del sistema la posibilidad de disponer, en tiempo real, de la información necesaria para sus misiones. Esta información está disponible al efectuar controles en la frontera, así como cuando se realizan otros controles de policía y de aduanas; en el caso de los extranjeros, la información está disponible a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de aquéllos en el marco de la aplicación de las disposiciones sobre la circulación de personas.

En el Capítulo Tercero del Título IV del Convenio se establecen los principios y mecanismos destinados a garantizar una adecuada protección de los datos de carácter personal incluidos en el SIS. En su artículo 114 figura que en cada país debe designarse una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre la parte nacional del SIS y de comprobar que el tratamiento y la utilización de los datos introducidos en el mismo no atentan contra los derechos de la persona que se trate. Asimismo, se indica que toda persona tendrá derecho a solicitar a esta autoridad que compruebe los datos referentes a ella integrados en el SIS, así como el uso que se haga de dichos datos. El artículo 10 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, encomienda a ésta el ejercicio del control aquí mencionado.

Por otra parte, el artículo 115 del Convenio establece la creación de una Autoridad de Control Común (ACC) encargada del control de la unidad de apoyo técnico del SIS; esta autoridad está compuesta por dos representantes de cada autoridad nacional de control. También el artículo 10 del Real Decreto mencionado establece que el Director de la Agencia designará a los dos representantes que formarán parte de la Autoridad de Control Común.

La delegación española ha asistido a las sesiones plenarias que ha celebrado la ACC durante el año 1999, en concreto, cinco en Bruselas y una en Florencia donde se presentó el anterior informe anual de la ACC. También ha participado en las cuatro reuniones técnicas relacionadas con la inspección de control que se realizó en la unidad de apoyo técnico central (CSIS) ubicada en Estrasburgo, así como en su ejecución en abril de 1999.

3.1.- DATOS INTRODUCIDOS POR LAS AUTORIDADES ESPAÑOLAS

El SIS incluye exclusivamente las categorías de datos que proporciona cada uno de los Estados miembros y que son necesarios para los fines previstos en el Convenio. Las categorías de datos introducidos corresponden a personas descritas, vehículos (cilindrada superior a 50 c.c. o remolques y caravanas de peso en vacío superior a 750 Kg. que hayan sido robados, sustraídos u ocultados fraudulentamente) y objetos (armas de fuego, documentos vírgenes y documentos de identidad expedidos que hayan sido robados, sustraídos u ocultados fraudulentamente, así como billetes de banco registrados). En el caso de las personas descritas se distinguen, entre otros, los siguientes fines por los que dichos datos pueden ser introducidos por las autoridades competentes: personas buscadas para su detención a efectos de extradición, extranjeros incluidos en las listas de no admisibles, datos de personas desaparecidas o que deban ser puestas a salvo provisionalmente (otorgarles protección, prevención de amenazas, menores de edad), datos de testigos o de personas que deban comparecer ante las autoridades judiciales.

Las autoridades competentes habilitadas para consultar el SIS son las siguientes: Cuerpo Nacional de Policía, Cuerpo de la Guardia Civil, Servicio de Vigilancia Aduanera, Dirección General de Asuntos Consulares, Policías Autonómicas, Policías Locales y Oficinas de Extranjería.

Según los datos disponibles a fecha de 31/12/99, las autoridades españolas habían introducido en el SIS los datos de 20.381 personas, lo cual representaba el 2'38% del total de datos que se habían introducido relativos a personas. Los datos de estas personas se distribuían por finalidad de la siguiente forma: 541 (detención a efectos de extradición), 12.671 (no admisibles), 4.062 adultos y 2.619 menores de edad (desaparecidos o que deban ser puestos a salvo provisionalmente), 462 (testigos y personas que deban comparecer ante las autoridades judiciales) y 26 (otras categorías).

3.2.- INSPECCIÓN DEL CSIS EN ESTRASBURGO

En abril de 1999 se realizó una inspección en la unidad de apoyo técnico central (CSIS) ubicada en Estrasburgo. La realización de este control se justificaba debido al tiempo que había transcurrido desde que se efectuó el último (octubre de 1996) y a que en el año 1998 se habían incorporado tres nuevos países: Austria, Grecia e Italia. Como ya se ha indicado, la delegación española participó en su preparación y ejecución.

Durante la preparación de la inspección la ACC aprobó un documento basado en dos notas de la delegación española, el cual constituye una base de referencia para las futuras revisiones que se vayan a realizar en el CSIS y para las que efectúen las autoridades nacionales de control de sus sistemas de información Schengen nacionales.

Como consecuencia de la inspección, el equipo técnico que la realizó elaboró un informe de carácter confidencial, a partir del cual la ACC confeccionó un resumen, ya público, con las principales deficiencias detectadas y con las recomendaciones emitidas. De entre las mismas cabe destacar:

- Respecto de la seguridad física se verificó que en general tanto su control como su mantenimiento eran satisfactorios,

aunque existían diferentes zonas en el interior del edificio donde la misma debía mejorarse. Se recomendaba mejorar los aspectos organizativos y el control de la sala de ordenadores, así como el de las salas que almacenaban los soportes magnéticos.

- Se verificó que no existían procedimientos formales para conceder autorizaciones de acceso a los sistemas, por lo que se recomendaba su formalización, así como proceder a la verificación periódica de los derechos de acceso otorgados a los usuarios.

- Se aportaron diferentes medidas que podrían mejorar la protección frente a accesos no autorizados.

- Se comprobó que el proceso de comparación de las diferentes copias nacionales con la base de datos central tenía una excesiva duración, por lo que debían adoptarse medidas adecuadas para acelerar el conjunto del proceso y asegurarse así de que las diferencias se detectaban y corregían con prontitud. Asimismo, se detectó que no todas las discrepancias detectadas en el proceso de comparación eran corregidas, por lo que se solicitaba su rectificación para asegurar que todas las copias fueran materialmente idénticas, de conformidad con el artículo 92 apartados 2 y 3 del Convenio.

- Se verificó que se incumplía lo dispuesto en el artículo 113 apartado 2 del Convenio, ya que las descripciones relativas a personas se mantenían por un período superior a un año una vez que habían sido canceladas de la base de datos.

- Algunos países tenían inscritos en el SIS como personas no admisibles a ciudadanos de la Unión Europea, en contra de lo dispuesto en el Convenio.

La ACC dio traslado del informe técnico a la instancias Schengen competentes con el fin de que pudieran subsanarse las deficiencias detectadas, así como para mejorar el nivel de seguridad del CSIS.

3.3..- INTEGRACIÓN EN LA UNIÓN EUROPEA

En el año 1999 entró en vigor el Tratado de Amsterdam, con lo que el marco institucional del funcionamiento de Schengen quedó modificado. En lo que se refiere a la ACC, el Consejo de Ministros adoptó el 20 de mayo de 1999 la "Decisión del Consejo relativa a la Autoridad de control común creada por el artículo 115 del Convenio de aplicación, firmado el 19 de junio de 1990, del Acuerdo de Schengen relativo a la supresión gradual de los controles en las fronteras comunes, de 14 de junio de 1985", con el fin de asegurar el correcto funcionamiento de la ACC ante la entrada en vigor del Tratado de Amsterdam.

En esta Decisión se considera a la ACC una autoridad independiente que no es asimilable a ningún comité o grupo de trabajo del Consejo y cuyo reglamento interno debería ser modificado para introducir las adaptaciones derivadas de la integración del acervo de Schengen en el marco de la Unión Europea.

En la Decisión se acuerda que la Secretaría General del Consejo de la Unión Europea acoja las reuniones de la ACC, brindando las mismas facilidades que a los grupos de trabajo del Consejo.

3.4.- ENTRADA EN FUNCIONAMIENTO DEL CSIS1+

En noviembre de 1999 entró en funcionamiento el CSIS1+, el cual venía a resolver los problemas planteados por el efecto 2000 y la integración de los países nórdicos, así como las deficiencias de administración y operación que presentaba el sistema anterior.

Aunque este sistema no ha sido todavía objeto de inspección por parte de la ACC, las instancias Schengen competentes han informado a esta autoridad de algunas de las mejoras introducidas y que habían sido demandadas por la ACC: ejecución más rápida de los procedimientos de comparación de las bases de datos nacionales con el CSIS, activación de las pistas de auditoría con el objeto de controlar las operaciones de los administradores, mejora del acceso a los datos históricos del SIS y aplicación de los requisitos de la categoría funcional ITSEC F-C2 a los distintos componentes del SIS1+.

4.- AUTORIDAD COMÚN DE CONTROL DE EUROPOL

Durante el año 1999, la Autoridad Común de Control de Europol (en adelante, ACC-EUROPOL), una vez conseguida la doble aprobación unánime de su Reglamento interno, tanto por el Plenario de la propia ACC como por el Consejo de la UE, ha comenzado a ejercer sus funciones plenamente.

Las actividades de este primer año han consistido, primordialmente, en establecer y afinar los mecanismos de control de los que el Convenio Europol dota a la misma para el ejercicio de sus funciones de supervisión de la legalidad del tratamiento automatizado de datos personales por parte de Europol.

Estas labores se han concretado en el proceso de examen y emisión de informe sobre las primeras órdenes de creación de Ficheros de Análisis de Europol, que ha sido un asunto constantemente presente en el orden del día de todas las reuniones celebradas.

Durante dicho proceso se ha producido un fructífero intercambio de ideas con Europol, tanto verbalmente como por escrito, realizando la ACC numerosos comentarios, sugerencias y propuestas respecto de las sucesivas versiones presentadas por Europol, que se han plasmado en la puesta en marcha de un modelo normalizado para la confección de dichas órdenes, satisfactorio para ambas partes.

Pasando a un análisis más detallado, en el año 1999 se han celebrado tres reuniones de la ACC-EUROPOL. La primera de ellas tuvo lugar en Bruselas, en el mes de abril y durante la misma todas las delegaciones, en general, y la española en particular, pusieron de manifiesto la necesidad de disponer de los documentos que deban discutirse en cada una de las lenguas oficiales de la Unión Europea.

Además, la ACC-EUROPOL tomó nota de la decisión de Europol de registrar la totalidad de las consultas o intentos de consulta sobre sus sistemas de información y no solamente sobre el 10% establecido en algunos casos en el artículo 16 del Convenio Europol, dado que cuenta con los medios técnicos para ello.

La segunda reunión se celebró el 24 de junio en La Haya. En ella se procedió a la planificación de los futuros trabajos de la ACC y al nombramiento como secretario provisional de la misma de un funcionario del Consejo de la UE, hasta tanto no se proceda a la creación de una Secretaría conjunta para todas las Autoridades de Control creadas por los instrumentos internacionales en materia de Justicia y Asuntos de Interior, que constituyen el Tercer Pilar de la UE, esto es Europol, Schengen y, en un futuro cercano, el Sistema de Información Aduanera. Dicho funcionario, en el ejercicio de sus funciones como secretario de la ACC, sólo recibe instrucciones de la misma y, en particular, de su Presidente.

De igual modo, se continuaron los trabajos de seguimiento de las órdenes de creación de ficheros de análisis en curso y se decidió la creación de un subgrupo para esta tarea, de manera que procediera a un primer análisis de las sucesivas órdenes que se sometieran a informe de la ACC y, así, agilizar la contestación de la misma en un área en el que la rapidez de respuesta es crítica para Europol.

En la tercera reunión celebrada en La Haya los días 28 y 29 de octubre, se constituyó un subgrupo integrado por representantes de Alemania, España, Países Bajos y Reino Unido encargado de preparar el programa de trabajo para el bienio 2000-2001 y, en concreto, para comenzar la planificación de una primera auditoría de los sistemas de información de Europol que se prevé tenga lugar antes del final del año 2000.

El secretario informó de la continuación de los trabajos en el seno del Consejo para la constitución de una secretaría conjunta y se abordó el tema del papel que debe jugar la ACC en la negociación de acuerdos entre Europol y Estados u Organismos terceros, acordándose que, aunque la ACC no pueda ser un participante activo ni en la decisión de los Estados u Organismos con los que se negocia ni en el propio proceso negociador (competencias ambas del Consejo), sí debe jugar un importante papel en la evaluación exhaustiva del nivel de protección de datos existente en el Estado u Organismo del que se trate, y, tras dicha evaluación, poner de manifiesto, ante todo, si existen serios obstáculos que pudieran impedir el inicio de las negociaciones.

En el transcurso de esta reunión y a petición propia, comparecieron ante la ACC varios representantes de Europol con el objetivo básico de continuar el análisis conjunto de aquellos puntos que se habían revelado como más conflictivos en las órdenes de creación de ficheros de análisis.

Aparte de las reuniones de la ACC ya mencionadas, se produjeron, coincidiendo con las dos últimas, sendas reuniones del Comité de Recursos de la ACC, que estuvieron dedicadas al análisis de aspectos prácticos de la puesta en marcha de dicho Comité y a la elaboración de un primer documento sobre cuestiones procedimentales.

5.- PARTICIPACIÓN EN OTROS GRUPOS DE TRABAJO INTERNACIONALES

5.1 GRUPO DE PROTECCIÓN DE DATOS EN TELECOMUNI-CACIONES

En 1999 ha habido dos reuniones del grupo de trabajo de protección de datos en materia de telecomunicaciones. La primera reunión se celebró en el mes de abril en Noruega y la segunda tuvo lugar a finales de agosto en Berlín. En ambas participaron representantes de agencias de países de la Unión Europea y de países del Este.

En la reunión de Noruega se aprobaron tres documentos (que, por su interés, se transcriben integramente en el anexo de esta memoria) que llevan por títulos: "Posición Común sobre tecnologías de reconocimiento del interlocutor y de análisis de voz en telecomunicaciones", "Posición Común sobre Agentes de Programa Inteligente" y "Posición Común sobre la protección de datos en bases de datos de imágenes de edificios".

También se intercambiaron experiencias y posturas sobre diferentes aspectos, entre las que cabe destacar la firme decisión del gobierno francés, que según informaron los representantes de la CNIL (Autoridad de Control Francesa), va a liberalizar la utilización de mecanismos de cifrado hasta una determinada longitud de clave que todavía está por determinar. Esta decisión, de llevarse a cabo, acercaría a Francia al resto de países de la UE, que hasta la fecha no han elaborado ningún tipo de normativa restrictiva en este sentido.

Otro aspecto de los tratados en la reunión de Noruega de especial interés es la situación de los registros de dominios de Internet de cada país y sus repercusiones en lo que a protección de datos se refiere. A este respecto, un representante de WIPO (World Intellectual Property Organisation) informó acerca de la situación de los registros de dominio en diversos países y los problemas existentes. Diversos representantes expusieron lo que en algunos casos eran situa-

ciones caóticas de dichos registros originadas por la ausencia de normativa a la hora de registrar dichos dominios, hecho que había originado numerosos litigios entre los administradores de los dominios, los titulares de registros de dominios y los titulares de marcas registradas. Afortunadamente, la situación en España es mucho más que aceptable ya que el registro de dominios español (".es") no registra ningún nombre de dominio si no se demuestra un interés legítimo, lo que ha evitado la situación descrita anteriormente. Es opinión generalizada de los representantes del grupo de trabajo que los dominios publiquen los datos personales que sean estrictamente necesarios y que, incluso, se creen dominios en los que no se publique ninguno.

En la reunión de Berlín se intercambiaron experiencias sobre diversos aspectos, en especial sobre la transposición de la Directiva 97/66/CE sobre protección de datos en el sector de las telecomunicaciones en cada país y sus repercusiones sobre Internet. En este sentido, la mayoría de los países han transpuesto la Directiva observándose una falta de uniformidad en cuanto al periodo de conservación que cada país aplica a los datos de tráfico y facturación, que han de ser mantenidos a efectos de reclamaciones.

Algunos aspectos a destacar son la decisión del regulador de telecomunicaciones del Reino Unido, OFTEL, que ha establecido un registro de las personas que no desean recibir llamadas de venta directa y otro para las personas jurídicas que no desean recibir faxes con la misma finalidad (para el envío de faxes de forma automática a personas físicas se necesita el consentimiento previo). Como caso particular, cabe señalar lo apuntado por el representante austríaco, que informó que un reciente cambio en la legislación de telecomunicaciones de su país prohibe el envío masivo de correos electrónicos no solicitados, también conocidos como "spam", pudiendo ser sancionado su uso indebido con multa de hasta aproximadamente 6 millones de pesetas.

5.2 **GRUPO DE TRABAJO SOBRE FICHEROS POLICIALES DE LOS COMISIONADOS EUROPEOS DE PROTECCIÓN DE DATOS**

Tras haberse puesto en marcha entre finales de 1998 y a lo largo de todo el año 1999 la Autoridad Común de Control de Europol, a la elaboración de cuyo complejo Reglamento interno estuvo dedicada prácticamente la totalidad de la actividad del grupo durante más de un año, éste pudo recobrar su carácter de foro de discusión abierto, tanto para el intercambio de información como para el estudio de todos aquellos temas que afectan al tratamiento de datos personales en el sector policial, con vistas al establecimiento de soluciones y criterios comunes por parte de las autoridades de control de todos los Estados miembros de la UE, habiéndose celebrado durante el año 1999 dos reuniones.

La primera de ellas tuvo lugar en marzo en la ciudad de La Haya y en ella se abordó, como primer punto del orden del día, el intercambio de información relativa al programa informático VICLAS (Violent Crime Link Analisys System), que está siendo utilizado por un número creciente de servicios de investigación policial para el esclarecimiento de crímenes seriales. El tema fue suscitado por la delegación belga, que había realizado un análisis de dicho producto recientemente y viendo el alcance paneuropeo que podría tener en un futuro, solicitó que hubiera un enfoque conjunto de los integrantes del Grupo respecto del mismo. Los representantes del Reino Unido aportaron los datos que obraban en su poder, fruto de un estudio anterior realizado por ellos. Se concluyó que la delegación belga suministraría una relación de aquellos puntos que, a su juicio y fruto de su análisis del producto, fueran más relevantes y sobre los que deberían focalizar su actuación el resto de delegaciones para, de esta manera, posibilitar un análisis conjunto de los resultados, sin que al término de 1999 se haya comunicado esta información.

El siguiente punto tratado fue el relativo al comienzo de los trabajos preparatorios para la elaboración de un Reglamento para la Autoridad de Supervisión Común cuya creación prevé el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros (Convenio SIA) en su artículo 18. Por ello, se inició en el seno del Grupo el debate sobre el Reglamento Interno de la ACC-SIA sobre la base de un texto propuesto por la Presidencia austríaca (muy próximo al elaborado para Europol) y una primera aproximación elaborada por la delegación del Reino Unido, tras dirigirse, en 1998, la Presidencia Británica al Grupo solicitando el inicio de los trabajos.

Como líneas maestras para continuar el proceso de redacción, se decidió tomar como base el texto de la Presidencia para seguir el mismo esquema utilizado en Europol, ya que la proliferación de distintas autoridades comunes de control en el marco del Tercer Pilar hace aconsejable que los reglamentos de las mismas tengan un esquema similar, pero utilizando el texto británico como piedra de toque para asegurar que todos los temas fundamentales se contemplan en el nuevo documento.

El siguiente asunto tratado fue el examen del estado de desarrollo del Convenio EURODAC, relativo al almacenamiento de las huellas dactilares de los solicitantes de asilo en algún Estado miembro de la UE, en un fichero centralizado. Por lo que respecta a los asuntos relativos a protección de datos, se informa por parte de la Presidencia del Grupo de la última redacción del borrador del Convenio, en el que se establece que las funciones de supervisión de los derechos de las personas en materia de protección de datos respecto del Convenio EURODAC serán asumidas, cuando se haya procedido a su creación, por el Supervisor Europeo de Protección de Datos, cesando en tal cometido la ACC que se preveía en dicho Convenio.

La segunda reunión se celebró en Bruselas, en el mes de marzo, y estuvo dedicada, prácticamente en su totalidad, a la discusión del Reglamento de la Autoridad de Supervisión Común establecida en el Convenio SIA, llegándose, al final de la misma, a una posición común de todas las delegaciones sobre el texto. Por ello, se decidió que el nuevo borrador de Reglamento se remitiría a las autoridades aduaneras competentes en el seno de la UE, comunicándoles que dicho texto podía ser utilizado como base para la elaboración de su Reglamento, cuando la nueva Autoridad de Supervisión Común se constituyese.

5.3 **PROYECTO HISPANO-HOLANDÉS SOBRE ESTÁNDARES DE INSPECCIÓN.**

Ya en la anterior edición de esta Memoria, se dio cuenta de la existencia de un proyecto conjunto entre los autoridades de control de España (Agencia de Protección de Datos) y los Países Bajos (Registratiekamer) para el desarrollo de metodologías y procedimientos comunes o armonizados para la realización de inspecciones o auditorías de privacidad. El motivo principal de este proyecto era la previsión de que, una vez que se haya establecido una legislación armonizada en materia de protección de datos en toda la Unión Europea mediante la transposición de la Directiva 95/46/CE, las competencias e instrumentos legales y tecnológicos que tendrían a su disposición las autoridades de control para llevar a cabo su misión serían similares. Y una de estas herramientas son las inspecciones o auditorías de los distintos tratamientos de datos personales realizados en cada Estado miembro de la UE, siendo previsible que, dada la cada vez mayor extensión de los tratamientos de datos de ámbito internacional, cada vez se hará más necesaria la cooperación en esta materia. Por lo tanto, para que dicha colaboración sea efectiva, es absolutamente necesario, como se ha dicho, el desarrollo de estándares y métodos comunes.

En el año 1998 se dio el primer paso en este proyecto, mediante un seminario que tuvo lugar en Madrid y en el que dos equipos de inspectores de ambas autoridades intercambiaron ideas y experiencias, planificándose los pasos posteriores del proyecto.

El primer resultado fue la presentación, en la Conferencia de Primavera de Autoridades de Control, celebrada en Helsinki en abril de 1999, de un informe conjunto de ambas delegaciones en el que se daba cuenta de los resultados del seminario celebrado durante dos días en Madrid, se delineaban las líneas generales que se pensaban seguir y se invitaba a otras delegaciones a unirse al proyecto.

Posteriormente, tal como se había acordado en la reunión de Madrid, se planificó y se llevó a cabo la primera inspección utilizando métodos comunes, en gran parte derivados de los sistemas de trabajo de la Inspección de Datos española, que cuenta con una gran experiencia en este tipo de trabajo. El sector elegido para esta primera experiencia fue el de proveedores de servicios de Internet (PSI), por considerarse que los servicios que prestan estas compañías son idénticos en cualquier parte del mundo.

Para estudiar los resultados de esta primera inspección en ambos países y confirmar que el método seguido ofrecía los resultados apetecidos, se celebró un nuevo seminario de dos días, en el mes de noviembre de 1999, en La Haya. En el primer día y en una sesión cerrada, ambas delegaciones compararon los resultados obtenidos y decidieron seguir utilizando el mismo modelo puesto que había dado los frutos esperados. Por lo tanto, se tomó el acuerdo de realizar dos nuevas auditorías a otros dos PSI para tener, de esta manera, un conocimiento del sector que permita extraer conclusiones respecto a sus prácticas en el campo de protección de datos personales.

En el segundo día y en respuesta a una invitación realizada por ambas autoridades de control, se celebró un seminario abierto a todas aquellas delegaciones que hubieran mostrado interés en el desarrollo del proyecto. El objetivo del mismo era tanto el comunicarles los resultados obtenidos hasta la fecha en la colaboración hispanoholandesa como el conocer las iniciativas que el resto de delegaciones estuvieran llevando a efecto en este campo. En este segundo día, participaron, además de los organizadores (España y los Países Bajos), representantes de Bélgica, Finlandia, Irlanda, Reino Unido y la Comisión Europea.
Para finalizar, está previsto que, en los primeros meses del año 2000 se lleven a cabo las dos auditorías restantes en cada uno de los países, para presentar el informe de conclusiones en la Conferencia de Primavera de Autoridades de Control que se celebrará en Estocolmo, el mes de abril de 2000.

6.- CONFERENCIA DE PRIMAVERA DE AUTORIDADES DE PROTECCIÓN DE DATOS EN HELSINKI (14 A 16 DE ABRIL DE 1999)

La Conferencia de Primavera de los Comisionados Europeos de Protección de Datos la forman los Comisionados de la Unión Europea además de los representantes de Noruega e Islandia. Se celebra anualmente en un país distinto y se ocupa del análisis de aquellos desarrollos legislativos o tecnológicos que pueden afectar a la privacidad de los ciudadanos europeos en aras de buscar soluciones armonizadas en el ámbito de los países que concurren a la misma.

En la Conferencia de 1999 se trataron los siguientes temas:

* Desarrollos desde la última Conferencia de Primavera: seguimiento de las discusiones de Dublín
* Desarrollo estratégico
* Los servicios de protección de datos del Comisionado de Finlandia
* Cooperación horizontal
* Schengen y la protección de datos
* Europol e Interpol
* El programa de acción para la aplicación de principios de protección de datos personales en los sitios web y la fiesta de Internet en Francia
* Material de información y otras guías para los ciudadanos y los negocios después de la entrada en vigor de la Directiva
* Códigos de conducta, diferentes niveles y aspectos
* Auditorías de la privacidad: informe del proyecto Hispanoholandés
* Trabajos relacionados con una recomendación sobre el tratamiento de las conexiones de los asalariados por Internet en las empresas y la supervisión de los asalariados

* Introducción a los aspectos éticos en las pruebas genéticas
* Banco de datos genéticos de Islandia: seguimiento de la Declaración de Santiago
* Tratamiento conducido (Managed Care)
* Flujos de datos internacionales
* Identificación electrónica en Finlandia
* Firma electrónica

La delegación española, aparte de participar en todas las actividades y debates de la Conferencia, expuso tres ponencias durante la misma. En concreto, la ponencia sobre "Flujos de datos internacionales" fue pronunciada por D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos, la relativa a "Códigos de conducta" estuvo a cargo de D. Jesús Rubí Navarrete, Adjunto al Director y en la presentación conjunta sobre "Auditorías de la privacidad: informe del proyecto Hispanoholandés", participó D. Emilio Aced Félez, de la Inspección de Datos de la Agencia.

7.- CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS EN HONG KONG S.A.R. (13 A 15 DE SEPTIEMBRE DE 1999)

Como un medio para, al menos una vez al año, estudiar desde una perspectiva global los desarrollos más importantes habidos en el mundo en el ámbito de la privacidad y en la defensa de los derechos fundamentales de la persona humana en todo aquello relativo al tratamiento de datos personales, se celebra la Conferencia Internacional de Autoridades de Protección de Datos.

En el año 1999, dicha conferencia se celebró en Hong Kong, S.A.R. y, aunque la Autoridad de Control española envió representantes a la misma, hay que resaltar que el Director de la Agencia de Protección de Datos no acudió a la cita.

El motivo de dicha ausencia se explica claramente en la carta que, con fecha 28 de junio, dirigió el Director de la Agencia al Presidente del Grupo del Artículo 29.

En la misma, se recuerda que ya en la Conferencia de Primavera de Helsinki se hizo constar la reserva de la delegación española sobre su asistencia a la XXI Conferencia Internacional *"(...) toda vez que, según mis noticias, en dicho territorio chino no se esta cumpliendo con el respeto a los derechos fundamentales de los ciudadanos, habiendo empezado a quebrase los principios del eslogan "Un País, Dos Sistemas". Mi intención era simplemente informar a mis colegas, como miembro leal, de lo que entonces eran simples sospechas aunque fundamentadas en información recibida por colegas jueces, a fin de que pudiera investigarse más a fondo la situación real de lo que estaba ocurriendo en Hong Kong. En todo caso, no trataba con ello de influir en la decisión personal que cada uno puede adoptar".*

Además, continúa con una descripción de la situación de aquel momento *"Lamentablemente lo que entonces eran simples sospechas se han convertido, a mi juicio, en realidad, toda vez que el Partido Comunista Chino ha tomado la decisión de desautorizar a los jueces de Hong Kong e interpretar a su manera la Constitución local (...).*

A mi modo de ver, con esta decisión de no respetar las sentencias judiciales, se ha quebrado abiertamente el principio de "Un País, Dos Sistemas" y se le sustituye por el de "Un País, Un Sistema" y con ello cualquier esperanza de respeto a los derechos humanos que sólo pueden ser garantizados por un poder judicial independiente.

Esta situación me produce especial alarma y desagrado no sólo como Autoridad de Protección de Datos, sino también por mi condición de Magistrado.

Una vez más trato de informar lealmente a mis colegas y en ningún caso de interferir en la decisión personal de cada cual".

Dado que en el momento de la celebración de la XXI Conferencia Internacional no se habían producido cambios sustanciales en la situación, la decisión final del Director de la Agencia fue no asistir a la misma.

No obstante, dado que sí asistió una representación española, aunque no al más alto nivel, a continuación se detallan los principales asuntos tratados en la Conferencia.

* Privacidad en el Nuevo Milenio: una crítica a los estándares de privacidad existentes a la luz de la innovación tecnológica
* La Directiva de Unión Europea - Un año después
* Promesas y peligros de la innovación tecnológica: innovación y privacidad
* La ley emergente del ciberespacio y sus implicaciones para la protección de datos
* Derechos del consumidor y comercio electrónico
* Protección de datos y libertad de información: ¿dos caras de la misma moneda?
* Privacidad y los medios de comunicación
* Seguridad y Auditorías de Privacidad
* Registros públicos - problemas y soluciones
* El incremento de la vigilancia ubicua
* Telecomunicaciones y privacidad
* Privacidad en el escenario global
* Aplicación de la Ley internacional/Cooperación policial internacional

8.- OTRAS ACTIVIDADES DE ÁMBITO INTERNACIONAL.

Aparte de lo anteriormente mencionado, la Agencia de Protección de Datos ha recibido diversas visitas de representantes de organismos extranjeros interesados en conocer directamente el funcionamiento de la misma y cómo se había implantado en España la legislación en materia de protección de datos.

En este sentido, merece la pena destacar la visita realizada en el mes de abril de 1999 por una delegación japonesa de la que formaban parte el Director de la División de Sistemas de Información del Ministerio de Industria y Comercio Exterior del Japón (MITI) y el Primer Secretario de la Embajada de Japón en España.

Asimismo, la Agencia recibió en una visita de trabajo que se prolongó durante tres días del mes de junio, a los directores de los departamentos de Protección de Datos y Relaciones Internacionales de la Oficina de los Sistemas de Información del Estado de la República Checa, organismo que se está encargando, en estos momentos, de coordinar las iniciativas gubernamentales de aquel país con vistas a la adopción de una nueva Ley de Protección de Datos acorde con lo que establece la Directiva 95/46/CE. En el transcurso de la visita se produjeron entrevistas de trabajo con los responsables y miembros de las distintas unidades de la Agencia así como sesiones prácticas encaminadas a un mejor conocimiento de los métodos de trabajo de la Agencia y de los Sistemas de Información de la misma.

Para finalizar, hay que hacer mención a la visita realizada en noviembre por el Profesor Giuseppe Santaniello, Vicepresidente de Il Garante per la Protezione dei Dati Personali, Autoridad de Control italiana, que pronunció una conferencia en la que expuso las líneas principales de la legislación italiana y su aplicación práctica en aquel país. Además, mantuvo una fructífera entrevista de trabajo con el Director de la Agencia que contribuyó a un mejor conocimiento mutuo de ambas instituciones.

1 Los documentos se encuentran disponibles en la dirección de Internet http://europea.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

MEMORIA DE 1999 - ANÁLISIS DE LOS PRINCIPALES DESARROLLOS LEGISLATIVOS EN MATERIA DE PROTECCIÓN DE DATOS

1. COMPARECENCIAS PARLAMENTARIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCION DE DATOS

Durante el año 1999 el Director de la Agencia de Protección de Datos ha comparecido ante Comisiones Parlamentarias del Congreso de los Diputados y del Senado.

En la Cámara Alta, la comparecencia tuvo lugar el 29 de abril ante la Comisión Especial sobre Redes Informáticas.

Las líneas generales de la intervención son las que se exponen a continuación.

El Director de la Agencia valoró el marco normativo para la protección de los datos personales en España y, en particular, la eficacia de la Ley Orgánica 5/1992, de 29 de octubre, porque siendo anterior en el tiempo a la aprobación de la Directiva 95/46/CE, otorga un nivel de protección equivalente al haber tenido en cuenta los trabajos preparatorios de aprobación de la Directiva comunitaria.

En relación a ella destacó, sintéticamente, los principios básicos de protección de datos, incluyendo entre ellos los de calidad en el tratamiento, información a los afectados, consentimiento de los mismos salvo las excepciones basadas legalmente, cesión de datos y protección específica de los datos sensibles.

En segundo lugar, la intervención abordó las cuestiones específicas relativas a la protección de datos en el ámbito del desarrollo tecnológico y de los servicios de telecomunicaciones.

En este aspecto señaló que, la Directiva 97/66, relativa al tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones y, en particular, en la red digital de servicios integrados y las redes móviles digitales públicas, considera que ante la aparición de las redes digitales públicas avanzadas de telecomunicaciones se tienen que crear normas específicas en materia de protección de datos.

En nuestro Derecho interno, la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la citada Ley, vienen a incorporar la Directiva comunitaria en materia de telecomunicaciones antes referida.

En ella son de destacar las garantías relacionadas con la protección de los datos que figuran en las guías telefónicas, con las llamadas no solicitadas para fines de venta directa y con la supresión de la identificación de la línea llamante y la línea conectada.

En cuanto a las actividades de las autoridades europeas de materia de protección de datos, resaltan en este ámbito los trabajos del Grupo del Artículo 29 sobre Internet y los documentos que han sido fruto de su actividad se refieren al tratamiento de datos en la red, al tratamiento automático e invisible en Internet y a la privacidad de las interceptaciones.

La finalidad del primer documento es la de aclarar que tanto la Directiva 95/46/CE como la Directiva 97/66/CE relativa al sector de las telecomunicaciones se aplican, sin lugar a dudas en Internet.

El segundo documento anima a la industria del "software" y del "hardware" a trabajar en proyectos que protejan la privacidad e incluyan las herramientas necesarias para cumplir con la normativa europea de protección de datos. Así, los productos de software y de hardware para Internet deberán facilitar a los usuarios información acerca de los datos que pretenden recoger, almacenar o transmitir y la finalidad para la que son necesarios. La configuración del "hardware" y del "software" no debería permitir, por defecto, la recogida, el almacenamiento o el envío de información persistente del cliente.

El tercer documento se refiere al respeto a la privacidad durante las interceptaciones, respecto de las que resulta de especial importancia que el Derecho nacional precise de forma rigurosa que los servicios autorizados para realizarlas especifiquen el fundamento legal de la intervención, manifiesten las circunstancias, condiciones y finalidades de la misma para poder apreciar el cumplimiento del principio de proporcionalidad, informen, si es posible, al afectado, adopten las medidas de seguridad pertinentes y se sometan a una autoridad de control independiente.

Con un criterio informativo entiende que, en el ámbito de Internet, la Agencia de Protección de Datos ha elaborado y promovido la difusión de unas recomendaciones que faciliten a los usuarios un acceso seguro a través de la red.

Asimismo, el Director de la Agencia entiende que, dentro de las dificultades que supone reglar las transacciones o las comunicaciones en la red, un medio eficaz para garantizar una protección adecuada pueden ser los códigos-tipo elaborados por los propios operadores. En este sentido, España ha sido el primer país de la Unión Europea en que se ha elaborado e inscrito un código de protección de datos promovido por la Asociación Española de Comercio Electrónico, aplicable a Internet.

El 21 de diciembre de 1999 el Director de la APD compareció ante la Comisión Constitucional del Congreso de los Diputados.

La comparecencia incluyó, como primera cuestión, un informe del Director sobre la Memoria de la Agencia correspondiente al año 1998.

De este modo, la presentación ante la Cámara de la Memoria anual de la Agencia consolida un precedente parlamentario homologable con los que desarrollan Organos Constitucionales de forma que el debate anual sobre la situación de la protección de datos en nuestro país se convierta en un punto de referencia obligado de la agenda parlamentaria.

En este sentido, el sometimiento de la Agencia al control de los representantes de la soberanía nacional refuerza la independencia de la entidad y la transparencia de sus actividades.

Además de informar sobre la Memoria anual, en la comparecencia se abordaron otras cuestiones de interés suscitadas por los Grupos Parlamentarios de la Cámara que se resumen a continuación:

Criterio sobre si los datos exigibles para determinar el calculo del tipo de retencion aplicable sobre los rendimientos del trabajo respeta el derecho a la intimidad de los afectados.

El Director aclaró que la Agencia de Protección de Datos no recibió solicitud de información en relación con las consecuencias que, para la protección de datos personales, se pudieran derivar de la Ley 40/1988, de 9 de diciembre, reguladora del Impuesto sobre la Renta de las Personas Físicas ni de los Reales Decretos de desarrollo reglamentario de aquélla. Unicamente se recibió solicitud de informe por parte de la Directora del Departamento de Gestión Tributaria de la Agencia Tributaria en relación con el proyecto de resolución del Departamento de Gestión Tributaria por el que se aprobaría el modelo de comunicación de la situación personal y familiar del perceptor de rentas de trabajo o de su variación ante el pagador y se determina la forma en que debe efectuarse dicha comunicación.

El informe emitido formuló diversas observaciones sobre la adecuación del proyecto de resolución a las exigencias de la LORTAD, cuyo contenido fue sintéticamente el siguiente:

La existencia de deficiencias respecto del deber de información previsto en el art. 5 de la LORTAD, al no existir en el modelo de declaración una cláusula de información. El informe apuntaba como posible solución la inclusión de una cláusula informativa en la que adicionalmente se recabara el consentimiento para el tratamiento de datos.

La necesidad de obtener el consentimiento expreso de los afectados para el tratamiento de datos especialmente protegidos, como son los relativos a la salud, puesto que el modelo de declaración prevé el tratamiento de información sobre discapacitados, tanto si son del propio contribuyente como de los miembros de la organización familiar. El informe apuntaba como posible solución la inclusión de una cláusula en el modelo de declaración para la prestación del consentimiento expreso exigido por el art. 7.3 de la LORTAD.

La falta de claridad sobre quién es el responsable del fichero, la Agencia Tributaria o las empresas retenedores, a los efectos de exigir garantías de la LORTAD, respecto de los tratamientos de datos. La exigencia como documentación que debe acompañar a la declaración del certificado de minusvalías y testimonios literales de las resoluciones judiciales sobre pago de anualidades por alimentos a favor de hijos o de pensiones compensatorias a favor del cónyuge, supone poner en conocimiento de retenedores, ajenos a la relación jurídico-pública del impuesto, informaciones que afectan a la intimidad protegida por la LORTAD. El informe proponía que se habilitara un sistema alternativo de acreditación directamente ante la Administración tributaria.

El 25 de febrero de 1999, la Agencia de Protección de Datos solicitó aclaraciones sobre diversos extremos antes de proceder a la emisión de un informe definitivo .

El informe definitivo y sus conclusiones afectan a las siguientes cuestiones:

La exigencia de proceder al tratramiento automatizado de los datos declarados a efecto de retenciones, circunstancia que determina la aplicación o no de las garantías de la LORTAD. En esta materia, el informe de la Agencia manifiesta que ni la resolución aprobada, ni el "software" facilitado por Agencia Tributaria, que pone a disposición de las empresas para efectuar el cálculo de la retención, implican una exigencia normativa de proceder al tratamiento automatizado de datos. La falta de exigencia normativa no excluye que exista una alta probabilidad de dicho tratamiento automatizado, toda vez que un número elevado de retenedores han declarado ficheros inscritos en el Registro General de Protección de Datos que tienen por objeto la gestión de retenciones. Por ello, la resolución debe facilitar el cumplimiento de las obligaciones de la LORTAD, aunque haya casos en los que la normativa no sea exigible.

En cuanto al responsable del fichero, siendo el tratamiento automatizado decisión autónoma del retenedor, éste tendrá aquella condición .

A juicio de la Agencia de Protección de Datos, la forma más conveniente de facilitar el cumplimiento de la norma citada implicaría incluir en el modelo de comunicación una cláusula tipo con la información del art. 5 de la LORTAD, incluir en el mismo modelo un apartado que facilite la prestación del consentimiento expreso de los afectados para el tratamiento de datos de salud, como son los relativos a la declaración de minusvalías y pueden ser otros especialmente protegidos por el art. 7 de la misma ley en los supuestos de pensiones compensatorias y anualidades por alimentos. La ausencia de tales previsiones en el modelo de declaración puede dar lugar al incumplimiento o al cumplimiento inadecuado de la LORTAD, con las consiguientes e innecesarias consecuencias sancionadoras .

Finalmente, aclarado y admitido que los medios para acreditar la existencia de pensiones compensatorias o por

alimentos son los que facilitan al contribuyente una cómoda acreditación de los hechos, pero no los únicos válidos para realizarla, sería conveniente, a juicio de la Agencia, que la resolución advirtiera expresamente sobre tales posibilidades alternativas.

Actuaciones realizadas por la agencia para esclarecer la presunta utilizacion ilegal de datos de origen desconocido en la convocatoria de la llamada "gran fiesta de la tercera edad", organizada por la consejería de bienestar social de la generalidad valenciana .

La Agencia realizó las oportunas actuaciones inspectoras, que dieron lugar a la iniciación de un expediente de infracción de administraciones públicas en el mes de marzo de 1999. En este procedimiento ha quedado acreditado lo siguiente: la Generalidad Valenciana remitió el 15 de octubre de 1998 a 558.454 personas mayores de 65 años, residentes en la Comunidad Valenciana, una invitación para asistir a la gran fiesta de la tercera edad, utilizando para ello los ficheros de la Consellería de Bienestar social.

La LORTAD exige que los datos personales sean tratados por las administraciones públicas, de acuerdo con la finalidad para la que se obtuvieron, art. 4º.2. Esta previsión se ha considerado incumplida por la Generalidad Valenciana, ya que en las normas de creación de los ficheros utilizados no se concreta la posibilidad de utilizar los datos para el acto convocado.

En consecuencia, se ha declarado la existencia de una infracción.

Medidas para prevenir la cesion ilicita de datos personales archivados por las administraciones publicas.

Adecuacion de las medidas adoptadas por el ministro de sanidad y consumo, a la ley organica 5/1992, de 29 de *octubre, de regulacion del tratamiento automatizado de los datos de carácter personal.*

Valoración de la agencia acerca de la cesion de historiales clinicos de los centros del insalud a empresas privadas .

El principio de finalidad, es decir, aquel para el cual fueron recogidos los datos, es el que debe imperar en las transferencias de los datos entre administraciones públicas. En aquellos supuestos en los que no esté previsto por una norma o una ley de creación de fichero, los datos entre Administraciones Públicas no deberán comunicarse a no ser que sea para una misma finalidad.

La Agencia está atenta a los problemas que puedan derivarse de la transmisión de datos entre administraciones públicas. Buena prueba de ello son los procedimientos de administraciones públicas, cada día más numerosos, y que tienen un especial relieve en el año 1999.

En relación con las Administraciones Públicas un caso de especial relevancia ha sido el denominado el sistema TAIR, que ha sido especialmente analizado por la Agencia de Protección de Datos. En abril de 1998 se presentó ante la Agencia una denuncia relativa al incumplimiento de la Ley de Protección de Datos en la implantación por el Insalud del denominado TAIR (Terminal Autónomo Identificativo del Paciente en las Recetas). La Agencia inició las siguientes actuaciones para el esclarecimiento de los hechos.

De las actuaciones practicadas se desprende que a partir del TAIR se generan dos flujos de información: Interno del Insalud, relativo a la actividad asistencial.

El circuito interno de Insalud está implantado parcialmente, encontrándose en fase de diseño y no operativa el resto del proyecto, que es el más relevante desde la perspectiva de la protección de datos. Sobre la implantación de las fases no operativas, la dirección del Insalud ha solicitado formalmente la colaboración de la Agencia de Protección de Datos, asumiendo el compromiso de mantenerla permanentemente informada .

El segundo circuito es el flujo externo al Insalud, relativo a la información generada por la receta médica, su grabación por los colegios farmacéuticos y su remisión posterior al Insalud. Este circuito está en funcionamiento y constituyó el objeto principal de la denuncia formulada. El TAIR genera una etiqueta para adherir a la receta que contiene datos del paciente, del médico, número de orden de la receta y la fecha de prescripción. Dado que el TAIR no recoge el dato relativo al medicamento prescrito, este es incluido en la receta de forma manual por el médico. Las oficinas de farmacia dispensadoras de los medicamentos recogen las recetas agregando físicamente el cupón precinto que contiene otro código de barras que corresponde al medicamento, así como los datos relativos a la propia farmacia. Posteriormente las recetas son enviadas a los respectivos Colegios Farmacéuticos, donde generalmente a través de terceras empresas contratadas al efecto, se graban en un CD-ROM para su envío mensualmente al Consejo General de Colegios Farmacéuticos.

En la resolución del Director de la Agencia de Protección de Datos de 24 de abril de 1999, se acuerda el archivo de las actuaciones en relación con el tratamiento de datos de las recetas. Los fundamentos de la resolución de archivo son sintéticamente los siguientes: Norma habilitante para realizar el tratamiento automatizado de datos. Según se desprende de las actuaciones practicadas por la inspección, las únicas novedades derivadas de la introducción del TAIR consisten en la incorporación a la receta del Código de Identificación Personal del paciente (CIP), en texto y en código de barras y en la impresión en código de barras del Código de Identificación de Asistencia Sanitaria (CIAS), correspondiente al médico, dato que ya se incluía con anterioridad en la receta. La norma habilitante para la creación del fichero específico de usuarios nacionales de la tarjeta sanitaria, inscrito en el Registro General de Protección de Datos que comprende, en el apartado relativo a la finalidad y usos, el correspondiente a la gestión y control sanitarios.

Las personas o colectivos afectados son todos los usuarios del sistema Nacional de Salud y los organismos oficiales de estadística.

El nuevo tratamiento de datos de titulares de la Tarjeta Sanitaria Individual (TSI) tiene habilitación normativa, puesto que es subsumible en el fichero de usuarios nacionales de tarjetas sanitarias, incluidos en la Orden de 21 de julio de 1994.

En lo que se refiere al consentimiento de los afectados para la obtención de datos personales, la regla general del art. 6 de la LORTAD es la exigencia del mismo, salvo que la ley disponga otra cosa. Sin embargo, el apartado 2 de dicho precepto exceptúa la obtención del consentimiento de los afectados cuando los datos se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias. Dado que el art. 85 de la Ley de Medicamento exige que la receta contenga los datos básicos de identificación del paciente y que tales se han asociado a los contenidos en la TSI, debe estimarse que la Administración sanitaria está actuando en el marco de sus competencias y que la recogida y el tratamiento de datos que figuran en la TSI son adecuados, pertinentes y no excesivos en relación a aquéllas.

El art. 8 de la Ley de Protección de Datos habilita para proceder al tratamiento automatizado de datos personales relativos a la salud de las personas que acudan a las instituciones y centros sanitarios o hayan de ser tratadas en los mismos, siempre que dicho tratamiento se realice de acuerdo con la normativa sanitaria. Dado que los aspectos actualmente operativos del proyecto TAIR se limitan a la grabación de los datos incorporados en las recetas, con la finalidad de efectuar su facturación y el control de ésta, y no a otros desarrollos pendientes en los términos expuestos en los antecedentes de hecho de la resolución, la habilitación para el tratamiento de datos por parte de la Administración sanitaria encuentra su fundamento en los arts. 85, 95, 96 y 98 de las Ley 25/1990, de 20 de diciembre del Medicamento.

El art. 97 de la Ley del Medicamento, que regula la colaboración farmacia-Sistema Nacional de Salud, destaca la calificación de las oficinas de farmacia como establecimientos sanitarios y el deber de colaboración que se les impone para garantizar el uso racional de los medicamentos y la posibilidad de ser objeto de concertación en cuestiones distintas de las obligaciones legales que se les imponen. Por su parte, la Ley 21/1974, de 13 de febrero, de Colegios Profesionales, configura a estas Corporaciones como de derecho público, y se les atribuye la representación de la profesión y el ejercicio de las funciones que les sean encomendadas por la Administración. La Ley de Colegios Profesionales regula los Consejos Generales de los Colegios como corporaciones de derecho público con personalidad jurídica propia y plena capacidad. Entre sus funciones incluye la de los propios colegios en cuanto tengan ámbito o repercusión nacional, artículos 1, 5 y 9. Atendiendo las normas citadas, debe estimarse que las actuaciones que el concierto exige de los colegios profesionales en las recetas constituye un supuesto de cesión de datos entre administraciones públicas, conforme al art. 19 de la LORTAD.

La participación de empresas privadas en la grabación de datos, se encuentra amparada en el art. 27 de la LORTAD, que prevé la posibilidad de realizar el tratamiento de datos personales por cuenta de terceros, siempre que cumplan las garantías de dicha norma y, en particular, la confidencialidad,

En lo que se refiere, dentro del ámbito sanitario, al tratamiento por terceros de historias clínicas, la Agencia de Protección de Datos lo ha inspeccionado en los casos del hospital Doce de Octubre, de Madrid; del hospital de Cabueñes, de Gijón; del hospital provincial de Castellón; del hospital clínico Universitario, de Valencia; del hospital universitario, la Fe, de Valencia; del hospital Nueve de Octubre, de Valencia, del hospital de Sagunto; del hospital psiquiátrico provincial Padre Jofré, de Betera, del complejo hospitalario provincial de Pontevedra y el Servicio gallego de detección precoz de cáncer de mama. Excepto el hospital Clínico de Valencia, el complejo hospitalario provincial de Pontevedra y el Servicio gallego de detección precoz de cáncer de mama, las otras inspecciones han quedado terminadas. Ello ha dado motivo a resoluciones de archivo, por cuanto que las historias clínicas se encuentran documentadas en soporte papel, sin que se produzca tratamiento automatizado de dato alguno, por lo cual es ajeno a la protección de la LORTAD.

2. **ANALISIS Y VALORACION DE DIVERSOS PROBLEMAS DE LA PROTECCION DE DATOS A ESCALA NACIONAL**

2.1. ADAPTACIÓN A 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. LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

2.1.1. Fundamento de la reforma de la LORTAD

La LORTAD tuvo en cuenta los trabajos desarrollados hasta entonces en el seno de la Comunidades Europeas para la adopción de una Directiva en materia de protección de dato, pese a ser anterior en el tiempo a la citada Directiva, recogió los principios fundamentales que se adoptarían posteriormente.

Por ello, para adaptar nuestra Ley a las exigencias de la Directiva la reforma de la LORTAD no precisaba ser más que parcial. Ello motivó que el Gobierno remitiera al Parlamento en el mes de agosto de 1998 un Proyecto de Ley que reformaba unos pocos preceptos de la LORTAD. El indicado Proyecto, junto con alguna mejora técnica que pudiera haber sido incorporada en la tramitación parlamentaria, hubiera mejorado nuestra Ley en algún aspecto que la práctica venía aconsejado, además de trasponer a nuestro derecho interno la repetida Directiva en su totalidad.

Sin embargo, en el trámite de la Ponencia en el Congreso de los Diputados se optó por los parlamentarios por redactar una nueva Ley que no sólo incorporara la Directiva comunitaria sino que estableciera además un mayor rigor en la protección del derecho a la intimidad de los ciudadanos ante el tratamiento de sus datos personales, conforme se deduce de lo expuesto en el diario de sesiones.

La nueva Ley fue mejorada en diversos aspectos en su tramitación por el Senado siendo aprobado este texto definitivamente por el Congreso en segunda lectura en el pleno celebrado el 25 de noviembre de 1999. No obstante es de señalar que la aplicación de la Ley no va a estar exenta de dificultades toda vez que la misma carece de Exposición de Motivos, las mayores novedades se introdujeron en un trámite legislativo no público y no existe una jurisprudencia interpretativa consolidable.

2.1.2. **Principales novedades de la Ley Orgánica 15/1999**

Las principales novedades de la Ley Orgánica 15/1999, si la comparamos con la LORTAD, son, las siguientes:

Se amplía el objeto de la Ley, que hasta ahora venía circunscrito a la protección de la intimidad personal y familiar de los ciudadanos ante el tratamiento informatizado de sus datos personales, en un doble aspecto:

De una parte se incluyen en el ámbito de protección de la Ley todos los ficheros de datos, informatizados o no. Esta es la principal obligación derivada de la Directiva comunitaria que debía ser objeto de transposición a nuestro Derecho interno, el extender la protección a los ficheros no informatizados. El legislador español haciendo uso del plazo que concede el legislador comunitario difiere esta protección al año 2007, sin perjuicio de que, desde la entrada en vigor de la Directiva los ciudadanos puedan ejercitar sus derechos de acceso, rectificación y cancelación respecto de los datos contenidos también en ficheros manuales.

El segundo aspecto en que amplía su objeto la Ley es en que ahora se protege el tratamiento de datos personales respecto del conjunto de libertades públicas y derechos fundamentales de las personas y, especialmente, en el ámbito de su intimidad.

Los derechos de los ciudadanos, hasta ahora circunscritos a los de acceso, rectificación y cancelación de sus datos, se ven completados con el derecho de oposición, de acuerdo con lo señalado por la Directiva, lo que posibilita que el posible tratamiento de datos no llegue a producirse.

Se refuerza por la nueva Ley el consentimiento de los ciudadanos para que sus datos puedan ser tratados. La LORTAD no definía el consentimiento, de lo que sí, en cambio, se ocupa la Ley de 1999, exigiendo que el mismo sea libre, inequívoco, específico e informado.

La Ley define y delimita la figura del encargado del tratamiento, persona física o jurídica que preste servicio al responsable del fichero o tratamiento. Esta figura, que tiene un precedente en el art. 27 de la LORTAD, viene ahora a regularse más detalladamente, de acuerdo con las exigencias de la Directiva. Es de resaltar que al encargado del tratamiento le son exigibles tanto la adopción de medidas de seguridad como la responsabilidad en supuestos de infracción.

Las fuentes accesibles al público, esto es aquellas de las que pueden tomarse datos personales sin el consentimiento del afectado, se delimitan en la nueva Ley al concretarse taxativamente en el censo promocional, repertorios telefónicos, listados de profesionales publicados, diarios y boletines oficiales y medios de comunicación.

Una importante novedad de la Ley es la creación del censo promocional en el que se recogerán los nombres, apellidos y domicilio del censo electoral, de aquellos ciudadanos que no se hayan opuesto a figurar en aquél, tratando de resolver la problemática generada por la utilización del Censo Electoral con finalidades comerciales, estudiada en otro lugar de esta Memoria, sin merma al derecho de los ciudadanos a decidir que sus datos se usen o no para aquellos fines.

El principio de finalidad para el empleo de los datos experimenta un reforzamiento, toda vez que los fines para los que podrán emplearse los datos han de ser, no sólo legítimos como se exigía en la antigua Ley, sino, además, determinados y explícitos. Indudablemente viene a concretarse y restringirse el alcance de este principio que junto con el del consentimiento, son principales en toda normativa sobre la protección de la intimidad ante el tratamiento de datos personales, siendo necesario que el afectado conozca en todo caso de forma indubitada las finalidades para las que se procede al tratamiento de los datos.

El derecho a la información previa a la recogida de datos, se explícita con mayor claridad, al exigirse en todo caso y sin excepción alguna, que se informe al afectado de la existencia del fichero, de la finalidad de la recogida de datos y de los destinatarios de la información, así como de la identidad y dirección del responsable. Además será necesaria la información al interesado cuando los datos no han sido recabados del mismo.

Siguiendo a la Directiva, la Ley 15/1999 incorpora entre los datos especialmente protegidos a los sindicales. Si bien no estaban éstos expresamente recogidos en la LORTAD entre los de esta categoría, venían obteniendo esta mayor protección toda vez que como ha señalado nuestro Tribunal Constitucional deben aquellos incluirse entre los que revelan ideología.

El sector de las empresas dedicadas a la prestación de servicios de información sobre solvencia patrimonial y crédito, sometido ya a una regulación específica en la LORTAD, sigue conservando un régimen específico, si bien la Ley Orgánica 15/1999 clarifica determinadas exigencias, concretando la procedencia de los datos que pueden incorporar y

estableciendo ciertas precisiones.

Así, se señala que estas empresas sólo podrán tratar datos de carácter personal obtenidos de los registros y de fuentes accesibles al público, enumerados taxativamente por la Ley, conforme a o ya indicado, así como de los propios interesados.

Por otra parte, también podrán tratarse datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta. Sólo en estos últimos supuestos, concreta la nueva Ley la obligación de comunicación a los interesados en el plazo de treinta días desde la inclusión en el registro.

La LORTAD no recogía en párrafos separados los dos grupos de ficheros anteriores, por lo que ha venido entendiendo la Agencia de Protección de Datos que la obligación de notificar alcanzaba también a los ahora concretados en el primer grupo. Este criterio de la Agencia de Protección de Datos ha sido en algunos supuestos ratificado por los Tribunales de Justicia y en otros no, creando con ello cierta inseguridad jurídica. La nueva Ley no obstante va a exigir la información a los ciudadanos afectados por las novedades incorporadas en el art. 5, así como, en su caso, por aplicación del principio de calidad de datos.

Finalmente, debe indicarse, respecto del registro y cesión de datos personales, que tanto la LORTAD como la Ley Orgánica 15/1999 sólo permiten conservar aquellos que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años, si bien además la nueva Ley viene a exigir que respondan con veracidad a la situación actual de aquellos.

Se producen también ciertas modificaciones en el régimen específico del sector de la publicidad y prospección comercial, conservando además las especificidades contenidas en la LORTAD. Así, en los supuestos de obtención de información procedente de fuentes accesibles al público, deberá informarse en cada comunicación que se dirija al afectado del origen de los datos, de la identidad del responsable y de los derechos que le asisten.

Por lo que se refiere al régimen sancionador cabe señalar que la tipificación de las infracciones como leves, graves y muy graves experimenta alguna modificación respecto del establecido por la LORTAD, estableciéndose los tipos con una mejor concreción.

En cuanto a las sanciones, se conservan los tres grados establecidos por la LORTAD, si bien con la importante novedad de posibilitar la rebaja en la sanción excepcionalmente, al permitir establecer la cuantía aplicando la escala relativa a la clase inmediata inferior en gravedad. Esta aportación se considera sumamente adecuada, siempre que se establezca su carácter excepcional para aquellos supuestos en que se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, máxime si se tiene en cuenta que el régimen administrativo sancionador en materia de protección de datos personales establecido en la Ley española es el más alto de la Unión Europea, atendiendo al importe de las sanciones.

2.1.3. **Reglamento de Medidas de Seguridad (Real Decreto 994/1999, de 11 de junio).**

2.1.3.1. *Introducción.*

El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, la LORTAD y la Directiva 95/46/CE se refieren a las medidas de seguridad que deben cumplir los ficheros automatizados que contengan datos de carácter personal.

Dentro de nuestro derecho interno, el desarrollo reglamentario de la Ley Orgánica, llevado a efecto por el Real Decreto 1332/1994, de 20 de junio, no ha incidido sobre las medidas de seguridad en contra de las previsiones establecidas en los números 2 y 3 del artículo 9. Ello, no sólo supone un retraso en la concreción de las medidas de seguridad, sino que también supone de hecho la inaplicación de la infracción correspondiente prevista en la Ley Orgánica 5/1992. En efecto, si el artículo 43.3.h) de la misma tipifica como sanción grave el mantenimiento de ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se desarrollen, necesariamente está exigiendo que para la aplicación de dicha falta administrativa exista un previo desarrollo reglamentario sin el que no podría aplicarse aquélla por suponer una infracción del principio de legalidad.

En consecuencia, la falta de desarrollo reglamentario ha impedido sancionar el incumplimiento de las medidas de seguridad por parte de los responsables de los ficheros que contienen datos de carácter personal y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

Por todo ello, la Agencia ha manifestado reiteradamente la preocupación que para la misma supone la inexistencia de un desarrollo reglamentario del artículo 9 de la LORTAD, en cuanto impide la aplicación de determinados principios aquélla. Esta laguna ha sido por fin subsanada mediante la aprobación, mediante Real Decreto 994/1999, de 11 de junio, del Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.1.3.2. *Contenido del Reglamento*

El Reglamento ha establecido tres niveles de seguridad (básico, medio y alto) atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información almacenada. Además, se parte de la idea de que es necesaria la determinación exacta de las medidas de

seguridad aplicables a cada organización a través del documento de seguridad, en donde se plasmen las medidas imprescindibles a cumplir en materia de seguridad de los datos personales. Se configura, por tanto, el documento de seguridad como un elemento básico en la determinación de las medidas de seguridad, que han de ser al menos las detalladas en el Reglamento.

Siguiendo estos criterios básicos, el Texto se articula en Cinco Capítulos, en donde se trata de determinar un marco general que deberá ser concretado por el responsable del fichero.

El Capítulo I "Disposiciones Generales" establece las principales definiciones, los conceptos básicos y los niveles de seguridad que determinan el contenido del Reglamento. Hay que destacar el hecho de que se tipifica la infracción de las medidas de seguridad como grave dado que así se determina con carácter genérico en el artículo 43.3.h) de la Ley Orgánica 5/1992 y en la nueva Ley Orgánica 15/1999, por lo que no existe la posibilidad de configurarla de forma diferente, sin perjuicio de poder graduarla atendiendo a los criterios establecidos en la propia Ley y reconocidos en el Reglamento. Además, en este capítulo I se incluyen dentro del ámbito de aplicación del Reglamento, el acceso a datos a través de redes de telecomunicaciones, el régimen de trabajo domiciliario y los ficheros temporales.

Los Capítulos II, III y IV determinan cuáles son las medidas de seguridad que han de cumplir los ficheros atendiendo al nivel en que se encuadren. Se parte, como ya se ha puesto de manifiesto, de la existencia de un documento de seguridad de obligado cumplimiento dentro de la organización, en el que se establezca la normativa de seguridad, en los términos que se recogen en el articulado del Reglamento.

Las medidas de seguridad de nivel básico se considera que son las mínimas exigibles a cualquier fichero que contenga datos de carácter personal, dada la protección que los mismos requieren de acuerdo con lo establecido en la LORTAD.

Las de nivel medio se aplican a ficheros que por la especial naturaleza de los datos que contienen se entiende que requieren una protección especial. Se exigen una serie de medidas que, atendiendo al estado de la tecnología y a un coste asumible, garantizan los principios de la Ley Orgánica.

Por último, las medidas de seguridad de nivel alto se aplican a los ficheros con datos especialmente protegidos. Si bien es cierto que en algunos supuestos, el coste de su implantación puede ser elevado, se entiende que es imprescindible exigirlas atendiendo a la especial naturaleza de los datos y al reforzamiento de la protección que los mismos requieren.

El Capítulo V señala cuales son las competencias del Director de la Agencia de Protección de Datos en relación con las medidas de seguridad. Dichas competencias son las que aparecen reconocidas en la Ley Orgánica 5/1992, si bien aplicándolas, en concreto, a las mismas.

Por último, la disposición transitoria se ha establecido únicamente para señalar unos plazos que hagan factible la implantación de las medidas de seguridad del Reglamento, teniendo en cuenta en algún caso su complejidad tecnológica y el coste económico que pueden suponer para las organizaciones.

2.1.4. **Régimen de la Firma Electrónica**

Debe dedicarse un apartado de este epígrafe a una cuestión, relacionada con el comercio electrónico, que presenta un cariz especialmente novedoso y que se relaciona directamente con el valor probatorio de las declaraciones de voluntad manifestadas en el negocio electrónico, pero que presenta un valor añadido en cuanto a la protección de la intimidad de las personas: la llamada firma electrónica.

2.1.4.1. *Concepto de firma electrónica.*

Por firma electrónica se entiende "cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita".

La Directiva sobre un marco común para la firma electrónica y servicios relacionados, por su parte, la define como aquella firma en forma electrónica integrada en unos datos, anexa a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

- está vinculada únicamente al firmante;

- es capaz de identificar al firmante;

- está creada de un modo o utilizando un medio que está únicamente bajo el control del firmante; y,

- con el fin de acreditar que no se ha modificado, está vinculada a los datos a los que se refiere de tal forma que si los datos son alterados la firma electrónica es invalidada.

2.1.4.2. *El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.*

La materia aquí analizada ha sido recientemente regulada en nuestro país por el Real Decreto-Ley 14/1999, de 17 de septiembre, que viene a establecer determinadas especificaciones en relación con el régimen jurídico de la firma electrónica, la validez de los documentos en que la misma se utilice y la protección de los datos de carácter personal

correspondientes al signatario.

Con carácter general, el Decreto-Ley define la firma electrónica como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge". Junto con la firma "convencional, se define la Firma electrónica avanzada, caracterizada por ser "la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos".

Respecto de ésta última, el artículo 3 establece que "la firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales", lo que supone una plena equiparación entre la firma manual y la electrónica a estos efectos.

Para que la firma surta todos sus efectos deberá ser certificada por un prestador de servicios de certificación, cuyo régimen se establece detenidamente en el Real Decreto-Ley.

En cuanto al régimen de protección de datos personales del signatario, aparece detalladamente regulado en el artículo 15 del Decreto-Ley, existiendo otras referencias en el artículo 13 del mismo. Este régimen se puede estructurar, siguiendo la propia sistemática de la Ley Orgánica 5/1992, del siguiente modo:

1.- Ámbito de aplicación de la Ley Orgánica 5/1992 en relación con la firma electrónica:

Según el artículo 15.1, quedará sujeto a la aplicación de la normativa reguladora de protección de datos el tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad; el que se realice en el Registro de Prestadores de Servicios de Certificación; añadiendo que el mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2.- Cumplimiento del principio de finalidad:

Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3.- Consentimiento del afectado y cesiones de datos:

La entidades prestadoras estarán obligadas a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992, de 29 de octubre.

Del mismo modo, en caso de cese en su actividad por parte del prestador de servicios, el artículo 13 del Decreto-Ley prevé que "el prestador de servicios de certificación que vaya a cesar en su actividad, deberá comunicarlo a los titulares de los certificados por él expedidos y transferir, con su consentimiento expreso, los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios que los asuma o dejarlos sin efecto. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad".

4.- Especial referencia al principio de calidad de los datos en los supuestos de uso de seudónimos:

Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica 5/1992. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

3. PROBLEMAS PLANTEADOS EN LAS CONSULTAS EFECTUADAS POR RESPONSABLES DE FICHEROS O TRATAMIENTOS O SUS REPRESENTANTES.

Dentro de la actividad llevada a cabo por la Unidad de Apoyo del Director de la Agencia de Protección de Datos, el Gabinete Jurídico ha venido desempeñando desde la creación de la Agencia, junto con la función de asesoramiento directo a los distintos órganos de la misma, una importante función de resolución de las cuestiones de mayor complejidad jurídica planteadas por las personas o entidades públicas o privadas que ostentan la condición de responsables de ficheros o por sus representantes legales o empresas que prestan a aquéllos asesoramiento en materias relacionadas con la informática y el derecho.

Esta actividad ha sufrido un enorme incremento a lo largo del año 1999, en que se ha pasado de la elaboración de 221 informes en 1998 a la cifra de 370 (un aumento del 67,87%).

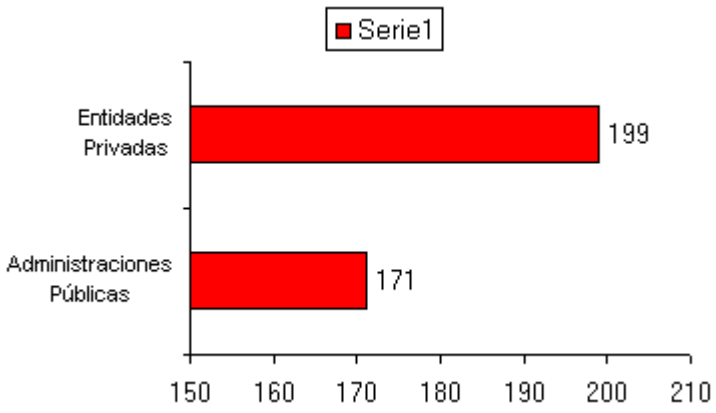
Debe recordarse, no obstante, que la actividad a la que estamos haciendo referencia se lleva a cabo con el ánimo de colaborar con las entidades antes mencionadas en el desarrollo de sus actividades, si bien esta tarea no se encuentra entre aquellas que la Ley y su Estatuto exigen de la Agencia. Precisamente por ello los informes, a no ser preceptivos, carecen de cualquier carácter vinculante, no prejuzgando de modo alguno la actuación de esta Agencia, por cuanto, en la mayor parte de los supuestos, no se tiene conocimiento de la totalidad de las circunstancias que concurren realmente en los hechos que motivan la consulta.

A continuación nos referiremos a las principales cuestiones que han sido planteadas en este tipo de consultas, haciendo en primer lugar referencia a diversas cuestiones relacionadas con el reparto de dichas cuestiones en función de diversos criterios para, posteriormente, analizar las cuestiones que o bien han sido objeto de un mayor número de consultas o bien revisten una mayor relevancia desde el punto de vista de la interpretación de la Ley. Se ha considerado de interés informar sobre el contenido de las consultas, debiendo tener en cuenta que esta cuestión no había sido tratada en anteriores memorias.

3.1. DATOS ESTADÍSTICOS DE INTERÉS RELACIONADOS CON LAS CONSULTAS.

En el siguiente cuadro se hace constar el reparto de informes remitidos atendiendo a la naturaleza pública o privada del consultante:

Administraciones Públicas	**171**
Admón. General del Estado	11
Organismos Públicos	22
Comunidades Autónomas	13
Entidades Locales	109
Ayuntamientos	101
Diputaciones Provinciales	7
Otros	1
Admón. Corporativa	16
Cámaras de Comercio	3
Colegios profesionales	13
Consultas privadas	**199**
Empresas	146
Particulares	19
Asociaciones/Fundaciones	18
Sindicatos	8
Otros	8
Total informes	**370**



Como se desprende del gráfico adjunto, el volumen de consultas provenientes de los sectores público y privado es sustancialmente similar, siendo de destacar la importancia numérica de las cuestiones planteadas por los Ayuntamientos (un 27 % del total), dentro del sector público, y por los empresarios mercantiles (un 39 % del total), dentro del privado.

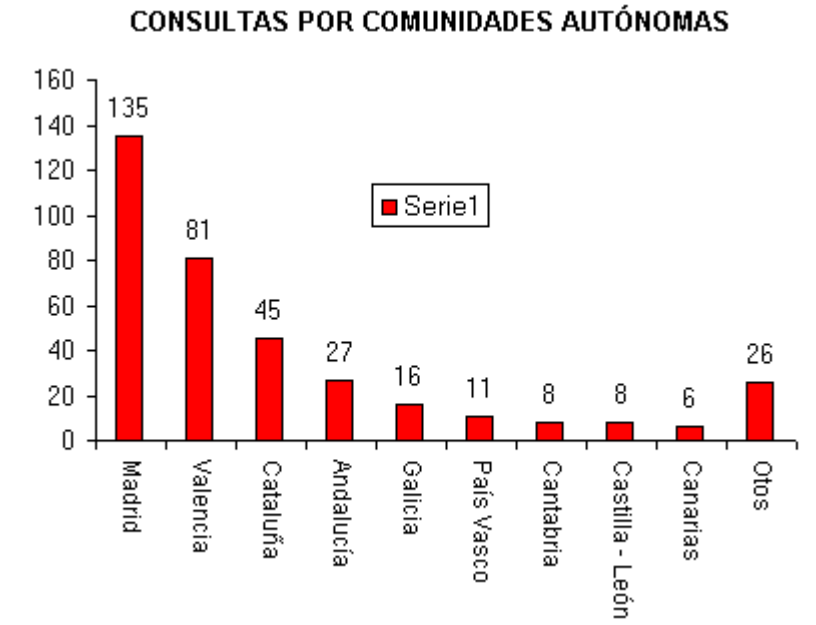
En el gráfico siguiente se refleja la distribución de las consultas planteadas por los empresarios, atendiendo al sector de actividad al que los mismos pertenecen:

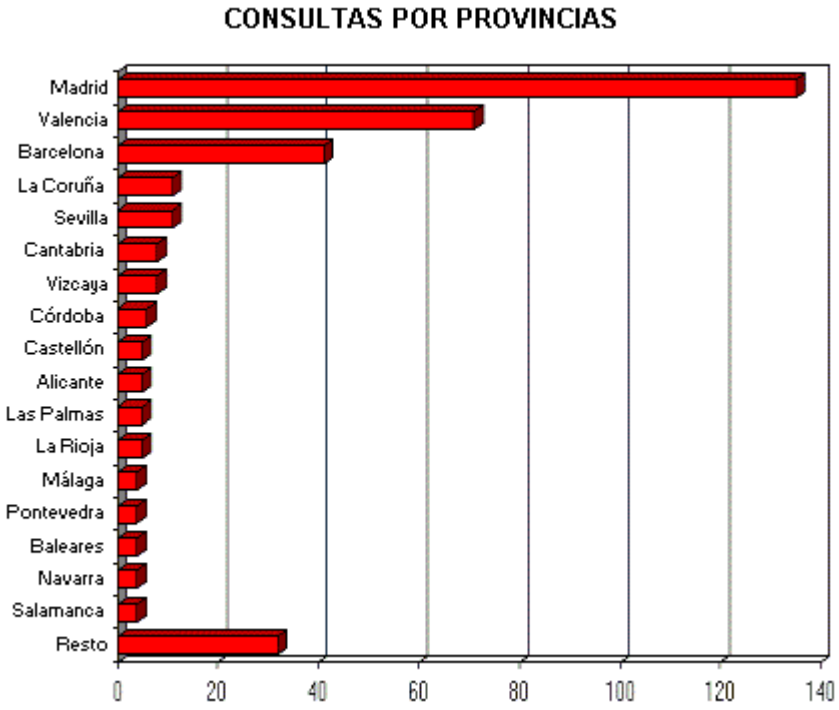
En esta distribución sectorial, resulta sumamente significativo el volumen de consultas planteadas por las entidades a las que corresponde el asesoramiento representación de los responsables de los ficheros (que ascienden a un 24 %), dada la especial complejidad de las cuestiones planteadas ante los mismos por sus clientes.

Una vez más debe reiterarse que en modo alguno encaja dentro de las actividades de la Agencia de Protección de Datos el deber de resolver aquellas cuestiones que puedan ser planteadas a las empresas destinadas a actividades de asesoría o consultoría por quienes solicitan los servicios de las mismas. En caso contrario se estaría obligando a la Agencia de Protección de Datos (al margen de las previsiones de la Ley Orgánica y del Estatuto) a llevar a cabo actividades propias de dichas entidades, sin contraprestación alguna, entrando en concurrencia con otras entidades del sector. Ello no obstante, se ha tratado de dar respuesta a aquellas cuestiones que plantean una mayor complejidad desde el punto de vista jurídico o técnico.

Al margen de esta referencia, es de reseñar el importante volumen de cuestiones planteadas por el sector financiero (al margen de las referentes a servicios de solvencia patrimonial y crédito) y el importante incremento de las cuestiones planteadas por las empresas del sector de las telecomunicaciones, respecto de las cuales se ha acentuado la actividad de la Agencia de Protección de Datos durante el año 1999, tal y como se expone en otros apartados de esta Memoria.

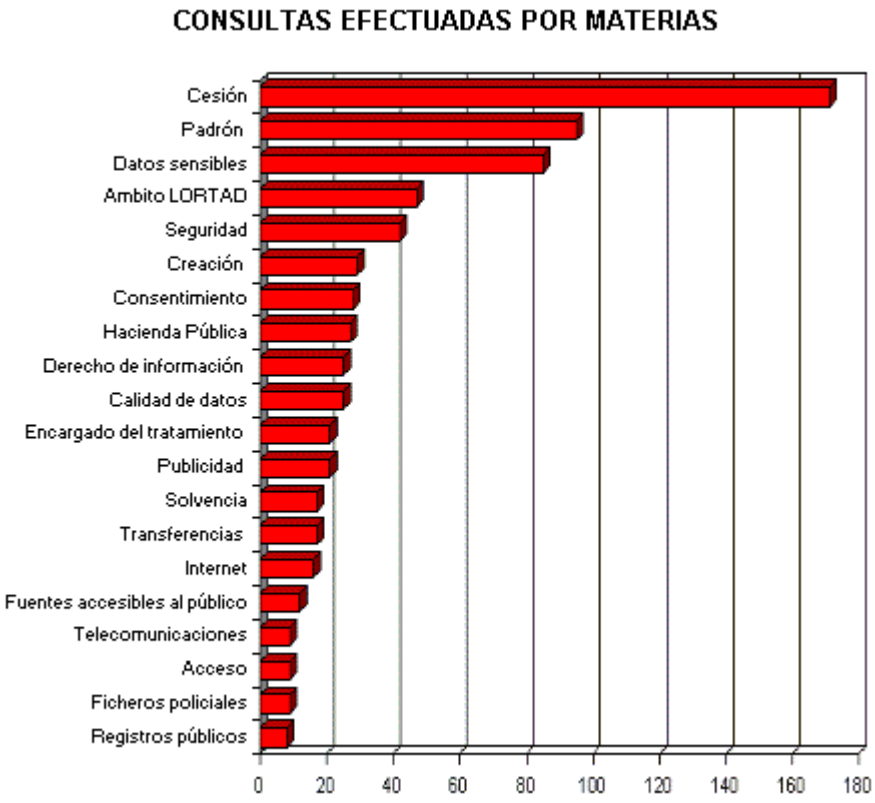
Atendiendo, por otra parte, al origen geográfico de las consultas planteadas, debe indicarse que la práctica totalidad de las mismas (363) se plantearon por entidades u organismos nacionales, siendo sólo 7 las planteadas por entidades extranjeras. En el Gráfico siguiente se observa la distribución de dichas consultas atendiendo a la Comunidad Autónoma desde la cual se efectuaron, indicándose asimismo el origen de las consultas por provincias.





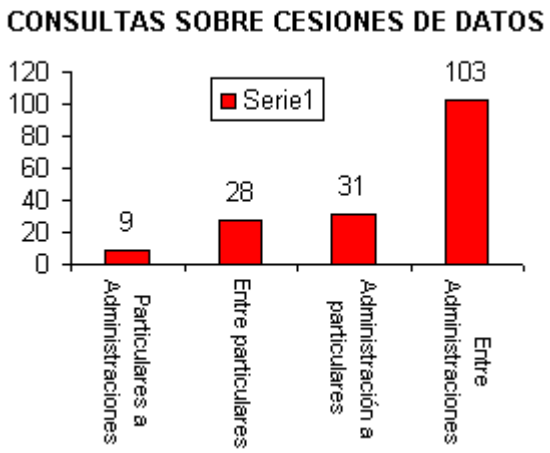
De estos datos se desprende que la mayor parte de las consultas planteadas (prácticamente las tres cuartas partes de las mismas) se concentran en los núcleos correspondientes a Madrid, Barcelona y Valencia, al ser éstos, como también se comprueba en otros lugares de esta Memoria, los lugares en que existe una mayor actividad relacionada con la utilización de datos de carácter personal. Es de destacar que un amplio porcentaje de las consultas correspondientes a las provincias que integran la Comunidad Valenciana procede de los Ayuntamientos sitos en su territorio, cuestión ésta que no se reproduce en el resto de los casos.

Por último, el gráfico adjunto se refiere a los temas objeto de consulta más frecuente:



En este punto, debe destacarse la importancia de las cuestiones relacionadas con la cesión de datos del padrón municipal (sobre todo en lo referente a la cesión de datos sensibles o especialmente protegidos, en la terminología empleada por la LORTAD). Asimismo resulta destacable el número de consultas planteadas como consecuencia de la entrada en vigor 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, así como las consultas relacionadas con ficheros de la Hacienda Pública y la realización de tratamientos de datos por cuenta de terceros, con la aparición, cada día más habitual, de la figura denominada "encargado del tratamiento" por la Directiva 95/46/CE, del Parlamento 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 y la nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

No obstante, de entre todos los temas sujetos a consulta, el más importante es el referente a las cesiones de datos. El gráfico adjunto pretende reflejar la distribución de este tipo de consultas, atendiendo a la naturaleza pública o privada del cedente y el cesionario:



3.2. **ESTUDIO DE LAS CUESTIONES MÁS RELEVANTES PLANTEADAS POR LOS RESPONSABLES DE FICHEROS O TRATAMIENTOS Y SUS REPRESENTANTES**

A continuación se hará referencia a aquellas cuestiones que, como consecuencia de su especial complejidad o dada la frecuencia con que han sido planteadas, resulta necesario estudiar con cierto detenimiento. Para ello, se ha dividido la exposición en cinco grandes apartado: El primero de ellos hace referencia a aquellas cuestiones relacionadas con el ámbito de aplicación de la LORTAD (tanto desde un punto de vista subjetivo como objetivo). En segundo lugar se analizará el alcance y supuestos en que es posible la cesión de datos contenidos en el Padrón Municipal de Habitantes. A continuación nos referiremos a las distintas dudas que han surgido como consecuencia de la aprobación del Reglamento de Medidas de Seguridad. Posteriormente, se tomarán en consideración determinadas cuestiones relacionadas con el sector de las telecomunicaciones, estudiándose por último otras materias que, sin poder ser incluidas en un epígrafe específico, resultan dignas de análisis.

3.2.1. **Cuestiones relacionadas con el ámbito de aplicación de la LORTAD**

Dentro de este apartado son muy habituales las consultas relacionadas con la cuestión de si resulta de aplicación la LORTAD al tratamiento de datos relacionados con las personas físicas que ejercen una actividad empresarial, resultando asimismo destacable el análisis de la naturaleza de los ficheros cuya titularidad corresponde a entidades integradas en la denominada Administración Corporativa (se analizó específicamente el supuesto de las Cámaras de Comercio). Por último, un gran número de las materias incluidas en este epígrafe se refiere a analizar si determinadas informaciones pueden ser consideradas datos de carácter personal, a partir del concepto que de los mismos prescribe la LORTAD.

3.2.1.1. *Aplicación de la LORTAD a los ficheros que contengan datos relacionados con empresarios individuales.*

En un lugar anterior de esta memoria, se ha recordado que las disposiciones contenidas en la LORTAD, dado su ámbito de aplicación y objeto resultan aplicables exclusivamente a las personas físicas. Ello no obstante, se plantea el problema de determinar si las citadas normas resultarán de aplicación a los empresarios individuales y a los profesionales.

Como ya se ha dicho, de lo dispuesto en los artículos 1 y 3 a) de la LORTAD se desprende que la protección de la "privacidad" conferida por la misma no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran exigirse en su caso.

Al propio tiempo se ha venido indicando por la Agencia que los datos referidos a empresarios individuales no pueden entenderse amparados en la LORTAD en el ejercicio de su actividad mercantil, dado que su objeto consiste en la protección de la intimidad personal y familiar de las personas físicas, siendo así que no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, no puede ser aplicable a esas personas la protección consagrada por la LORTAD, ni siquiera cuando su actividad se identifique plenamente con la de una persona física determinada, habida cuenta que el ámbito personal que se protege debe ser considerado como distinto del empresarial.

No obstante, debe tenerse en cuenta que, aunque no entrará en vigor hasta 14 de enero de 2000, la nueva Ley Orgánica 15/1999 extiende su manto protector más allá de la mera protección del derecho a la intimidad personal y familiar para consagrar el denominado derecho a la "autodeterminación informativa", por lo que es objeto de la Ley la protección de cualesquiera derechos fundamentales y libertades públicas de las personas físicas frente al tratamiento automatizado de sus datos de carácter personal. Ello supone que, si bien los empresarios individuales, en el ejercicio de su actividad mercantil, pueden carecer de un derecho a la intimidad personal y familiar, sin embargo el tratamiento de los

datos referidos a los mismos podrá suponer una vulneración de otros derechos que les atribuye la Constitución (por ejemplo, el tratamiento de los datos relacionados con la pertenencia de un empresario a una determinada asociación puede vulnerar el derecho de asociación, consagrado por el artículo 22 de la Constitución).

Por ello no será posible, dentro de este nuevo marco normativo, ofrecer una solución unívoca de la cuestión planteada, debiendo estarse estrictamente a los datos que sean objeto de tratamiento en cada caso concreto para apreciar si el fichero se encuentra o no sujeto a las normas reguladoras de la protección de datos de carácter personal.

En todo caso, deberá tenerse en consideración al delimitar si cada concreto fichero o tratamiento se encuentra sometido a las exigencias de la nueva Ley la reiterada jurisprudencia de nuestro Tribunal Constitucional que exige atender en cada caso concreto a una adecuada protección de los derechos fundamentales consagrados en la Constitución (aunque dicha interpretación no suponga necesariamente la mayor protección de los mismos).

3.2.1.2. *Régimen de los ficheros de que son titulares las Cámaras de Comercio.*

Una de la las consultas planteadas tenía por objeto que se delimitara la naturaleza pública o privada de los ficheros relacionados con la gestión del Recurso Cameral Permanente, cuyo responsable son las Cámaras de Comercio. La respuesta a esta cuestión resulta sumamente importante, dado el distinto tratamiento jurídico que la LORTAD establece para los ficheros atendiendo a su carácter público o privado.

Para analizar la misma, se atendió, fundamentalmente, a las funciones que desarrollan tales entidades, aclarando el artículo 1.1 de la Ley 3/1993, de 22 de marzo, Básica de las Cámaras Oficiales de Comercio, Industria y Navegación, que "las Cámaras Oficiales de Comercio, Industria y, en su caso, de Navegación son Corporaciones de derecho público con personalidad jurídica y plena capacidad de obrar para el cumplimiento de sus fines, que se configuran como órganos consultivos y de colaboración con las Administraciones Públicas, sin menoscabo de los intereses privados que persiguen".

De lo dispuesto en esa norma se desprende que dentro las funciones desarrolladas por las Cámaras pueden distinguirse aquéllas que persiguen un interés privado de los miembros (las personas que las integran y que ejercen la actividad a que se refiere la corporación) de aquéllas otras que suponen el ejercicio de auténticas potestades administrativas, vinculadas al ejercicio por la corporación de potestades de imperium sobre sus miembros. Dentro de éstas últimas puede hacerse referencia a las potestades derivadas de aquellas normas que hayan establecido la obligatoriedad de pertenecer a las mismas para el posible ejercicio de la actividad correspondiente, aquéllas que las atribuyan en determinados casos potestades recaudatorias (tales como las relacionadas con el Recurso Cameral Permanente) o las referentes a la imposición a los miembros de medidas de carácter disciplinario o sancionador.

Con base en estas consideraciones, y teniendo en cuenta la coexistencia en la actuación de las Cámaras de Comercio de funciones que llevan implícito el ejercicio de potestades administrativas con otras de naturaleza propiamente privada, los ficheros cuya responsabilidad ostente la corporación habrán de ser concebidos como de naturaleza pública o privada en atención a la finalidad que por los mismos se persiga: Así, serán de naturaleza pública los ficheros cuya finalidad sea el ejercicio por la responsable de las potestades administrativas que a la misma hayan sido conferidas por las leyes y reglamentos, siendo de titularidad privada los ficheros vinculados al desempeño de actividades propiamente de derecho privado.

En el presente caso, y dado que la gestión y recaudación del Recurso Cameral Permanente se encuentra vinculada al ejercicio por las Cámaras de una potestad de derecho público, el fichero tendrá carácter público, siendo indispensable que el mismo sea creado por una disposición de carácter general (dictada por la Administración Pública de tutela de la Cámara de Comercio) en que se haga constar la totalidad de los extremos contenidos en el artículo 18.2 de la LORTAD, comunicándose esta circunstancia al registro General de Protección de datos para su inscripción, por imperativo del artículo38.2 a) de la LORTAD y quedando el fichero sujeto al régimen prevenido en el Capítulo I del Título IV de la propia Ley Orgánica.

3.2.1.3. *Tratamiento de la huella digital de los trabajadores por el empresario.*

Se planteó por una Corporación Local la posibilidad de tratamiento automatizado de la huella digital para la comprobación de la identidad de los funcionarios al servicio de dicha Corporación y el cumplimiento por los mismos de su jornada de trabajo. La cuestión a resolver en ese caso era la de determinar si la huella digital puede ser considerada dato de carácter personal, en caso de serlo si se encuentra sometida a algún tipo de regla especial y, por último, si el empleador puede tratar la huella sin consentimiento de los trabajadores.

Para resolver esa cuestión se plantea cuál es la incidencia que los datos biométricos tienen en el ámbito de aplicación de la LORTAD, siendo datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión (tales como las huellas digitales, el iris del ojo, la voz, etc.).

El artículo 3 a) de la LORTAD, define los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". En este sentido debe indicarse que, si bien el procesado de los datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento, éste deberá ajustarse a la LORTAD. El problema consiste en determinar si el tratamiento de la huella digital puede ser considerado excesivo para

el fin que lo motiva, atendiendo al principio de proporcionalidad consagrado por la Ley.

Se entendió por esta Agencia de Protección de Datos que los datos biométricos tenían la condición de datos de carácter personal y que, dado que los mismos no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tendrá mayor trascendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos.

En cuanto a la posibilidad de que las huellas sean tratadas sin consentimiento del interesado, y teniendo en cuenta que el tratamiento trae su origen, precisamente de la necesidad de asegurar el debido cumplimiento de las obligaciones derivadas de la relación estatutaria que vincula al funcionario con la Administración, será posible el tratamiento inconsentido, ya que el artículo 6.2 de la LORTAD prevé que no será preciso el consentimiento cuando los datos "se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

En todo caso se indicó que el fichero quedaba sometido a las demás disposiciones de la LORTAD, en cuanto a su creación y funcionamiento, siendo necesario informar a los interesados de su existencia y de los demás extremos a que se refiere el artículo 5.1 de la Ley Orgánica.

3.2.1.4. *Naturaleza de la dirección de correo electrónico a efectos de la LORTAD.*

Se planteó si la venta o cesión de un fichero que contenga direcciones de correo electrónico ha de ser considerada como cesión de datos a los efectos de la LORTAD, lo que exigía analizar si dichas direcciones tenían la consideración de dato de carácter personal, partiendo del concepto establecido en el artículo 3.a) de la LORTAD.

En este sentido, debe indicarse que la dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular. Por ello podemos referirnos a dos supuestos esenciales de dirección de correo electrónico, atendiendo al grado de identificación que la misma realiza con el titular de la cuenta de correo:

a) El primero de ellos se refiere a aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado). En este supuesto, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal. Ejemplos característicos de este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del país en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso así delimitarse el centro de trabajo en que se realiza la prestación).

b) Un segundo supuesto sería aquel en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (por referirse, por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno). En este caso, un primer examen de este dato podría hacer concluir que no nos encontramos ante un dato de carácter personal. Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello se considera que también en este caso, y en aras a asegurar, en los términos establecidos por la Jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18. 4 de la Constitución, será necesario que la dirección de correo electrónico, en las circunstancias expuestas, se encuentre amparada por el régimen establecido en la LORTAD.

Tomando esta circunstancia en consideración se concluye que la cesión de un listado de direcciones de correo electrónico se encuentra sujeta al artículo 11 de la LORTAD, sin que la mera publicación en Internet de un directorio de direcciones de correo electrónico puede ser considerada como circunstancia que convierte los datos en accesibles al público, toda vez que dicha inclusión supone un tratamiento que, debe haber sido efectuado recabando el consentimiento informado de los afectados, al que se refieren los artículo 5 y 6 de la LORTAD.

3.2.1.5. *Tratamiento de registros de voz.*

Se plantearon a la Agencia de Protección de Datos diversas cuestiones relacionadas con la recopilación por parte de una empresa de diversos registros de voz, con la finalidad de elaborar un programa de "software" de reconocimiento de voz. La recopilación tendría lugar mediante la realización de llamadas telefónicas efectuadas desde un Estado miembro de la Unión Europea.

En relación con esta cuestión, se considera que siempre que quien haya de realizar el tratamiento tenga conocimiento directo o indirecto de quién es la persona cuya voz está siendo objeto de grabación, así como de su número de teléfono, la grabación efectuada tendrá la naturaleza de dato de carácter personal y el tratamiento efectuado estará sometido a la

normativa de protección de datos, al incorporarse al mismo los datos identificativos del sujeto (nombre y apellidos), su número de teléfono y su voz, conforme a lo dispuesto en el artículo 3.a) de la LORTAD y el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, que indica que dichos datos podrán proceder de información acústica.

Por otra parte, se suscitaba la cuestión de que los datos iban a ser recogidos mediante llamadas telefónicas efectuadas desde otro Estado miembro de la Unión Europea, planteándose si en dicho caso existirá una transferencia internacional de datos.

A estos efectos, se indicó, en primer lugar que, como se desprende de lo establecido en el artículo 4 de la Directiva 95/46/CE, será aplicable la Ley española siempre que el tratamiento se efectúe en territorio español, considerándose a estos efectos que habrá de tenerse en consideración el lugar en que radique la persona cuyos datos están siendo objeto de recogida. Por ello, la recogida de estos datos exigirá el cumplimiento de las disposiciones de la LORTAD para dicha recogida.

3.2.2. Cuestiones relacionadas con el Padrón Municipal de habitantes.

Se han venido planteando durante los últimos años diversas cuestiones relativas a la posible cesión por las corporaciones locales de los datos contenidos en el Padrón Municipal de Habitantes a diversos organismos e instituciones, públicas o privadas, o a particulares. Del mismo modo, estas cuestiones han sido planteadas por el Instituto Nacional de Estadística.

Ante esta situación, se ha hecho preciso el análisis, con carácter general, de la cuestión, sin perjuicio de la resolución de cada caso concreto.

Con carácter general, ha de partirse del principio de delimitación de la finalidad a las cesiones entre Administraciones Publicas consagrado por el artículo 19 de la LORTAD, al exigir que si los datos son cedidos a otras Administraciones Publicas sirvan sólo para el ejercicio de competencias iguales o que versen sobre materias semejantes, con la única excepción de que el cambio de finalidad esté prevista en las disposiciones de creación del fichero o por una disposición posterior de igual o superior rango, pudiendo ser sustituida la necesidad del consentimiento para el cambio de finalidad por una previsión realizada en una disposición de carácter general de rango suficiente que complemente las previsiones realizadas en la norma de creación del fichero, de modo que, en aras del interés público, se sustituye el consentimiento para el tratamiento y para las alteraciones en la finalidad a que sirve este por una previsión de una norma jurídica.

Asimismo, del apartado tercero de dicho artículo 19 se deduce que no es posible, sin el consentimiento del ciudadano, ceder datos de un fichero de titularidad pública a uno de titularidad privada, salvo previsión legal en contrario.

El régimen jurídico del Padrón municipal viene recogido en los artículos 15 y siguientes de la Ley de Bases de Régimen Local, en la redacción dada por la Ley 4/1996, de 10 de enero, normativa que debe considerase como la disposición de creación del fichero «Padrón municipal», en cuyo cumplimiento los municipios deben organizar y mantener el fichero previsto legalmente, de modo que los cambios en la finalidad a que se destina el mismo deben hacerse mediante una norma de modificación de la citada Ley Reguladora de las Bases del Régimen Local.

De la LBRL se deduce que la finalidad para que sirven los datos del Padrón municipal es la constitución de la población del municipio (artículo 15.2 LBRL), la adquisición de la condición de vecino (art. 15.3 y 4) y la acreditación de la residencia en el municipio y del domicilio habitual del mismo (art. 16.1).

Para la efectividad de la atención de estas finalidades se establece la obligación de inscripción en el Padrón municipal por parte de quien resida habitualmente en el municipio respectivo, lo que supone una excepción al principio básico de la necesidad del consentimiento del ciudadano para la legalidad del tratamiento de sus datos.

La cantidad de información que se acumula hace del Padrón municipal un fichero que despierta un enorme interés para las Administraciones Públicas así como para los particulares, recogiéndose en el articulo 16.3 de la LBRL los principios que regulan ese tratamiento.

El artículo citado dispone, en primer lugar, la posible cesión de datos a las Administraciones públicas para el ejercicio de sus respectivas competencias y, exclusivamente, para asuntos en los que la residencia y el domicilio sean datos relevantes. Respecto del resto de supuestos se remite el precepto comentado a la LORTAD.

Según se entiende por la Agencia de Protección de Datos, una interpretación literal de este precepto que conduciría a que cualquier Administración Pública que se interese por algún dato de un ciudadano pudiera consultarlo libremente en el Padrón municipal, no puede admitirse como valida, puesto que es una regla general que contradice lo dispuesto en los principios generales del Título I de la LORTAD y en el artículo 19 que regula el régimen de cesiones de datos de ficheros de titularidad pública, sin que sea válido entender que, si los artículos 18 y 19 de la LORTAD tienen rango de Ley ordinaria (Disp. Final tercera de la LORTAD), la LBRL tiene rango suficiente para modificar o derogar tales preceptos, puesto que el amparo de las especialidades recogidas en estos artículos está en el artículo 6.1 (orgánico), que autoriza la excepción por Ley a la necesaria obtención del consentimiento. Ello se debe a que esa interpretación debería armonizarse con lo dispuesto en el artículo 4.2 de la LORTAD, que establece la delimitación de la finalidad, lo que supone que la finalidad consentida por el ciudadano o autorizada por la Ley tiene que estar determinada, por lo que no cabe un tratamiento de datos personales creado o modificado sin concretar la finalidad o finalidades a que se destina.

Por ello, se considera por la Agencia de Protección de Datos más acertado entender el precepto comentado en el sentido de que la expresión «datos del Padrón municipal» que se emplea en el artículo 16.3 de la LBRL se refiere, no a la totalidad de la información que se contiene en el Padrón, sino, a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio.

Además, debe tenerse en consideración que existen numerosas excepciones a esta regla general, como son, como son las establecidas en las Leyes Orgánicas de Reclutamiento y de Régimen Electoral General, la establecida en el artículo 11.3 f) de la LORTAD, respecto de cesiones a la Administración Sanitaria, la establecida en el artículo 20 de la LORTAD, respecto de cesiones a las Fuerzas y Cuerpos de Seguridad, las previsiones de la Ley Orgánica 4/1981, de 1 de junio, Reguladora de los Estados de alarma, excepción y sitio, la establecida en la Ley Orgánica del Poder Judicial y en el artículo 11.2 d) de la LORTAD, respecto de la colaboración con la Administración de Justicia y determinadas instituciones públicas, la Ley General Tributaria, de colaboración con la AEAT, así como la Ley General de la Seguridad Social, en cuanto a procedimiento recaudatorio de recursos, así como en cualesquiera otras disposiciones con rango de Ley que regulen efectivamente excepciones a la norma fundamental en materia de protección de la privacidad sin suponer una derogación de hecho de la misma.

Por último, y aunque su entrada en vigor no vaya a tener lugar hasta el mes de enero de 2000, debe señalarse que el párrafo primero de la Disposición Adicional Segunda de la Ley Orgánica 15/1999 establece que: "la Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población".

Esta disposición prevé exclusivamente la posibilidad de que el censo poblacional al que la misma se refiere pueda ser solicitado por las Administraciones Estatal y Autonómica del Instituto Nacional de Estadística, único al que se autoriza expresamente la cesión inconsentida de los datos a que la Disposición se refiere, por lo que los Ayuntamientos sólo podrán ceder los datos padronales en aquellos supuestos que se han indicado. En los demás casos, sólo está admitida por la Ley la cesión que efectúa el Instituto Nacional de Estadística, en los términos previstos en la citada Disposición Adicional Segunda.

3.2.3. **Cuestiones relacionadas con el Reglamento de Medidas de Seguridad (Real Decreto 994/1999, de 11 de junio).**

La entrada en vigor 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, que desarrolla el artículo 9 de la LORTAD, ha supuesto el planteamiento de distintas cuestiones relacionadas con las previsiones contenidas en el mismo, tal y como puede comprobarse en el gráfico referido a la distribución de las consultas planteadas en 1999, atendiendo a las materias a que las mismas se refieren, de forma que casi un 12% de las consultas planteadas en el año se refiere a esta materia, siendo importante destacar que todas ellas fueron planteadas durante el segundo semestre.

A continuación se hará referencia a aquellas cuestiones planteadas que, a juicio de la Agencia, revisten una mayor relevancia a efectos de su conocimiento por la totalidad de las personas y entidades que hayan de implantar el Reglamento.

3.2.3.1. *Aplicación de los niveles de seguridad*

En este apartado se hará referencia a aquellas cuestiones relacionadas con los ámbitos establecidos para cada nivel de seguridad en el artículo 4 del Reglamento, centrándonos en aquellas que revisten una mayor complejidad.

3.2.3.1.1. *Alcance de la referencia a los servicios financieros*

Siendo el sector financiero uno de los más afectados por las disposiciones reguladoras de la protección de datos, una de las principales cuestiones relacionadas con el alcance de los diversos supuestos que han de entenderse contenidos en cada uno de los niveles de seguridad a que se refiere el artículo 4 del Reglamento es el sentido que ha de darse a la expresión "servicios financieros", contenida en su apartado segundo, respecto de cuyos ficheros se exige la adopción de medidas de seguridad de nivel medio.

Para delimitar el sentido de esta referencia deberá atenderse al ámbito que, en relación con dicho tipo de servicios, establece la normativa vigente que, en todo caso, excederá de lo que deba de ser considerado, meramente, como servicios bancarios o actividades tradicionales llevadas a cabo por las entidades de crédito.

En concreto, el Real Decreto 1560/1992, de 18 de diciembre, por el que se aprueba la clasificación nacional de actividades económicas, considera las actividades de intermediación financiera como una categoría específica, incorporada en el apartado "J" de la clasificación, estableciendo tres epígrafes separados para las actividades de intermediación financiera en sentido estricto, las relacionadas con seguros y planes de seguros (excepto Seguridad Social obligatoria) y las actividades auxiliares de las anteriores.

Partiendo de esta clasificación, no cabe duda de que habrán de ser consideradas actividades de intermediación financiera, y por ello integradas en el concepto "servicios financieros" al que se refiere el artículo 4.2 del Reglamento de Medidas de Seguridad, las actividades incluidas en el epígrafe 65 (intermediación financiera) y las incorporadas al epígrafe 67.1 (auxiliares de las anteriores).

Estas actividades, que sin duda habrán de ser incorporadas al artículo 4.2 son la intermediación monetaria, las actividades relacionadas con la Banca Central, Bancos, Cajas y Cooperativas, las actividades de arrendamiento financiero, las llevadas a cabo por Sociedades de crédito hipotecario, entidades de financiación, Sociedades mediadoras en el mercado de dinero y el Instituto de Crédito Oficial (ICO),así como las efectuadas por Instituciones de inversión colectiva de carácter financiero, Sociedades y fondos de capital riesgo y otras sociedades de inversión en activos financieros. También son servicios financieros los relacionados con la Administración de mercados financieros, y las actividades llevadas a cabo por Sociedades de valores, sociedades de garantía recíproca y de reafianzamiento, sociedades de tasación, casas de cambio, fondos de garantía de depósito y sus sociedades gestoras.

La consulta plantea el problema de la inclusión o no dentro del ámbito de los servicios financieros de las actividades relacionadas con la prestación de servicios relacionados con los seguros y planes de pensiones. En relación con esta actividad, la conclusión que puede alcanzarse es, en principio, proclive a considerar las actividades aseguradoras como de prestación de servicios financieros. Así se deduce de lo establecido en la Exposición de Motivos de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los seguros privados, al indicar que la dinámica que les afecta (a la actividad aseguradora y la concerniente a los planes y fondos de pensiones) es de las más avanzadas de nuestro sistema financiero".

En este mismo sentido, debe recordarse que el artículo 8.4 de la Ley 13/1992, de 1 de junio, reguladora de los Recursos propios y supervisión en base consolidada de las Entidades Financieras, incluye a las Sociedades Gestoras de Fondos de Pensiones entre las entidades financieras que deberán incluirse en el grupo consolidable de entidades de crédito lo que no hace sino reiterar su configuración como entidades prestadoras de servicios financieros.

Por su parte, la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, considera, en su artículo 2 b), servicios financieros "cualquier servicio relativo a las actividades de las entidades de crédito, de las compañías de seguros y de las empresas de inversiones".

Por este mismo motivo la Clasificación Nacional de Actividades Económicas, a la que anteriormente se ha hecho mención incluye dentro de los servicios de intermedidación financiera los relacionados con seguros de vida (incluso si se realizan por entidades de previsión social), los planes de pensiones y, dentro del epígrafe referido a "seguros no vida", los seguros de daños y el reaseguro. Asimismo se consideran actividades de intermediación financiera las efectuadas por agentes y corredores de seguros e intermediarios de seguros.

3.2.3.1.2. *Sentido de la expresión "datos relativos a Hacienda Pública".*

En segundo lugar, se ha planteado reiteradamente el alcance que ha de darse a la expresión "ficheros que contengan datos relativos a Hacienda Pública", contenida en el artículo 4.2 del Reglamento.

A este respecto, la Agencia de Protección de Datos ha considerado que la expresión anteriormente citada se refiere exclusivamente a los ficheros cuya titularidad corresponda a la Hacienda Pública, debiendo entenderse esta expresión como aplicable a aquellos ficheros cuyo responsable sea una Administración Pública que ostente potestades en materia tributaria; esto es aquellos ficheros cuyo responsable sea la Agencia Estatal de la Administración Tributaria, los que correspondan a las Comunidades Autónomas en materia de Tributos que les hayan sido cedidos o aquellos padrones fiscales, correspondientes a los tributos locales, de los que son responsables las Haciendas Locales, como por ejemplo los regulados en los artículos 77.1 y 91.1 de la Ley 39/1988, de 28 de diciembre, Reguladora de las mismas y cualesquiera de las Administraciones Públicas que tengan por objeto la exacción de algún recurso de naturaleza tributaria.

En consecuencia, la expresión contenida en el articulo 4.2 resultará aplicable exclusivamente a estos ficheros, de titularidad pública y nunca a ficheros de titularidad privada, aunque de los mismos pudiera derivarse la existencia de datos con transcendencia tributaria.

3.2.3.1.3. *Especialidades relativas a los ficheros de nóminas*

Por último, ha sido objeto de frecuente consulta el nivel de seguridad que habrá de ser aplicado a los ficheros de la nóminas, tomando en consideración que en los mismos pueden incluirse datos referentes a la afiliación a sindicatos, grado de minusvalía y retenciones a cuenta del Impuesto sobre la Renta de las Personas Físicas.

Con carácter general, debe indicarse que estos ficheros se encontrarán sujetos al nivel de seguridad básico en caso de que en los mismos no se contenga ninguno de los datos a los que posteriormente se hará referencia.

En cuanto a los datos relativos a las retenciones, y por los motivos que se acaban de indicar, el tratamiento por el empresario de tales datos no supone la inclusión del fichero dentro de los que se refieren a la Hacienda Pública.

El problema se circunscribe, en consecuencia, a establecer el nivel de protección que deberá ser impuesto sobre los ficheros de nóminas en caso de que los mismos contengan datos relativos a la afiliación sindical y a la salud de las personas.

Pues bien, de lo establecido en el artículo 4.3 del Reglamento se deduce que, con independencia de la finalidad en virtud de la cual se haya procedido al tratamiento de los datos, será imprescindible que siempre que al fichero se incorporen este tipo de datos se apliquen las medidas de nivel alto.

Sin perjuicio de lo anteriormente señalado, la Agencia de Protección de datos ha puesto de manifiesto que será posible que se proceda a la creación de diversos ficheros, conteniendo cada uno de ellos datos diferenciados que permitan la implantación en cada caso de medidas de distinto nivel (por ejemplo, discriminado los datos de salud e ideología en un fichero distinto al que contengan los datos identificativos básicos de los trabajadores o del puesto de trabajo que desempeñan). En todo caso, debe reiterarse que el nivel alto sólo será de aplicación en caso de que los ficheros contengan datos que hayan de ser considerados estrictamente como relacionados con la salud (por ejemplo, la indicación del grado de minusvalía) o con la afiliación sindical (por ejemplo, a efectos de deducir la cuota sindical correspondiente) u otros especialmente protegidos.

3.2.3.2. *Conceptos generales*

También ha generado diversos problemas relacionados con la aplicación del Reglamento, la delimitación del sentido y alcance que debe darse a ciertas expresiones contenidas en el mismo. A continuación nos referiremos a las de mayor relevancia:

3.2.3.2.1. *Concepto de "usuario".*

Se han planteado diversas cuestiones referentes al concepto que ha de darse a las referencias efectuadas por los artículos 9 y 11 del Reglamento, a las expresiones "usuarios" y "personal". En particular, si es posible cumplir con lo establecido en estos preceptos mediante una invocación general del departamento o unidad en que el personal ejerza sus funciones

El artículo 9 del Reglamento se refiere a la necesaria documentación y definición de las funciones y obligaciones atribuidas a cada una de las personas con acceso a los datos de carácter personal, añadiendo el apartado segundo que "el responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento".

Por su parte, en cuanto a lo establecido en el artículo 11, se exige al responsable del fichero la existencia de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información. En este sentido el artículo 2.2 del Reglamento define al usuario como sujeto o proceso autorizado para acceder a datos o recursos.

Del tenor de lo dispuesto en ambos artículos, parece deducirse que será indispensable que las obligaciones impuestas en ambos preceptos hagan referencia a las personas físicas con acceso a los datos o que ostenten la condición de usuarios de los mismos. Esta referencia, en virtud de lo indicado en el artículo 2.2, ya citado, podrá efectuarse bien mediante la plena identificación de la persona usuaria de los datos o bien mediante la indicación de las circunstancias concurrentes en la misma, como por ejemplo el puesto de trabajo desempeñado, de forma que sea posible conocer en cada momento la persona concreta que puede acceder a los datos por referencia a esas circunstancias. Ello permite diferenciar las obligaciones de identificación impuestas en los niveles de seguridad básico y medio, toda vez que respecto de este último el artículo 18 impone "la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información".

3.2.3.2.2. *Responsable de seguridad.*

Se han planteado también los requisitos que habrá de cumplir quien ostente la condición de responsable de seguridad, al que se refiere el artículo 16 del Reglamento, al indicar que "el responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento".

El Reglamento no especifica de forma taxativa los requisitos que habrá de cumplir este responsable de seguridad, si bien los mismos se desprenden de sus propias funciones, ya que le corresponderá, como se ha indicado "coordinar y controlar las medidas definidas en el documento de seguridad", analizando el contenido del informe de auditoría con el fin de proponer la adopción de las medidas pertinentes. Por ello, sin perjuicio de que su configuración habrá de depender según el tamaño de la empresa o la existencia de uno o varios centros de actividad, habrá de ser una persona con los conocimientos suficientes para llevar a cabo eficazmente estas funciones, adoptando las medidas necesarias para el cumplimiento de las medidas exigibles.

Además, debe añadirse que la delimitación del concepto de responsable de seguridad no exige que el mismo sea distinto del propio responsable del fichero, dependiendo esta circunstancia de la actividad llevada a cabo por éste. Por otra parte, debe indicarse que el responsable del seguridad no aparece como responsable a efectos de la imposición del régimen sancionador previsto en la LORTAD, recayendo tal responsabilidad sobre el responsable del fichero y, tras la entrada en vigor de la Ley Orgánica 15/1999, el encargado del tratamiento.

3.2.3.2.3. *Alcance de la auditoría a que se refiere el Reglamento.*

Se ha consultado a la Agencia de Protección de Datos si de lo dispuesto en el Reglamento de Seguridad se deduce la existencia de algún mecanismo de aprobación de los informes de auditoría de seguridad por parte de la propia Agencia.

En este sentido, el artículo 17 dispone, junto con la obligación general de someter los sistemas e instalaciones a auditoría y el contenido de ésta que "los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos". De ello se desprende que, una vez elaborado el informe de auditoría, deberán comunicarse sus resultados, adoptándose las medidas pertinentes, sin que ello exija una "aprobación" formal y externa de su contenido, que no habrá de ser remitido a la Agencia de Protección de Datos, sino "puesto a su disposición". Ello supone que será el responsable del tratamiento, siguiendo las recomendaciones del responsable de seguridad quien habrá de implantar las medidas precisas, derivadas del informe, de forma que, en caso de no implantarse y no cumplirse los requisitos de seguridad establecidos en el Reglamento, incurrirá en responsabilidad, constitutiva de infracción grave según el artículo 43.3 h) de la LORTAD, lo que se comprobará por esta Agencia de Protección de Datos a través del examen, en su caso, del informe de auditoría y de la implantación efectiva de las medidas requeridas.

Asimismo, se ha planteado en varias ocasiones si el sistema de auditoría establecido en la norma cuarta de la Instrucción 1/1995, de la Agencia de Protección de Datos, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito y del artículo 17 del Reglamento de Medidas de Seguridad se refieren a un mismo supuesto.

La respuesta a esta cuestión es afirmativa, dado que el contenido de ambas auditorias es similar, de forma que el artículo 17.2 del Reglamento de Medidas de Seguridad no hace sino reiterar, para la totalidad de los ficheros sometidos al nivel medio de seguridad, en los términos establecidos en el artículo 4.2 del propio Reglamento, lo que ya disponía el apartado quinto de la norma cuarta de la Instrucción 1/1995, diferenciándose únicamente ambos supuestos en que el Reglamento de Medidas de Seguridad no exige la remisión del informe de auditoria a la Agencia, quedando éste sin embargo a disposición de la misma

En consecuencia, teniendo en cuenta que el Reglamento de Medidas de Seguridad es norma posterior reguladora de la misma materia que la Instrucción 1/1995, en cuanto a los ficheros a los que se refiere el artículo 28 de la LORTAD, habrá de entenderse que la norma cuarta de la Instrucción ha sido derogada por el artículo 17 del Reglamento, siendo este el que habrá de regir en lo sucesivo para todos los ficheros sujetos a medidas de seguridad de nivel medio, entre los que se encuentran los relacionados con la solvencia patrimonial y crédito de las personas físicas.

3.2.3.3. *Implantación de las medidas de seguridad*

En relación con la implantación de las medidas se han planteado dos tipos de cuestiones: en primer lugar, al margen del supuesto en que existan encargados del tratamiento, a quién corresponde la implantación efectiva de las medidas de seguridad; por otra parte, se ha planteado en diversas ocasiones si los plazos a que se refiere la Disposición Transitoria Única del Reglamento son acumulativos o sucesivos.

En cuanto a la primera de estas cuestiones, la responsabilidad de la implantación de las medidas recaerá, a nuestro juicio, sobre el responsable del fichero, toda vez que, si bien el Reglamento no establece esta exigencia expresamente, la misma se deriva de su articulado. Así, por ejemplo, el artículo 6 exige autorización expresa del responsable del fichero para "la ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero". En el mismo sentido el artículo 16 impone al responsable del fichero la designación del responsable de seguridad.

En segundo lugar, se plantea concretamente si los distintos plazos establecidos para la implantación de cada uno de los tipos de medidas son sucesivos o si debe tenerse en consideración únicamente cada uno de los plazos de forma separada, dependiendo del nivel de seguridad que haya de establecerse para cada fichero.

A juicio de la Agencia, los plazos establecidos en la Disposición transitoria del Reglamento han de ser concebidos como independientes, de tal modo que, por ejemplo, el establecimiento de las medidas de seguridad de nivel medio deberá haberse efectuado, a lo sumo, transcurrido uno año desde la entrada en vigor del Reglamento.

Ello se funda en el hecho de que la regulación establecida en el Reglamento viene a establecer las medidas a adoptar de forma separada, aunque exigiendo en las de nivel superior medidas añadidas a las de nivel inferior. Precisamente por ello, y atendiendo a la complejidad de tales medidas, se establecen plazos mayores para la implantación de las medidas de mayor dificultad. Una interpretación contraria carecería de sentido, dado que no sólo se establecerían plazos mayores para la adopción de medidas de mayor complejidad, sino que dichos plazos se verían además incrementados por los concedidos para la adopción de medidas más sencillas, siendo así, que aplicando esa regla, el plazo para la implantación de medidas de nivel alto sería de tres años y seis meses, lo que no casa con el espíritu del propio Reglamento que establece un plazo máximo de tres años en caso de que "los sistemas de información que se encuentren en funcionamiento no permitan la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento".

En consecuencia, todos los ficheros que ya existieran al entrar en vigor el Reglamento deberán implantar las medidas de seguridad básicas en el plazo previsto en el mismo, gozando de lo que reste hasta completar el año desde la entrada en vigor del Reglamento para implantar las de nivel medio, en su caso, y de otro año más para implantar las de nivel alto si estuvieran obligados a ello.

3.2.3.4. *Otras cuestiones relacionadas con el Reglamento de Medidas de Seguridad*

3.2.3.4.1. Registros de acceso

También ha sido objeto de consulta el sentido en que se debe interpretar la medida relacionada con el registro de accesos, a la que se refiere el artículo 24 del Reglamento de Medidas de Seguridad, por cuanto se consideraba que la indicación de la totalidad de los extremos indicados en la norma podía resultar sumamente gravosa para la responsable del fichero.

Para realizar una correcta interpretación de la exigencia impuesta por esta norma, debe partirse de la regulación establecida con carácter general en el Reglamento para regular las medidas que garanticen un adecuado acceso a los ficheros que contengan datos de carácter personal. Dichas medidas se circunscriben a las previsiones contenidas en los artículos 12 y 19 del Reglamento, en lo referente al establecimiento de controles de acceso y acceso físico para los ficheros sujetos a medidas de nivel bajo y medio, respectivamente, y el ya citado artículo 24.

El artículo 2.7 del Reglamento define el control de acceso como el "mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos". En estos términos el articulo 12 se refiere al acceso como cualquier actuación por la que un usuario pueda tener conocimiento directo de "aquellos datos y recursos que precisan para el desarrollo de sus funciones". En desarrollo de este concepto, para los ficheros a los que el Reglamento quiere dotar de un máximo nivel de seguridad, el artículo 24 exige la llevanza del registro de acceso al que ya se ha hecho referencia.

De todo ello se desprende que el Reglamento no establece diferenciación alguna en atención a la persona que accede a los datos o de las actividades que aquella lleva a cabo, por lo que en el registro deberán figurar la totalidad de los accesos que se hayan producido.

3.2.3.4.2. *Transmisión de los datos a través de redes de Telecomunicaciones.*

Por otra parte, se ha planteado cuáles son los supuestos en que el artículo 26 del Reglamento de Seguridad exige el cifrado de datos cuando los mismos van a ser transmitidos a través de redes de telecomunicaciones.

En cuanto al ámbito de aplicación del articulo 26, aplicable únicamente a los ficheros que requieran medidas de seguridad de nivel alto, debe estarse al hecho de que en la transmisión de los datos se empleen redes de telecomunicaciones, definidas por el artículo 2. c) de la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, como "los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicaciones.

En consecuencia, las medidas a las que se refiere el artículo 26 del Reglamento serán de aplicación a la transmisión de datos entre distintas dependencias de la entidad cuando sea necesaria para dicha transmisión la utilización de redes de telecomunicaciones cuya titularidad sea ajena a la propia empresa, no siendo preciso el cifrado de los datos en caso de que las comunicaciones en ningún momento accedan a dicha red.

3.2.4. **Cuestiones relacionadas con el sector de las Telecomunicaciones.**

Tal y como se expone en otros lugares de esta memoria, la entrada en vigor del Real Decreto 1736/1998, de 31 de julio, que supone la transposición a nuestro Derecho de lo establecido en la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones, ha supuesto una gran incidencia tanto en la actividad del sector como en las relaciones que se producen entre el mismo y la Agencia de Protección de Datos.

En el presente epígrafe nos referimos a aquellas cuestiones en que ha sido preciso el parecer de esta Agencia, planteadas tanto por las propias operadoras como por las autoridades que intervienen en la regulación del sector (Secretaría General de Comunicaciones y Comisión del Mercado de las Telecomunicaciones).

3.2.4.1. *Cláusulas para el consentimiento al tratamiento de los datos.*

Se ha sometido al parecer de esta Agencia de Protección de Datos la conformidad con la vigente normativa reguladora de la protección de datos de carácter personal de distintas cláusulas existentes en los contratos de prestación de servicios telefónicos de diversas compañías de telecomunicaciones. La resolución de esta cuestión exige analizar coordinadamente lo dispuesto en la propia LORTAD con las normas reguladoras del sector, a las que ya nos hemos referido.

Así, con carácter general, el artículo 5.1 de la LORTAD prevé que: "los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero".

En similares términos a los indicados se pronuncia el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, que entrará en vigor el 14 de enero de 2000, si bien eliminando la referencia exclusiva al tratamiento automatizado (apartado a)), incluyendo entre los derechos de los afectados el de oposición (apartado d)) y estableciendo la posibilidad de que se haga constar la identidad y dirección del representante del responsable del fichero (apartado e)).

Por otra parte, en el ámbito de las telecomunicaciones, el artículo 65 del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento que desarrolla el Título III de la Ley General de Telecomunicaciones prevé, en su apartado segundo los datos que podrán ser objeto de tratamiento, limitándose a los siguientes:

"a) El número o la identificación del abonado.
b) La dirección del abonado y el tipo de equipo terminal empleado para las llamadas.
c) El número total de unidades que deben facturarse durante el ejercicio contable.
d) El número del abonado que recibe la llamada.
e) El tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitidos.
f) La fecha de la llamada o del servicio.
g) Otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes".

Además, el Reglamento especifica las finalidades a que podrán destinarse los datos, indicando que los mismos sólo podrán ser tratados "con objeto de realizar la facturación y los pagos de las interconexiones", así como "para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento previo".

De lo establecido en este precepto se desprende que será posible el tratamiento de los datos de facturación con fines de promoción comercial, si bien dicho tratamiento exigirá, en todo caso, el consentimiento previo del interesado. Por ello será absolutamente necesario que en los contratos se haga constar expresamente la facultad del usuario de no prestar su consentimiento a la utilización de los datos con fines de promoción comercial de los servicios de telecomunicaciones.

Por último fuera de las finalidades anteriormente indicadas, debe señalarse que, a tenor del artículo 65.1 "Los operadores deberán destruir los datos de carácter personal sobre el tráfico relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto termine la misma".

Con carácter general se apreció por la Agencia de Protección de Datos que ninguno de los contratos presentados a su informe contenía una cláusula expresa en que se permitiera, por el mecanismo indicado, al interesado oponerse al tratamiento de los datos. Del mismo modo, se apreció que las finalidades no aparecían expuestas con la debida claridad en la cláusula de protección de datos, toda vez que en las mismas se hacía referencia, generalmente a "labores de información, formación y comercialización del servicio de telefonía y de actividades relacionadas con el mismo". Del mismo modo, la Agencia apreció que en ninguno de los contratos se indicaba el carácter obligatorio o facultativo de las respuestas a las cuestiones que se planteaban.

3.2.4.2. *Teléfono de emergencia 112*

También se ha planteado por órganos de distintas Comunidades Autónomas la posibilidad de la recogida de los datos sin consentimiento del interesado para la prestación de servicios de atención de llamadas de emergencia a través del número de teléfono 112, teniendo en cuenta que en ciertos casos se procederá a tratar datos especialmente protegidos.

Con carácter general, se indicó que existe cobertura legal suficiente para que, en aplicación del artículo 6.2 de la LORTAD procediera el tratamiento de los datos sin recabar el consentimiento del afectado. En este sentido, cabe recordar lo siguiente:

1.- La creación del servicio de urgencias a través del número 112 tiene su origen en la decisión del Consejo de las Comunidades Europeas, de 29 de julio de 1991, debiendo recordarse que, conforme al artículo 189 del Tratado Constitutivo de la Comunidad Europea "la decisión será obligatoria en todos sus elementos para todos sus destinatarios".

2.- En este sentido, el servicio señalado viene expresamente reconocido en el artículo 40.4 de la Ley 11/1998, General de Telecomunicaciones, imponiendo a los operadores la obligación de encaminamiento de llamadas.

3.- Por su parte, la Directiva 97/66/CE, del Parlamento y del Consejo, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones establece, en su artículo 9 b) que "los Estados velarán por que existan procedimientos transparentes que determinen la forma en que el proveedor de una red pública de telecomunicación y/o de un servicio de telecomunicación accesible al publico puede anular la supresión de la presentación de la identificación de la línea llamante por línea, para las entidades reconocidas por un Estado miembro que atiendan las llamadas de urgencia, incluidos los cuerpos de policía, los servicios de ambulancia y los cuerpos de bomberos, para que puedan responder a tales llamadas".

4.- Por otra parte, el artículo 7 de la Directiva 95/46/CE, del Parlamento 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, prevé la posibilidad de tratamiento cuando el mismo sea necesario para "proteger el interés vital del interesado" (apartado d) o "para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos" (apartado e).

Además, se planteaba si procedía el consentimiento, a pesar de lo indicado, cuando se tratara de la recogida de datos relacionados con la salud de las personas, indicándose por la Agencia que será posible su tratamiento en caso de que la finalidad del fichero sea, precisamente, solucionar una urgencia que requiera acceder a un fichero automatizado, por cuanto este supuesto se encuentra exceptuado de la obligación de prestación del consentimiento para la cesión de datos automatizados, pudiendo entenderse aplicable al presente caso, dada la propia naturaleza del servicio de emergencias.

3.2.4.3. *Identificación de la línea llamante.*

También ha sido objeto de informe por parte de esta Agencia de Protección de Datos los escritos a los que se refiere el artículo 69.3 del Real Decreto 1736/1998, según el cual "los operadores citados en el apartado primero de este artículo (esto es, los operadores que, conforme a lo dispuesto en el artículo 40 del Reglamento, tengan la obligación de prestar servicios avanzados de telefonía con las facilidades de identificación de la línea llamante y de la conectada) informarán individualmente a cada uno de sus abonados, con quince días de antelación al inicio de la prestación de las facilidades de identificación de la línea llamante y de la línea conectada, de las características de dichas facilidades". Estas comunicaciones fueron sometidas al parecer de la Agencia de Protección de Datos, dado que el párrafo tercero del artículo 69.3 prevé que "los operadores deberán facilitar a la Agencia de Protección de Datos, con una antelación de quince días a la fecha de su envío, copia de la comunicación que vayan a utilizar para informar a sus abonados".

En particular, se planteó en un caso concreto si, pese a lo indicado en el párrafo segundo del artículo 69.3, que exige una segunda notificación a aquellos abonados que hubieran solicitado no aparecer en las guías de los operadores, era posible la realización de una única notificación.

A esta cuestión se respondió por la Agencia indicando que el espíritu y finalidad del Reglamento es asegurar que quienes personalmente han optado por la no incorporación de sus datos de carácter personal a los directorios de abonados no vean perjudicado el derecho a la intimidad por el que éstos han optado mediante la aparición, en las llamadas telefónicas que por ellos, se realicen de sus datos personales. Al propio tiempo se indicó que resultaba absolutamente clara la dicción del precepto, que prevé que estos abonados deberán recibir una comunicación adicional a la anterior, en la que poniéndose de manifiesto su especial situación, se explique con mayor detalle cómo la utilización de las mencionadas facilidades puede afectar a la protección de su intimidad.

En cuanto al contenido de los escritos, con carácter general se consideró que los mismos cumplían los requisitos exigidos por el Reglamento, si bien se apreció que en todos los casos se había omitido la referencia al código "067", establecido por la Resolución de 2 de diciembre de 1998 de la Secretaría General de Comunicaciones, recordándose asimismo que el coste del servicio en aquellos supuestos en que el Reglamento permitiera la repercusión del mismo al abonado deberá ser "orientado a costes".

3.2.5. Otras cuestiones de interés en matera de protección de datos

3.2.5.1. *Ejercicio de los derechos de acceso, rectificación y cancelación por medio de representante*

Se sometió al parecer de esta Agencia de Protección de Datos por varias empresas prestadoras de servicios de solvencia patrimonial y crédito el alcance de las normas por las que la LORTAD y el Real Decreto 1332/1994, de 20 de junio regulan el modo en que pueden ejercitarse por los afectados los derechos de acceso, rectificación y cancelación. La consulta se fundaba en la existencia de una pluralidad de solicitudes de ejercicio de estos derechos, planteadas por una determinada Asociación en virtud de mandato genérico otorgado por diversos interesados, por el que se autoriza a la misma a intervenir en su nombre ante cualesquiera responsables de ficheros para ejercer los derechos establecidos en la LORTAD, así como para obtener o facilitar documentación y ejercitar acciones ante esta Agencia de Protección de Datos y el Defensor del Pueblo.

Como punto de partida deberá tenerse en cuenta para resolver esta cuestión lo dispuesto en el artículo 11, párrafo primero, en conexión con el artículo 14.2, ambos del Real Decreto 1332/1994. A tenor del primero de estos preceptos "los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto". Por su parte, el artículo 14.2 establece que "tratándose de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado". En este mismo sentido se pronuncian las normas primera (apartado primero) y segunda (apartado quinto) de la Instrucción 1/1998 de la Agencia de Protección de Datos. Estos preceptos deberán ser interpretados tomando en consideración el hecho de que la LORTAD, según su artículo primero "en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos", y siguiendo el llamado "principio de interpretación conforme a la Constitución", reiteradamente consagrado por nuestro Tribunal Constitucional, según el cual las normas que conforman nuestro Ordenamiento Jurídico deberán ser interpretadas en el sentido que resulte más

congruente con lo que la Norma Suprema establece.

Tomando en consideración todo ello, la Agencia de Protección de Datos estima que la referencia que el artículo 11 del Real Decreto 1332/1994, relativa al ejercicio de los derechos de acceso, rectificación y cancelación por el afectado, deberá ser interpretada de modo que quede perfectamente conciliado su derecho a que ese ejercicio se produzca de la forma que le resulte menos gravosa (lo que resulta conforme con las garantías atribuidas por nuestro texto constitucional) con la seguridad de que sólo el interesado podrá ostentar la voluntad adecuada para decidir dicho ejercicio, dado el carácter personalísimo del derecho.

Pues bien, de lo establecido en este precepto, resulta evidente que sólo el interesado podrá efectuar la manifestación de su voluntad consistente en la emisión de una declaración por la que pretenda el ejercicio de los derechos de acceso, rectificación o cancelación, a menos que se trate de una persona que carezca de la suficiente capacidad de obrar, en cuyo supuesto su voluntad podrá resultar suplida por la de su representante legítimo (tal y como prevé el párrafo segundo). Ahora bien, lo establecido en el citado artículo 11 no obsta a que la declaración de voluntad que inequívoca y específicamente haya de efectuar el interesado pueda ponerse en conocimiento de su último destinatario (el responsable del fichero) a través de la persona a la que aquél haya legítimamente otorgado su representación.

En consecuencia, el artículo 11 del Real Decreto 1332/1994 pretende que nadie, salvo el propio interesado pueda decidir si quiere ejercitar los derechos que la LORTAD le atribuye, ante quién desea ejercitar esos derechos, a qué ficheros se refiere tal ejercicio y en qué condiciones habrá de producirse el mismo pero, una vez efectuada por el interesado una declaración clara, inequívoca y suficientemente explícita en ese sentido, la transmisión al responsable del fichero de esa declaración de voluntad, en los estrictos términos en que aquélla se haya manifestado, podrá encomendarse a un representante voluntario o mandatario, que actuará (dentro de esos límites) ante el responsable del fichero.

Por tanto, se estima que de lo dispuesto en el artículo 11 del Real Decreto 1332/1994 no se desprende una prohibición del ejercicio de los derechos de acceso, rectificación y cancelación por un representante voluntario o mandatario del propio afectado, por cuanto ese ejercicio se producirá siempre en nombre y por cuenta del propio afectado, considerándose el ejercicio del derecho por el mandatario como efectuado por el propio interesado que le confiere la representación (tal y como se desprende *a sensu contrario* de lo dispuesto en el artículo 1717 del Código Civil).

Por otra parte, se entiende que no son admisibles los apoderamientos genéricos, sino aquéllos que se refieran concretamente al ejercicio de alguno de los derechos consagrados por la LORTAD ante los responsables de los ficheros, indicando los términos en que el apoderamiento se realiza, sin que el mandatario pueda, en modo alguno, exceder de lo dispuesto en esos términos y sin que quepa atribuir al mismo una potestad genérica de actuación. Esta atribución genérica desvirtuaría la exigencia contenida en el artículo 11 del real Decreto 1332/1994, por cuanto no supondría una concreta manifestación de la voluntad del interesado de ejercitar los derechos, toda vez que éstos serían ejercidos únicamente si el apoderado lo considerase oportuno y en los términos en que el mismo estimase adecuados.

Por último, en cuanto a los requisitos formales que deberá ostentar el apoderamiento que se confiera, no será posible un mandato verbal puesto que sólo mediante un apoderamiento escrito podrá conocer el responsable del fichero la concreta voluntad de ejercicio del derecho por el afectado. Por otra parte, si el apoderamiento fuera efectuado mediante documento privado sería preciso, a fin de que el mismo pudiera dar fe ante el responsable del fichero que dicho apoderamiento deriva directa e inequívocamente del interesado, titular del derecho protegido, que la firma de éste último apareciera autenticada mediante medio que permitiese a aquél tener perfecto conocimiento de que la declaración de voluntad procede inequívocamente del propio afectado, aportándose por el representante el original de dicho apoderamiento. Por último, será posible el ejercicio del derecho por apoderado cuyo poder aparezca otorgado en escritura pública, siempre y cuando dicho apoderamiento cumpla los requisitos de contenido a los que nos hemos referido con anterioridad.

En todo caso, lo indicado hasta ahora debe entenderse aplicable a los supuestos de ejercicio de los derechos ante el responsable del fichero. En caso de que el afectado pretenda solicitar la tutela de sus derechos ante la Agencia de Protección de Datos, conforme a lo establecido en el artículo 17 de la LORTAD, la representación se regirá por lo dispuesto en el artículo 32.3 de la Ley 30/1992, según el cual la representación deberá acreditarse "por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado".

3.2.5.2. *Solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal.*

Se ha planteado por diversas empresas la posibilidad de acceder a solicitudes efectuadas por miembros de las Fuerzas y Cuerpos de Seguridad, ejerciendo funciones de Policía Judicial, cuando no existe un previo mandato del órgano jurisdiccional o requerimiento del Ministerio Fiscal para que se obtengan los datos, llevando a cabo la actuación por propia iniciativa o a instancia de su superior jerárquico.

En este caso nos encontramos ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, por lo que resultará aplicable a este segundo supuesto lo dispuesto en el artículo 20.2 de la LORTAD, según el cual "la recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la

prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad".

El citado artículo habilita a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan las siguientes condiciones:

Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.

Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.

Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.

Que, en cumplimiento del artículo 20.4 de la LORTAD, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

Con referencia a la última de las conclusiones señaladas, debe indicarse que, tratándose de actuaciones llevadas a cabo en el ámbito de las competencias consagradas en el apartado a) del artículo 445.1 de la Ley Orgánica del Poder Judicial, la Policía Judicial se encuentra obligada a dar cuenta de los hechos a la Autoridad Judicial y Fiscal de forma inmediata.

A mayor abundamiento, debe recordarse que, conforme dispone el artículo 11.2 b) de la LORTAD, procederá la cesión si ésta "tiene por destinatario...al Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas", lo que, conforme se ha señalado, ocurre en el presente supuesto, dada la obligación de los miembros de la Policía Judicial de poner los datos que hayan sido obtenidos en conocimiento de la Autoridad Judicial o Fiscal. Por ello, la cesión solicitada tendrá amparo no sólo en el artículo 20.2 de la LORTAD, sino también en el propio artículo 11.2 d) de la misma, siendo en consecuencia conforme a la LORTAD el cumplimiento de la cesión solicitada.

3.2.5.3. *Naturaleza de los datos psicológicos a efectos de su tratamiento.*

Se planteó por una Corporación Local la posibilidad de proceder, dentro del tratamiento de los datos efectuado en el ámbito de sus competencias en materia de asistencia social, al tratamiento de datos de carácter psicológico, incluyendo determinados datos, obtenidos de la apreciación subjetiva de las personas encargadas de llevar a cabo la realización material de encuestas, referentes a los "problemas" que presenta el perfil psicológico de los sujetos encuestados (tales como dificultades en el aprendizaje, alcoholismo, drogodependencia, ludopatía, conflictos de pareja, síntomas depresivos, conflictos de adaptación al medio familiar o social, desarraigo, etc.).

La resolución de esta cuestión exige delimitar la naturaleza jurídica de los datos anteriormente enumerados, a fin de concluir si procede su inclusión dentro del concepto de datos referentes a la salud de las personas, debiendo partirse en el estudio del concepto que quepa dar a los datos de salud, tomando en cuenta las normas, nacionales e internacionales, vigentes en España.

Si bien la LORTAD se refiere expresamente a los datos de salud, considerándolos expresamente protegidos y limitando la posibilidad de su recopilación y cesión, no establece un concepto concreto de este tipo de datos.

Ello exige atender, para la delimitación del concepto establecido en la Ley Orgánica, por imperativo del artículo 10.2 de nuestra Constitución a las normas contenidas en Tratados Internacionales reguladores de la Protección de Datos de carácter personal que hayan sido válidamente ratificados por España, pasando a formar parte de su ordenamiento interno, según dispone el artículo 1.5 del Código Civil.

En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, como el artículo 6 del Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección, de tal forma que, como indica el citado Convenio, tales datos "no podrán tratarse automáticamente a menos que el derecho interno prevea garantías adecuadas".

El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de "datos de carácter personal relativos a la salud", considerando que su concepto abarca "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo", pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que "debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas".

En este mismo sentido, la Recomendación nº R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos afirma que "la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas".

En cuanto a la incorporación al citado concepto de los datos psicológicos y referentes a la salud mental de las personas, baste recordar la existencia de la Recomendación nº R (91) 15 del Comité de Ministros, en materia de estudios epidemiológicos en el ámbito de la salud mental, en la que se hace expresa referencia a la necesidad de establecer las garantías necesarias para la protección de los datos referentes a este tipo de transtornos .

De todo lo anteriormente expuesto se desprende que los datos psicológicos deben ser considerados, a los efectos de la aplicación de la LORTAD, como datos relativos a la salud de las personas. Para delimitar el fundamento de esta inclusión habrá de distinguirse entre los datos incorporados a historiales clínico-psiquiátricos o psicológicos y los no incorporados a los mismos:

En cuanto a los primeros, atendidos los conceptos ya señalados, no puede existir duda alguna acerca de la naturaleza, como datos de salud, de los datos que se deriven expresamente de expedientes médicos, habida cuenta que, comprendiendo el concepto de datos sanitarios los referentes a la salud mental, siempre habrán de incorporarse al concepto de aquéllos cualesquiera datos obrantes en una de las fuentes de tratamiento establecidas en el artículo 8 de la LORTAD.

El problema se planteará en relación con aquellos datos que no se deriven de un determinado tratamiento psicológico o psiquiátrico, sino en las propias manifestaciones de los sujetos encuestados o en la apreciación del encuestador ante las citadas afirmaciones. En este caso, cabría plantearse la inclusión de los datos en el concepto anteriormente señalado.

La respuesta a esta cuestión, es la de considerar que estos datos, aún cuando no procedan expresamente del historial clínico de los sujetos, deben ser considerados como datos referentes a la salud de las personas, habida cuenta que, o bien conciernen directamente a la salud mental del individuo (apartado 45 de la Memoria del Convenio 108) o bien se encuentran estrechamente relacionados con la salud (Recomendación R (97) 5 del Comité de Ministros).

La justificación de esta incorporación es evidente, dado que el sometimiento de estos datos a la especial protección conferida por los artículos 7.3, 8 y 11.2 f) de la LORTAD evita que se pueda proceder al tratamiento de estos datos con base en meras sospechas o apreciaciones subjetivas que no presenten una constatación fáctica real, generando una situación de riesgo que puede, con base en esas sospechas o apreciaciones, crear una situación social de prejuicio hacia las personas cuyos datos psicológicos "negativos" han sido incorporados al fichero automatizado.

Precisamente, éste es el motivo que indujo a incorporar al concepto de "datos de carácter personal relativos a la salud" incluido en la memoria del Convenio 108 del Consejo de Europa, "las informaciones relativas al abuso del alcohol o al consumo de drogas", cuando estos datos no se refieren, en sentido estricto, a la salud de las personas.

A mayor abundamiento, no debe olvidarse que el tratamiento de datos de carácter psicológico podría, en la práctica, generar un perfil completo del individuo, del que se desprendiese el conocimiento de otros datos especialmente protegidos por el legislador, tales como las creencias morales y religiosas o la vida sexual del sujeto. Ello no hace sino ratificar la conclusión del necesario sometimiento de los datos de carácter psicológico al régimen de los datos relativos a la salud de las personas, consagrado por la LORTAD.

En consecuencia, se ha entiendo que los datos de carácter psicológico o psiquiátrico han de ser considerados datos especialmente protegidos referentes a la salud de las personas, regulados en el artículo 7.3 de la LORTAD.

3.2.5.4. *Conformidad a la LORTAD en los supuestos de contestación a preguntas parlamentarias cuando la contestación contiene datos de carácter personal.*

Se ha planteado a la Agencia de Protección de Datos el problema de si es posible que se aporte determinada información, en respuesta a una pregunta parlamentaria escrita, teniendo en cuenta que la misma incluye un listado nominativo de personas.

Con carácter general, debe indicarse que dicha relación contendrá datos de carácter personal, toda vez que el artículo 3 a) de la LORTAD, define los mismos como cualquier información concerniente a personas identificadas o identificables.

Dicho lo anterior, la entrega de los datos a las Cámaras constituye un supuesto de cesión de datos de carácter personal, respecto de la que establece el artículo 11.1 de la LORTAD que sólo será posible efectuarla previo consentimiento del interesado, si bien el artículo 11.2 de la Ley Orgánica exceptúa del consentimiento aquellos supuestos en los que una norma con rango de ley habilite la cesión de los datos.

En este sentido, el artículo 111.1 de la Constitución Española dispone que "el gobierno y cada uno de sus miembros están sometidos a las interpelaciones y preguntas que se le formulen en las Cámaras". La interpretación de este precepto debe realizarse en el sentido de que el sometimiento a las citadas preguntas se materializa en el deber de contestación, de modo que debe entenderse que dicho deber de contestación determina como consecuencia la obligación de facilitar a las Cámaras la información que sea requerida en la pregunta.

La única limitación que cabe considerar a este respecto es la establecida en el articulo 186, apartados 2 y 3, del Reglamento del Congreso de los Diputados de 1982 y el artículo 162, apartados 2 y 3 del Reglamento del Senado, texto refundido de 3 de mayo de 1994, que previene que "no serán admitidas preguntas de exclusivo interés personal de quien las formula o de cualquier otra persona singularizada, ni las que supongan consulta de índole estrictamente

jurídica. La Mesa calificará el escrito y admitirá la pregunta si se ajusta a lo establecido en el presente capítulo".

En consecuencia, tan sólo cabe entender limitada la obligación de contestar las preguntas de la Cámara cuando concurran las circunstancias señaladas, en el bien entendido que la competencia para poder calificar la concurrencia o no de tales circunstancias corresponde a la Mesa.

3.2.5.5. *Utilización de los datos del Censo Electoral por responsables de ficheros de titularidad privada.*

Se ha planteado reiteradamente si es posible que por las empresas del sector de la publicidad y del marketing directo pueda procederse al tratamiento automatizado de datos contenidos en el Censo Electoral. Ello se ha fundado en la aprobación de la Ley de Ordenación del Comercio Minorista, de la que, según algunos responsables, parecía deducirse la posibilidad de efectuar dicho tratamiento.

Sentado lo anterior, la cuestión se circunscribe a determinar si el censo electoral tiene el carácter de fuente accesible al público, en los términos previstos en el artículo 6.2 de la LORTAD. Según prescribe el citado precepto, no será preciso el consentimiento del interesado cuando los datos de carácter personal se recojan en fuentes accesibles al público, añadiendo el artículo 11.2 b) que, en estos casos no será preciso el previo consentimiento del afectado para la cesión de los datos.

El artículo 41.2 de la Ley Orgánica 5/1985, reguladora del Régimen Electoral general establece que "queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial".

En este sentido, hay que tener en cuenta que la Junta Electoral Central en fecha 2 de octubre de 1995, en contestación a una consulta formulada por el Director de la Agencia de Protección de Datos, señala que "en virtud de lo establecido en el artículo 41 de la Ley Orgánica del Régimen Electoral General, está prohibida la información particularizada de los datos personales contenidos en el censo electoral, no estando permitida la recopilación de los datos existentes en las mismas por cualquier medio sea manual, fotográfico, informático o de cualquier otra naturaleza, bajo las responsabilidades legales procedentes".

Como consecuencia de la aprobación de la Ley de Ordenación del Comercio Minorista y el tenor literal de su artículo 40. 1 se vuelve a formular consulta sobre la prohibición del artículo 41 de la Ley Orgánica del Régimen Electoral General, señalándose expresamente que "dado el carácter orgánico de la Ley del Régimen Electoral General, esta Junta Electoral Central considera que la Administración Electoral y la Oficina del Censo Electoral han de atenerse a lo dispuesto en el articulo 41.2 de la citada Ley, a cuyo tenor: "Queda prohibida cualquier información particularizada sobre los datos personales contenidos en el Censo Electoral, a excepción de los que se soliciten por conducto judicial". En el marco de dicho precepto se entiende que el nombre, apellidos y domicilio de los electores constituyen datos personales de los mismos, que únicamente pueden usarse para los propios fines para los que han sido recogidos, con la única excepción prevista en el articulo referido de datos que se "soliciten por conducto judicial".

En virtud de todo ello, la Agencia de Protección de Datos considera que de acuerdo con los criterios señalados que el Censo Electoral no constituye una fuente accesible al público, en los términos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal.

No obstante, debe indicarse que la cuestión ha sido resuelta por la regulación, por el artículo 31 de la Ley Orgánica 15/1999, del censo promocional, cuya elaboración corresponderá al Instituto Nacional de Estadística.

4. ANALISIS DE LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL RELACIONADA CON EL ARTICULO 18.4 DE LA CONSTITUCION

Durante 1999 se han dictado por el Tribunal Constitucional tres sentencias, la 30/1999, de 8 de marzo y la 44/1999 y 45/1999, de 23 de marzo, que guardan directa relación con las cuestiones relativas a la protección de datos de carácter personal. En ellas, el Tribunal Constitucional viene a reiterar la doctrina sentada a lo largo de 1998, año en que se dictaron otras 18 sentencias sobre el mismo supuesto de hecho, consagrando el denominado derecho a la "autodeterminación informativa".

Las tres sentencias se refieren a un mismo supuesto, consistente en la utilización por el empresario de datos relacionados con la afiliación sindical para deducir las cantidades derivadas del ejercicio por los trabajadores de su derecho de huelga. Al mismo tiempo, todas ellas vienen a reiterar la doctrina sentada por el Tribunal a partir de su sentencia 11/1998, de 13 de enero.

A continuación pasamos a hacer un somero comentario de los antecedentes y razonamientos contenidos en las sentencias citadas.

Antecedentes.

Los recurrentes, afiliados a un determinado sindicato, prestaban servicios para la empresa RENFE.

El Comité Empresa de RENFE convocó huelga, apoyada por los Sindicatos CC OO y CGT -no por UGT y SEMAF- para los días 11, 13, 15, 18, 20, 22, 25, 27 y 29 de abril de 1994, pero únicamente de seis treinta a ocho treinta y de diecio-

cho treinta a veinte treinta horas, no coincidiendo estos horarios con aquellos en los que los trabajadores recurrentes desarrollaban su jornada.

Pese a que los recurrentes no participaron en la huelga y así lo comunicaron a la Empresa, por el responsable de la dependencia donde aquellos desarrollaban su labor se les descontaron las retribuciones correspondientes en la nómina del mes de mayo de 1994. No obstante, su reclamación de reintegro de la cantidad fue atendida en el mes de junio. Al efecto, la Empresa cursó instrucciones para que ante posibles errores en los descuentos practicados, el personal presentara con urgencia la oportuna reclamación y pudieran abonarse las diferencias en nómina adicional de mayo o en la nómina regular de junio.

El descuento afectó, asimismo, a la práctica totalidad de los empleados respecto de los que constaba su afiliación a CC OO y en medida muy inferior a los afiliados a otros Sindicatos convocantes e incluso a trabajadores sin opción sindical declarada. La Empresa conoce el dato de la afiliación porque descuenta de los salarios la cuota sindical mediante diversas claves informáticas, una específica para cada Sindicato.

Fundamentación jurídica.

La sentencia otorga el amparo solicitado por los trabajadores, al entender vulnerado el artículo 28.1, en conexión con el artículo 18.4, ambos de la Constitución, refiriéndose al contenido del denominado derecho a la "libertad informática" (*habeas data*).

En relación con la configuración del derecho contenido en el artículo 18.4 de la Constitución, el Tribunal Constitucional pone de manifiesto la doble naturaleza de este derecho, al consistir en un derecho autónomo que, a su vez, resulta ser un derecho instrumental ordenado a la protección de otros derechos fundamentales.

En este sentido, la sentencia configura el llamado derecho a la libertad informática o, según la doctrina alemana, derecho a la autodeterminación informativa, al indicar que el derecho contemplado en el artículo 18.4 "además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos". Además se indica que "la garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático *(habeas data)* y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

Siguiendo con esta tesis, el Tribunal recalca la doble naturaleza del derecho consagrado en el artículo 18.4 de la Constitución. Así, se señala que "el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical, entendida ésta en el sentido que ha sido establecido por la doctrina de este Tribunal, porque es, en definitiva, el derecho que aquí se ha vulnerado como consecuencia de la detracción de salarios, decidida por la empresa al trabajador recurrente por su incorporación a determinado Sindicato".

Pero al propio tiempo, en el mismo fundamento jurídico se indica que el artículo 18.4 "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica reguladora del Tratamiento Automatizado de Datos de Carácter Personal- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios".

En suma, y atendiendo estrictamente a las circunstancias que concurren en el supuesto analizado, el Tribunal Constitucional consideró que la afiliación del trabajador recurrente a determinado Sindicato se facilitó por aquél con la única y exclusiva finalidad lícita de que la Empresa descontara de la retribución la cuota sindical y la transfiriera al Sindicato, de acuerdo con lo establecido en el art. 11.2 LOLS. Sin embargo, dice el Tribunal Constitucional, que "el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al período de huelga".

Se concluye así en la consideración de la conducta como inconstitucional, por cuanto se entiende que, como consecuencia de la utilización del dato para un fin distinto del que motiva su recogida, se presumió que por el simple hecho de pertenecer a uno de los Sindicatos convocantes de la huelga, se había participado en la misma, lo que se ratifica por el hecho de que tan sólo el 1 por 100 de los errores afectara a trabajadores afiliados a sindicatos no convocantes o sin militancia sindical conocida.

5.- ANÁLISIS DE LAS SENTENCIAS MÁS SIGNIFICATIVAS DICTADAS POR LOS ÓRGANOS DE LA JURISDICCIÓN CONTENCIOSO-ADMINISTRATIVA DURANTE 1999 EN SU FUNCIÓN FISCALIZADORA DE LA ACTIVIDAD DE LA AGENCIA DE PROTECCIÓN DE DATOS

Toda vez que a resoluciones del Director de la Agencia de Protección de Datos ponen fin a la vía administrativa (art. 109 Ley 30/1992), las mismas, al margen del recurso potestativo de reposición (art. 116 Ley 30/1992), sólo son impugnables en vía contencioso-administrativa (art. 48.2 LORTAD). En este orden jurisdiccional, los órganos fiscaliza-

dores competentes durante 1999 han sido las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia (art. 74 Ley 6/1985, de 1 de julio, Orgánica del Poder Judicial), si bien este control variará a partir del próximo ejercicio pasando a ser ejercido por la Audiencia Nacional (art. 25 y disposición adicional cuarta de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa.

Pues bien, durante 1999 han recaído 29 sentencias de los Tribunales Superiores de Justicia en virtud de recursos contencioso-administrativos interpuestos contra resoluciones de la APD, lo que supone un notable incremento respecto de las sentencias (13) dictadas por esos mismos órganos jurisdiccionales en el ejercicio anterior como lógica consecuencia de la mayor actividad de la Agencia al haber aumentado el número de resoluciones dictadas por ésta.

De las 29 sentencias recaídas en el presente año, 27 se corresponden con procedimientos sancionadores y 2 con procedimientos de tutelas de derechos. Del total de aquéllas, 19 han sido confirmatorias de los criterios mantenidos por la APD en sus resoluciones, desestimando, en consecuencia, el recurso contencioso-administrativo interpuesto y en 10 de ellas se ha revocado o anulado la resolución de la Agencia, estimando total o parcialmente el recurso interpuesto. Significa ello que los criterios sostenidos por la Agencia a la hora de interpretar y aplicar la LORTAD han sido mayoritariamente correctos y ajustados a Derecho en cuanto que, de las 10 citadas sentencias revocatorias, la mitad de ellas afecta a un mismo tema o cuestión respecto del cual ni siguiera la propia Jurisdicción mantiene un criterio uniforme como tendremos ocasión de exponer.

Del total de sentencias recaídas, atendiendo a una distribución por sectores, se desprende la siguiente estadística:

Solvencia patrimonial y crédito	12
Publicidad directa	5
Entidades financieras	8
Otras	4

De entre las sentencias recaídas, y atendiendo al objeto o razón de la impugnación, cabe destacar las que afectan a aquellos criterios mantenidos por la Agencia y que han sido más discutidos por los recurrentes, y que, sin embargo, han sido confirmados por los Tribunales de lo contencioso-administrativo; sin perjuicio de aludir también a las que se refieren a criterios más discutibles sostenidos por la Agencia y que los Tribunales han revocado.

5.1 SENTENCIAS CONFIRMATORIAS DE LA POSICIÓN Y CRITERIOS DE LA AGENCIA

* La Sentencia nº 989 del Tribunal Superior de Justicia de Madrid, Sección novena, de 29 de septiembre de 1999, confirma como falta leve la ausencia de notificación del art. 28.1 de la LORTAD.

* La Sentencia nº 684 del Tribunal Superior de Justicia de Madrid, Sección Novena, de 22 de junio de 1999, relativa a la notificación prevista en el art. 28.1 de la Ley 5/1992 e Instrucción 1/1995, establece la obligación del responsable del fichero de notificar al afectado tantas veces cuantas haya incluido en su fichero incidencias sobre datos personales de aquél, y no sólo una vez; es decir, se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o distintos acreedores, informando al afectado de la totalidad de los datos incluidos en el fichero y no sólo el primero.

* La Sentencia nº 405 del Tribunal Superior de Justicia de Madrid, Sección 8ª, de 23 de junio de 1999, entre otras, confirma la obligación del responsable del fichero de cancelar cautelarmente el dato ó, en su caso, informar motivadamente de las razones del mantenimiento del registro, en el plazo de cinco días, desde que recibió el escrito de la afectada.

* La Sentencia del Tribunal Superior de Justicia de Madrid, Sección 8ª, de 21 de julio de 1999, confirma la procedencia de sanción grave por mantenimiento de datos no actualizados. Así mismo establece la obligatoriedad del responsable del fichero de realizar frecuentes "barridas" a fin de evitar la continuación de la inclusión de datos inexactos en el fichero, en virtud de la *"culpa in vigilando".*

* La Sentencia nº 526 del Tribunal Superior de Justicia de Madrid, Sección 8ª, de 15 de septiembre de 1999, entre otras, confirma el criterio de la APD de que el censo electoral no puede ser considerado como fuente accesible al público a tenor de lo dispuesto en la Ley 5/1985, de Régimen Electoral General. Ya en la Memoria de 1998 se explicita pormenorizadamente la confirmación por los Tribunales de que los datos obtenidos del censo electoral y del padrón municipal no son fuentes accesibles al público, a tenor de lo dispuesto en la citada Ley y en la Ley 7/1985, Reguladora de las Bases de Régimen Local.

* Sentencia 1234, de Tribunal Superior de Justicia de Madrid, Sección 9ª, de 9 de noviembre de 1999, confirmando el criterio sostenido por la Agencia de que las actuaciones de inspección son actuaciones previas, anteriores e independientes del procedimiento sancionador propiamente dicho, que se encuadran claramente en la potestad de inspección conferida a la APD por el art. 39 de la LORTAD, no computándose el tiempo transcurrido en su realización en el cómputo del plazo de seis meses de caducidad del procedimiento por inactividad de la Administración. Dicho en otros términos, el plazo de caducidad del procedimiento sancionador comienza a correr desde del momento en que se dicta

el acuerdo de incoación del procedimiento y no desde que se iniciaron las actuaciones previas de inspección.

5.2 ANÁLISIS DE LAS SENTENCIAS ANULATORIAS DE LA RESOLUCIONES DE LA APD.

Del total de las 10 sentencias estimatorias de los recursos interpuestos y que, en consecuencia, han revocado o anulado, total o parcialmente, las resoluciones de la APD, 5 de ellas se refieren y afectan a un mismo tema o cuestión relativo a si la obligación impuesta al responsable del fichero por el art. 28.1 *in fine* de la LORTAD, de notificar al afectado su inclusión en un fichero, afecta a las dos clases de ficheros que regula dicho artículo (ficheros comerciales de evaluación de solvencia patrimonial y crédito y ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias o ficheros de morosos), o, por el contrario, únicamente afecta y obliga respecto de la segunda clase de ficheros citados.

El criterio mantenido por la APD a este respecto es el de que la carga de notificar es obligatoria para los responsables de ambos tipos de ficheros por las siguientes razones:

a) En primer lugar, tanto del análisis sistemático y gramatical del art. 28.1 de la LORTAD, como desde el punto de vista de los antecedentes legislativos de la misma, cabe llegar a la conclusión de la que la notificación requerida por dicho artículo es predicable de todos los supuestos recogidos en el mismo, esto es, tanto para los ficheros de evaluación de solvencia patrimonial como para los ficheros de morosos.

En efecto, el título que encabeza el artículo 28 lleva la rúbrica "*Prestación de servicios de información sobre solvencia patrimonial y crédito".* Parece, pues, que el legislador anuncia un régimen legal con un criterio de unidad sistemática, sin que los ficheros de morosos (lo relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor, en la terminología legal) aparezcan con autonomía conceptual propia en la literalidad de la norma legal. En definitiva, con la rúbrica del artículo 28 parece que el legislador quiere seguir un criterio integrador que unificará todos los ficheros del art. 28, a efectos de la exigencia de notificación al afectado.

Asimismo, desde el punto de vista gramatical, el signo de puntuación "punto y aparte" se emplea para indicar que se ha terminado de expresar una idea completa (o un aspecto de una idea), de manera que lo que precede forma un sentido completo y lo que sigue va a constituir una exposición aparte. Quiere ello decir, en buena técnica legislativa, que al estar comprendidos los dos tipos de ficheros en un mismo párrafo, la exigencia de notificación afecta por igual a todos los supuestos allí contemplados. Además, de entender el legislador que la notificación al afectado sólo es preceptiva en el caso de los ficheros de morosos, habría empleado el singular "en este caso" y no el plural "en estos casos", más bien expresivo de la preceptividad de la notificación a todos lo supuestos contemplados en el punto 1 de tan citado artículo 28.

b) En segundo término, de los debates parlamentarios que precedieron a la aprobación de la LORTAD se desprende que la intención del legislador era que la notificación fuera preceptiva para todos los supuestos del art. 28.1, toda vez que fue rechazada la enmienda número 262 del Grupo Parlamentario Popular en el Congreso que proponía una adición al art. 28.1 de la Ley, facultando a la Agencia de Protección de Datos a que dispensara de la notificación cuando ésta resultara imposible o exigiera esfuerzos desproporcionados, y tal dispensa afectaba a todo el apartado anterior, es decir, a las dos clases de ficheros que tienen cabida en el apartado 1 del repetido art. 28.

c) Por último, y no por ello de menor importancia, debe entenderse que del art. 28.1 de la LORTAD se deriva un deber de notificación al afectado, exigible, además, en el plazo de 30 días a partir del registro en el fichero correspondiente, y si bien los ficheros de solvencia patrimonial no exigen para su formación el consentimiento del afectado cuando provienen de fuentes accesibles al público (art. 6.2 LORTAD), sí obligan a una notificación del afectado a fin de que éste pueda ejercer "*su derecho a recabar información"* (art. 28.1 in fine). Así entendido, el deber legal de notificación adquiere un significado instrumental para hacer valer (y sin el cual no se podrían hacer valer) los derechos de información, acceso, rectificación y cancelación recogidos en los artículo 13 14 y 15 de la LORTAD. Dicho en otros términos, la "plenitud" para el ejercicio de los derechos del afectado no estaría suficientemente garantizada frente a los sistemas electrónicos de almacenamiento masivo de información si no se exigiera tal deber de notificación, con lo que el derecho fundamental a la intimidad, tal y como aparece recogido en el art. 18 de la Constitución, quedaría vaciado de contenido.

Ciertamente, los criterios mantenidos por los Tribunales de lo contencioso no siempre han coincidido con los sostenidos por la Agencia sobre este tema, si bien tampoco entre aquéllos se ha mantenido siempre la misma unidad de criterios. Así, pueden destacarse tres tipos de criterios diferentes, según la Sección que conociera el asunto:

1- Criterio mantenido con carácter general por la Sección 8ª del Tribunal Superior de Justicia de Madrid, que establece la no obligatoriedad del responsable del fichero de notificar al afectado su inclusión en un fichero de solvencia patrimonial y crédito cuando sus datos han sido obtenidos de fuentes accesibles al público o proceden de informaciones facilitadas por el afectado ó con su consentimiento (Sentencias nº 480 de 21 de julio de 1999 y nº 572 de 29 de septiembre de 1999).

2- Posición mantenida por la Sección Novena del mismo Tribunal, que destaca que la obligación de notificar la inclusión en un fichero sobre solvencia, aun cuando se trate de datos provenientes de fuentes accesibles al público, constituye una obligación legal, por imponerlo así el art. 28 de la Ley Orgánica 5/1992. Según el Tribunal, de acuerdo con la Ley, hay que notificar a los afectados una relación de los datos de carácter personal que se hubieren incluido en los ficheros automatizados, tanto si los ficheros son de prestación de servicios sobre solvencia patrimonial y crédito, como si son relativos al cumplimiento o incumplimiento de obligaciones dinerarias (Sentencias nº 689 de 22 de junio de 1999).

3- Posición mantenida por la Sección Octava del citado Tribunal Superior de Justicia de Madrid, en su sentencia de 26 de mayo de 1999, que si bien excluye de notificación los supuestos del art. 28.1 (ficheros de solvencia patrimonial y crédito) cuando los datos se hayan obtenido de fuentes accesibles al público o cuando provengan de informaciones suministradas por el afectado o con su consentimiento, de hecho y en la práctica, el cumplimiento de la obligación impuesta en el art. 4.3 "*datos exactos y puestos al día"*, (principio de veracidad), implica la obligación de notificar al afectado el registro de sus datos cualesquiera que sea la fuente de la que se obtengan.

Esta disparidad de criterios sobre una misma cuestión mantenida por las distintas Secciones de un mismo Tribunal, demuestra lo controvertido de la misma y justifica por sí sola el criterio sostenido por la APD.

Por último, las restantes Sentencias estimatorias de los recursos planteados se refieren a los siguientes temas:

* Sentencia nº 680 del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-Administrativo, de 16 de junio de 1999, sobre el derecho de "Rectificación y Cancelación", que interpreta que el responsable del fichero común no tiene competencia para rectificar o cancelar los datos inexactos que constan en el fichero, precisamente por no ser el acreedor.

* Sentencia nº 331 del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-Administrativo, Sección 8ª, de 26 de mayo de 1999 que considera que el registro de datos no correspondiente a la realidad, cuando los datos provienen de fuentes accesibles al público y existe constancia de que titular del fichero no tiene conocimiento de la inexactitud del dato inscrito y no se da una actitud obstruccionista o negativa por su parte, no es tipificable como infracción grave (art. 43.3 f) de la LORTAD) sino como leve "*mero incumplimiento de las obligaciones previstas en el artículo 4.3 y 4 en relación con el art. 43.2 c)".*

* Sentencia nº 862 del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-Administrativo, Sección 8ª, de 15 de diciembre de 1999, establece que las obligaciones del art. 29.2 de la LORTAD "*ficheros con fines de publicidad"* corresponden al responsable del fichero sin que en ningún modo se imponga ningún tipo de obligación a las empresas que contraten los servicios de los titulares del los ficheros automatizados de datos de carácter personal. El beneficiario de la publicidad no es responsable del fichero, al cual la Ley impone las obligaciones de rectificar y cancelar.

* Sentencia nº 1087 del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-Administrativo, Sección 9ª, de 21 de octubre de 1999 que determina al estimar el recurso que el juego de etiquetas identificativas no puede considerarse un fichero automatizado en el sentido a que se refiere la LORTAD.

MEMORIA DE 1999 - OTRAS ACTIVIDADES

1. TERCERA EDICIÓN DEL PREMIO PROTECCIÓN DE DATOS PERSONALES

Se ha convocado la **TERCERA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES",** con una dotación de un millón de pesetas, y un accésit dotado de 250.000 pesetas, con la finalidad de profundizar en el estudio del desarro - llo del artículo 18.4 de la Constitución.

El Jurado establecido en las Bases de la convocatoria otorgó el Premio a la obra " Protección de los datos de carácter personal relativos a la salud" presentada por la Doctora en Medicina Dª Carmen Sánchez Carazo y el Licenciado en Derecho D. Juan Mª Sánchez Carazo.

La obra premiada aborda las siguientes materias:

* INTRODUCCIÓN

* 1. APROXIMACIÓN HISTÓRICA A LA INTIMIDAD
* 1.1.- Introducción
* 1.2.- La intimidad en la antigüedad
* 1.3.- La intimidad en la modernidad
* 1.4.- Nuevo concepto de intimidad

* 2. PRECISIÓN NOCIONAL DE LOS TÉRMINOS INTIMIDAD, CONFIDENCIALIDAD Y PRIVACIDAD
* 2.1.- Intimidad
* 2.2.- Confidencialidad
* 2.3.- Privacidad
* 2.4.- Diferencias y similitudes

* 3. EL DERECHO A LA INTIMIDAD
* 3.1.- Introducción
* 3.2.- Aspectos éticos
* 3.2.1.- La bioética de la confidencialidad
* 3.3.- Aspectos legales
* 3.3.1.- La intimidad antes de la Constitución de 1978
* 3.3.2.- El derecho a la intimidad alcanza la mayoría de edad
* 3.4.- Conflicto entre el derecho a la intimidad y el derecho a la información: la confidencialidad.

* 4. DATOS ESPECIALMENTE PROTEGIDOS
* 4.1.- Protección de datos: nacimiento y desarrollo
* 4.2.- Datos especialmente protegidos
* 4.3.- Datos especialmente protegidos y el Consejo de Europa
* 4.3.1.- Nacimiento de la protección de datos
* 4.3.2.- Resolución (73) 22 y Recomendación (74) 29 del Consejo de Europa
* 4.3.3.- La Recomendación de la OCDE
* 4.3.4.- Estados Unidos y la protección de datos
* 4.3.5.- La protección de datos en los diferentes estados que componen la Unión
* 4.3.6.- El Consejo de Europa y los datos sanitarios

* 5. EL SECRETO MÉDICO
* 5.1.- La huella hipocrática
* 5.2.- El secreto
* 5.3.- El secreto médico
* 5.3.1.- La legislación civil
* 5.3.2.- La legislación penal
* 5.3.3.- Los Códigos Deontológicos
* 5.3.4.- Un secreto en conflicto

* 6. PROTECCIÓN DE DATOS SANITARIOS 1: ASPECTOS GENERALES
* 6.1.- Introducción
* 6.2.- Datos de carácter personal relativos a la salud
* 6.2.1.- Datos de carácter personal
* 6.2.2.- Datos de salud
* 6.3.- El tratamiento de los datos sanitarios
* 6.3.1.- El artículo 8 de la Ley 5/92
* 6.4.- La historia clínica
* 6.5.- El consentimiento informado
* 6.5.1.- La información y el tratamiento de los datos sanitarios
* 6.5.2.- El consentimiento
* 6.6.- El derecho de acceso a los datos sanitarios

* 6.6.1- Defensa del derecho de acceso por la Agencia de Protección de Datos
* 6.7.- El derecho de rectificación y cancelación de los datos sanitarios
* 6.8.- Cesión de datos sanitarios
* 6.8.1.- Transferencias internacionales
* 6.9.- La seguridad y los datos sanitarios
* 6.10.- Retos tecnológicos

* 7. PROTECCIÓN DE DATOS SANITARIOS II: CASOS PARTICULARES
* 7.1.- Introducción
* 7.2.- Atención primaria y la intimidad
* 7.3.- Salud laboral y protección de datos
* 7.4.- Investigación médica y protección de datos
* 7.4.1.- El Convenio de Oviedo
* 7.5.- La confidencialidad y la salud mental
* 7.6.- Enfermedades infecciosas y confidencialidad
* 7.7.- La confidencialidad de los datos genéticos

* 8. CONCLUSIONES

* BIBLIOGRAFíA

Se concedió un áccesit, dotado con 250.000 pesetas, a la obra titulada "El Derecho a la autodeterminación informativa. Marco constitucional y europeo", de la que es autora Dª Juana Marí Cardona, Profesora de la Universidad de Barcelona . Se trata de un estudio de interés general de la legislación en materia de protección de datos, que recopila la información existente. Entre los principales temas que aborda cabe destacar el estudio de la configuración constitucional del derecho a la autodeterminación informativa, su desarrollo normativo, las referencias a la Agencia de Protección de Datos o el flujo transfronterizo de datos de carácter personal.

2. PARTICIPACION DEL DIRECTOR DE LA AGENCIA EN CONFERENCIAS, SEMINARIOS Y JORNADAS Y REUNIONES INSTITUCIONALES.

El Director de la Agencia de Protección de Datos, en su comparecencia ante la Comisión Constitucional del Congreso de los Diputados celebrada en el año 1998 puso de manifiesto, como una de sus prioridades, la necesidad de dar a conocer la normativa reguladora de la protección de datos personales.

En coherencia con dicha prioridad, durante el año 1999, se han multiplicado los foros en los que la Agencia ha participado para aproximar el conocimiento de la norma a los sectores afectados y resolver "in situ" las dudas que se les suscitan.

El abanico de entidades respecto de las que se han producido tales intervenciones se ha ampliado incluyendo a grupos de comunicación, entidades académicas, públicas y privadas, asociaciones, fundaciones, institutos especializados, federaciones empresariales, Consejos Generales de Colegios Profesionales y Administraciones Públicas.

El temario de cuestiones abordadas es, asimismo, extenso y completo, incluyendo tanto cuestiones generales como las relativas a los principios de la LORTAD, a la transposición de la Directiva 95/46/CE y a la nueva Ley Orgánica 15/1999, de 13 de diciembre, como debates especializados acerca de la actividad de "marketing", el sector farmacéutico, la protección de incapacitados o las cesiones de datos a efectos estadísticos.

Las intervenciones del Director han contemplado, también, fenómenos novedosos que van alcanzando rápidamente un gran desarrollo, como son los relativos a Internet, al comercio electrónico y a la firma electrónica.

Junto a ellos ha sido preciso informar y debatir respecto de las cuestiones contempladas en la normativa de protección de datos que han alcanzado mayor notoriedad, bien por exigencias de los operadores económicos, bien por la aprobación de desarrollos reglamentarios pendientes. Entre las primeras destacan los debates relacionados con las transferencias internacionales de datos, que van alcanzando un volumen creciente en el mundo de una economía globalizada. De los segundos ocupa un papel muy relevante la participación en jornadas sobre el Reglamento de Medidas de Seguridad en materia de Protección de Datos, aprobado por Real Decreto 924/1999, de 11 de junio, que ha afectado de forma relevante al conjunto de los responsables de ficheros impulsando el conocimiento por parte de operadores públicos y privados de la normativa de protección de datos, ante la necesidad de adecuarse al mismo.

También han sido objeto de intervenciones del Director de la Agencia la protección de datos en relación con otras instituciones como la Fiscalía y las Autoridades Autonómicas de Protección de Datos.

En este último aspecto debe hacerse mención específica a las relaciones mantenidas con la Agencia de Protección de Datos de la Comunidad de Madrid, única autoridad de carácter autonómico existente en el período que abarca la presente Memoria.

La Agencia autonómica ha desarrollado una intensa actividad en la que destaca la imprescindible función informativa y pedagógica sobre la normativa de protección de datos.

Fruto de la colaboración entre ambas entidades ha sido, no sólo un permanente intercambio de información, sino también la participación directa en los foros públicos organizados por la autoridad autonómica de protección de datos.

En otro ámbito de relaciones institucionales adquieren especial relevancia las tenidas con el Defensor del Pueblo. La Ley Orgánica 5/1992 prevé una relación específica con dicha Institución dado que la Agencia debe notificarle las resoluciones de procedimientos que afecten a las Administraciones Públicas. Sin embargo, las relaciones entre ambas han ido más allá de la previsión legal con el fin de mantener una estrecha relación entre Instituciones cuyas competencias protegen, en sus respectivos ámbitos, derechos de los ciudadanos. Así, el Director de la Agencia se dirigió al Defensor del Pueblo para hacerle entrega personal de la Memoria del año 1998 y propiciar un intercambio directo de opiniones sobre las actividades de ambas Instituciones. Por otro lado, la Agencia ha respondido a los requerimientos específicos de información que le han sido remitidos por el Defensor del Pueblo.

El conocimiento de los problemas relacionados con la LORTAD ha sido, asimismo, desarrollado a través de reuniones de trabajo celebradas a instancia de sectores afectados como despachos profesionales, empresas y asociaciones empresariales, administraciones públicas, representaciones diplomáticas, magistrados y fiscales, universidades, asociaciones de consumidores y usuarios, colegios profesionales y federaciones deportivas.

Las actividades dirigidas a la proyección de la normativa de protección de datos ha tenido, finalmente, dos hitos relevantes.

En primer lugar, la presentación pública de las ponencias de la XX Conferencia Internacional de Autoridades de Protección de Datos, organizada por la Agencia en septiembre de 1998, en Santiago de Compostela, que tuvo lugar en el Ilustre Colegio de Abogados de Madrid con participación del Director de la Agencia y el Decano del Colegio, así como de dos relevantes parlamentarios que participaron como Ponentes en la tramitación del proyecto de Ley de Protección de Datos de Carácter Personal.

En segundo lugar, la presentación de la Memoria anual de 1998 que se celebró el 22 de julio en la sede del Consejo Superior de Cámaras de Comercio, Industria y Navegación, interviniendo el Director de la Agencia y el Presidente del Consejo. La celebración del acto en dicha sede tuvo como finalidad aproximar el conocimiento directo de la actividad de la Agencia entre las empresas como titulares de un importante número de ficheros.

FECHA	LUGAR	ACTIVIDAD
ENERO		
28/1/99	MADRID	I Jornadas de Protección de Datos de la Comunidad de Madrid. Título Ponencia: **"Los Datos especialmente protegidos".**
MARZO		
1/3/99	MADRID	Curso especializado de Derecho Informático y de las Telecomunicaciones, organizado por el Grupo Recoletos. Título Ponencia**: "El Derecho de los contenidos. Protección de Datos"**
12/3/99	MADRID	Novedades Jurídicas del Comercio Electrónico, organizado por el Instituto de Empresa. Título Ponencia**: "La Protección de Datos Personales: Legislación actual"** **Vigencia de los principios de la LORTAD en el comercio electrónico.** **Aplicación de los principios que establecen las directivas (95)46 y (97)66** **Recomendaciones de las autoridades de control de los países de la UE.** **Códigos éticos.**
ABRIL		
6/4/99	MADRID	1er. Curso de "Iniciación al Derecho de la Publicidad", organizado por la Asociación de Autocontrol de la Publicidad. Título Ponencia**: "La Regulación del Marketing Directo. La oferta a distancia y la protección de datos personales".**
28/4/99	MADRID	Congreso "SECURMáTICA 99", organizado por la Revista Seguridad en Informática y Comunicaciones. Título Ponencia: **"La protección de Datos Personales. Impacto de la transposición de la Directiva de protección de datos personales 95/46/CE".**
28/4/99	MADRID	Presentación en el Ilustre Colegio de Abogados de Madrid del libro editado por la Agencia de Protección de Datos que contiene las Ponencias de la XX Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Santiago de Compostela en septiembre de 1998.
MAYO		
6/5/99	MADRID	"XIII Encuentro sobre Informática y Derecho", organizado por la Universidad Pontificia de Comillas. Título ponencia**: "Transferencia de datos personales a terceros países.** Mesa redonda: Excepciones al consentimiento en ficheros de titularidad privada".
18/5/99	MADRID	Jornada: Experiencias Jurídicas en Protección de Datos en el Sector Farmacéutico, organizada por la Fundación CEFI.
19/5/99	MADRID	Jornada "Protección de Datos y Consumidores", organizada por la Unión de Consumidores de España (UCE). Título Ponencia**: "El Papel de la Agencia de Protección de Datos"**
20/5/99	MADRID	Jornada sobre "Medidas Legales de Seguridad Informática",organizadas por el Institute for International Research España. Apertura de Honor.
25/5/99	MADRID	Jornada de "Marketing Directo y Comercio Electrónico", organizada por la Federación de Comercio Electrónico y Marketing Directo. **Participación en una mesa redonda titulada "La definición de la nueva LORTAD: Cambios en la aplicación de la Ley"**
JULIO		
1-2/7/99	MERIDA	Jornadas sobre "Privacidad, Comercio Electrónico e Internet" organizadas conjuntamente por la APD y la UNED **.** Tema: **"Flujo Internacional de Datos"**
7/7/99	MADRID	Curso "Criminalidad Informática e Internet", organizado por el Centro de Estudios Jurídicos. Tema Ponencia: "**El Papel de la APD en la protección de la intimidad; relaciones con el Ministerio Fiscal"**.
22/7/99	MADRID	Presentación en el Consejo Superior de Cámaras de Comercio, Industria y Navegación, de la Memoria de la Agencia de Protección de Datos de 1998.
AGOSTO		
24/8/99	SANTANDER	Curso de la Universidad Internacional Menéndez Pelayo, organizado por el Consejo General del Notariado. Título Ponencia: "**Medidas para la humanización del proceso de incapacitación y su seguimiento. La Protección de datos y el discapacitado".**

MEMORIA DE 1999 - ANEXO I - LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: que las Cortes generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente Ley Orgánica 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.

Artículo 2. Ámbito De Aplicación

1. La presente Ley Orgánica será de aplicación a 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 los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c) 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.
d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e) 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.

Artículo 3. Definiciones

A los efectos de la presente Ley Orgánica se entenderá por

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: 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.
d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado

c) del presente artículo.
f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: 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.
h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

TÍTULO II

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Artículo 4. Calidad De Los Datos

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5 . Derecho De Información En La Recogida De Datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

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

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e **)** del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el

tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento Del Afectado

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal 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 de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos Especialmente Protegidos

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos Relativos A La Salud

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad .

Artículo 9. Seguridad De Los Datos

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía

reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber De Secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso A Los Datos Por Cuenta De Terceros

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

DERECHOS DE LAS PERSONAS

Artículo 13. Impugnación De Valoraciones

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su

comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho De Consulta Al Registro General De Protección De Datos

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho De Acceso

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 16. Derecho De Rectificación Y Cancelación

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. 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.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación .
5. 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.

Artículo 17. Procedimiento De Oposición, Acceso, Rectificación O Cancelación

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.
2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela De Los Derechos

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.
2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del Organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho A Indemnización

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.
3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

DISPOSICIONES SECTORIALES

CAPÍTULO PRIMERO

Ficheros de titularidad pública

Artículo 20. Creación, Modificación O Supresión

1. La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación De Datos Entre Administraciones Públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2 b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros De Las Fuerzas Y Cuerpos De Seguridad

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.
4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.
A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones A Los Derechos De Acceso, Rectificación Y Cancelación

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones

inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras Excepciones A Los Derechos De Los Afectados

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.
2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación E Inscripción Registral

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.
En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.
5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. Comunicación De La Cesión De Datos

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por Ley.

Artículo 28. Datos Incluidos En Las Fuentes De Acceso Público

1. Los datos personales que figuren en el censo promocional o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3 j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.
2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.
Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.
La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.
En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.
4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. Prestación De Servicios De Información Sobre Solvencia Patrimonial Y Crédito

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el creedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
3. En los supuestos a que se refieren los dos apartados anteriores cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.
4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos.

Artículo 30. Tratamientos Con Fines De Publicidad Y De Prospección Comercial

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.
2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. Censo Promocional

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.
2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.
3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.
4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos Tipo

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.
En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen

las correcciones oportunas.

TÍTULO V

MOVIMIENTO INTERNACIONAL DE DATOS

Artículo 33. Norma General

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

AGENCIA DE PROTECCIÓN DE DATOS

Artículo 35. Naturaleza Y Régimen Jurídico.

1. La Agencia de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.
2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al Derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
En todo caso, el Director deberá oír al Consejo Consultivo en aquéllas propuestas que éste le realice en el ejercicio de sus funciones.
3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1 a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.
4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.
Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno.
Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades.
Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.
El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General De Protección De Datos

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos

a) Los ficheros de que sean titulares las Administraciones Públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción , su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad De Inspección

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos Correspondientes De Las Comunidades Autónomas

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.
2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.
3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros De Las Comunidades Autónomas En Materia De Su Exclusiva Competencia

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.
2. Si la Administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

INFRACCIONES Y SANCIONES

Artículo 43. Responsables

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias

que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.
b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
j) La obstrucción al ejercicio de la función inspectora.
k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.
b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
ºg) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.
2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.
3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la

escala relativa a la clase de infracciones que preceda inmediantamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones Públicas

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.
2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.
3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.
2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.
4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.
5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.
6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.
2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. Potestad de inmovilización de ficheros

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

DISPOSICIONES ADICIONALES

Primera. Ficheros preexistentes

Los ficheros y tratamientos automatizados, inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Segunda. Ficheros y Registro de Población de las Administraciones Públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al

Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.
2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones Públicas.

Tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido 50 años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

4. La cesión de aquellos datos de carácter personal, objeto de tratamiento que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones Públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.

Quinta . Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

DISPOSICIONES TRANSITORIAS

Primera. Tratamientos creados por Convenios Internacionales

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Segunda. Utilización del Censo Promocional

Reglamentariamente se desarrollarán los procedimientos de formación del Censo Promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del Censo Promocional.

Tercera. Subsistencia de normas preexistentes.

Hasta tanto se lleven a efecto las previsiones de la Disposición Final Primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

DISPOSICIÓN DEROGATORIA

Única

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

DISPOSICIONES FINALES

Primera. Habilitación para el desarrollo reglamentario

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Segunda. Preceptos con carácter de Ley Ordinaria

Los títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera, tienen el carácter de Ley Ordinaria.

Tercera. Entrada en vigor

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el Boletín Oficial del Estado.

MEMORIA DE 1999 - ANEXO II - 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.

PREÁMBULO

El artículo 18.4 de la Constitución española establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

La Ley Orgánica 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de carácter personal prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3, h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día ...

Dispongo:

Artículo único.- Aprobación del Reglamento.

Se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única.- Entrada en vigor.

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

ELÉVESE AL CONSEJO DE MINISTROS
Madrid,
LA MINISTRA DE JUSTICIA,

Margarita Mariscal de Gante y Mirón.

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

CAPÍTULO I.- DISPOSICIONES GENERALES

Artículo 1.- Ámbito de aplicación y fines.

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

Artículo 2.- Definiciones.

A efectos de este Reglamento, se entenderá por:

1.- **Sistema de información:** Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

2.- **Usuario**: Sujeto o proceso autorizado para acceder a datos o recursos.

3.- **Recurso**: Cualquier parte componente de un sistema de información.

4.- Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

5.- **Identificación**: Procedimiento de reconocimiento de la identidad de un usuario.

6.- **Autenticación**: Procedimiento de comprobación de la identidad de un usuario.

7.- **Control del acceso**: Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.

8.- **Contraseña**: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

9.- **Incidencia**: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

10.- **Soporte**: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

11.- **Responsable de seguridad**: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

12.- **Copia de respaldo:** Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación **.**

Artículo 3.- Niveles de seguridad.

1.- Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2.- Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4.- Aplicación de los niveles de seguridad.

1.- Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2.- Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el articulo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3.- Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

4.- Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

5.- Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5.- Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6.- Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7.- Ficheros temporales.

1.- Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

2.- Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II.- MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 8.- Documento de seguridad.

1.- El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

2.- El documento deberá contener, como mínimo, los siguientes aspectos:

a.- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b.- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c.- Funciones y obligaciones del personal.
d.- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e.- Procedimiento de notificación, gestión y respuesta ante las incidencias.
f.- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3.- El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4.- El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9.- Funciones y obligaciones del personal.

1.- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c)

2.- El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 10.- Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Artículo 11.- Identificación y autenticación.

1.- El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan **acceso autorizado** al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2.- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3.- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12.- Control de acceso.

1.- Los usuarios tendrán **acceso autorizado** únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2.- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3.- La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá **el acceso autorizado** para cada uno de ellos.

4.- Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular **el acceso autorizado** sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13.- Gestión de soportes.

1.- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2.- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada, por el responsable del fichero.

Artículo 14. - Copias de respaldo y recuperación.

1.- El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2.- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3.- Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III.- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15.- Documento de seguridad.

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del **responsable o responsables** de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16.- Responsable de seguridad.

El responsable del fichero designará **uno o varios responsables de seguridad encargados** de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17.- Auditoría.

1.- Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2.- El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3.- Los informes de auditoría serán analizados por el responsable de seguridad **competente,** que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18.- Identificación y autenticación.

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19.- Control de acceso físico.

Exclusivamente el personal autorizado en el documento **de seguridad** podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20.- Gestión de soportes.

1.- Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirecta-

mente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2.- Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3.- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4.- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21.- Registro de incidencias.

1.- En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y , en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2.- Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22.- Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

CAPÍTULO IV.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 23.- Distribución de soportes.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24.- Registro de accesos.

1.- De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2.- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3.- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4.- El período mínimo de conservación de los datos registrados será de dos años.

5.- El responsable de seguridad **competente** se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25.- Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26.- Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO V.- INFRACCIONES Y SANCIONES.

Artículo 27.- Infracciones y sanciones.

1.- El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.

El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

2.- Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

Artículo 28.- Responsables.

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI.- COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

Artículo 29.- Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1.- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

2.- Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única.- Plazos de implantación de las medidas.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, **las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.**

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

MEMORIA DE 1999 - ANEXO III - INFORMES PRECEPTIVOS EVALUADOS POR LA AGENCIA DE PROTECCIÓN DE DATOS

Proyecto de Disposición	Solicitado por	Fecha informe
Informe sobre el Proyecto de Real Decreto por el que se desarrolla el artículo 81 de la Ley 66/1997, de Medidas Fiscales, Administrativas y del Orden Social, en materia de servicios de seguridad en las comunicaciones de la Administración a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT)	Subsecretaría Ministerio de Economía y Hacienda	15/01/99
Informe sobre el Proyecto de Real Decreto por el que se crea la Comisión para el análisis y prevención del fraude en los sectores agroalimentario y pesquero.	Secretario General Técnico del Ministerio de Justicia	18/01/99
Informe sobre el Anteproyecto de Ley sobre medidas de control de sustancias químicas susceptibles de desvío para la fabricación de armas químicas en aplicación de la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas hecha en París de 13 de enero de 1993.	Secretario General Técnico del Ministerio de Justicia	27/01/99
Informe sobre el Proyecto de Real Decreto por el que se modifica el Real Decreto 426/1980, de 22 de febrero, en desarrollo de la Ley 30/1979, sobre extracción y trasplante de órganos	Secretario General Técnico del Ministerio de Justicia	03/02/99
Informe sobre Proyecto de Orden sobre cesión de información tributaria a las Administraciones Públicas.	Subsecretaría de Economía y Hacienda	03/02/99
Informe sobre el Proyecto de Encuesta de Deficiencias, Discapacidades y Estados de Salud.	Director de Estadísticas de Población e Información INE	04/02/99
Informe acerca de una Propuesta de Directiva sobre Comercio Electrónico de la Comisión Europea.	Secretario General Técnico del Ministerio de Justicia	11/02/99
Informe sobre el Proyecto de Orden por el que se crea y regula el índice Nacional de Defunciones.	Director General de Salud PúblicaMinisterio de Sanidad y Consumo	19/02/99
Informe sobre el Real Decreto por el que se regula la expedición de la Tarjeta Nacional de Investigador para la consulta de los archivos de titularidad estatal y adheridos al sistema archivístico español.	Subsecretaría de Educación y Cultura	22/03/99
Informe sobre el proyecto de convenio entre el Ayuntamiento de Madrid y el Decanato de los Juzgados madrileños.	Ayuntamiento de MadridConcejal Delegado del área de Régimen Interior y Personal	22/03/99
Informe sobre el proyecto de Orden por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del impuesto sobre la Renta de las personas físicas	Subsecretaría de Economía y Hacienda(Por teléfono Directora del Departamento de Gestión Tributaria de la AEAT)	29/03/99
Informe relativo al Real Decreto por el que se establecen las condiciones de autorización y Registro para la importación de determinados productos del sector de la alimentación animal procedentes de países terceros, y por el que se modifica el Real Decreto 1191/1998, de 12 de junio, sobre autorización y registro de establecimientos e intermediarios del sector de la alimentación animal.	Secretario General TécnicoMinisterio de Justicia	05/04/99
Informe sobre el Proyecto de Orden Ministerial por la que se crea y regula el índice Nacional de Defunciones.	Director de Salud Pública	17/05/99
Informe referente al Proyecto de Real Decreto por el que se establecen criterios de imagen institucional y se regula la producción documental y el material impreso de la Administración del Estado.	Secretario General TécnicoMinisterio de Justicia(MAP)	01/06/99
Informe referido a la propuesta de norma con rango de Ley para la actualización de la regulación de la Central de Información de Riesgos del Banco de España (CIRBE).	Director General del BANCO DE ESPAÑA	15/06/99
Informe referente al Proyecto de Orden Ministerial por la que se regula la remisión de información sobre subvenciones y ayudas públicas, para la creación de una base de datos nacional, en desarrollo de lo dispuesto en el artículo 46 del Real Decreto 2188/1995.	Interventor General IGAEMº de Economía	16/06/99
Informe referido al Anteproyecto de Ley de Creación de la Agencia Catalana de Protección de Datos.	Generalitat de CataluñaDirección General de Informática	28/06/99
Informe sobre el Proyecto de Orden Ministerial por la que se	Secretaría General de la	30/06/99

MEMORIA DE 1999 - ANEXO IV - COMPARECENCIA DEL DIRECTOR DE LA AGENCIA EN EL CONGRESO DE LOS DIPITADOS

CORTES GENERALES
DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS
COMISIONES
Año 1999 VI Legislatura Núm. 825

CONSTITUCIONAL
PRESIDENCIA DEL EXCMO. SR. D. GABRIEL CISNEROS LABORDA
Sesión núm. 27
celebrada el martes, 21 de diciembre de 1999
ORDEN DEL DÍA:

Comparecencia del señor director de la Agencia de Protección de Datos (Fernández López) para informar sobre:

- La memoria de la Agencia de Protección de Datos correspondiente al año 1998. Apetición propia. (Número de expediente 212/002115.) ... (Página 24542)

- Su criterio sobre si los datos exigibles para determinar el cálculo del tipo de retención aplicable sobre los rendimientos del trabajo respeta el derecho a la intimidad de los afectados. A solicitud del Grupo Parlamentario Federal de Izquierda Unida. (Número de expediente 212/001869.) ... (Página 24556)

- Contenido del dictamen emitido el 23 de diciembre en relación al modelo oficial «IRPF, Retenciones del trabajo personal. Comunicación de datos al pagador». Asolicitud del Grupo Socialista del Congreso. (Número de expediente 212/001872.) ... (Página 24556)

- Informar, a la vista de lo sucedido con la Generalidad Valenciana en la preparación de una fiesta de la tercera edad, de las medidas y actuaciones que va a adoptar encaminadas a garantizar el cumplimiento por las Administraciones públicas de los preceptos de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal (Lortad). A solicitud del Grupo Parlamentario Mixto. (Número de expediente 212/001901) ... (Página 24560)

- Actuaciones realizadas por la Agencia para esclarecer la presunta utilización de datos de origen desconocido en la llamada «Gran fiesta de la tercera edad», organizada por la Consejería de Bienestar Social de la Generalidad Valenciana, así como su entrega a una empresa privada. A solicitud del Grupo Socialista del Congreso. (Número de expediente 212/001911.) ... (Página 24560)

- Actuación de la Agencia en defensa de los derechos de los ciudadanos afectados por su inclusión ilegítima en los llamados «ficheros de morosos», así como de las reformas legislativas necesarias para su mayor eficacia en este ámbito. A solicitud del Grupo Parlamentario Mixto. (Número de expediente 212/001910.) ... (Página 24566)

- Medidas que pudieran adoptarse para prevenir la cesión ilícita de datos personales archivados por las Administraciones públicas. A solicitud del Grupo Socialista del Congreso. (Número de expediente 212/001933.) ... (Página 24566)

- Adecuación de las medidas adoptadas por el ministro de Sanidad y Consumo a la ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (Lortad). Asolicitud del Grupo anterior. (Número de expediente 212/002141.) ... (Página 24566)

- Valoración de la Agencia acerca de la cesión de historiales clínicos de los centros del Insalud a empresas privadas. A solicitud del Grupo Parlamentario Mixto. (Número de expediente 212/002403.) ... (Página 24566)

Se abre la sesión a las cinco y cinco minutos de la tarde.

COMPARECENCIA DEL SEÑOR DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (FERNÁNDEZ LÓPEZ) PARA INFORMAR SOBRE:

- LA MEMORIA DE LA AGENCIA DE PROTECCIÓN DE DATOS CORRESPONDIENTE AL AÑO 1998. A PETICIÓN PROPIA. (Número de expediente 212/002115.)

El señor PRESIDENTE: Buenas tardes, señoras y señores diputados. Esta Comisión Constitucional se reúne para celebrar su sesión número veintisiete correspondiente a la legislatura. Me encantaría poder anunciarles con alguna solemnidad que se trataba de la última y aprovechar para felicitarles las Pascuas -bueno, eso en todo caso-, pero no está descartada la eventualidad de que tengamos que celebrar una última reunión entre los días 24 y 31, a la vista de la evolución final de los trabajos de la subcomisión sobre el modelo público de Radiotelevisión Española. Esperemos que la hipótesis no se verifique.

La Comisión Constitucional quiere agradecer la presencia de don Juan Manuel Fernández López, director de la Agencia de Protección de Datos, y acogerle muy cordialmente. El señor Fernández López había solicitado esta comparecencia a efectos de informar sobre la memoria de la Agencia que tan dignamente preside correspondiente al ejercicio de 1998. Ese es el punto primero del orden del día y sobre él agruparemos un primer debate por parte de los portavo-

ces de los grupos parlamentario que quieran participar en él, tras la exposición del señor director de la Agencia. Después, y a la vista del asentimiento que me otorguen los señores portavoces, introduciremos respecto a los restantes ocho puntos del orden del día un criterio de agrupación bien sea temático, en razón de las tres materias sobre las que versan las iniciativas, bien según los grupos que las suscriben. En uno u otro caso, creo que eso nos permitirá aligerar el desarrollo de una sesión que se presume ardua, por lo que agradezco de antemano la colaboración del señor director, de SS.SS. y de los señores funcionarios de la Cámara que nos asisten.

Sin más, el señor Fernández López, don Juan Manuel, director de la Agencia de Protección de Datos, tiene la palabra.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor presidente.

Buenas tardes, señorías. Es para mí un honor y una satisfacción comparecer ante esta Comisión parlamentaria directamente vinculada con la tutela y desarrollo de los derechos fundamentales. Convocar a la Agencia de Protección de Datos demuestra la sensibilidad de SS.SS.

en cuanto a la protección de la intimidad de los ciudadanos y el reconocimiento de las funciones atribuidas a este ente público independiente que es la Agencia de Protección de Datos. El control parlamentario es una garantía más de esa independencia que exige la propia ley. Es por ello que a los pocos días de tomar posesión como director de la Agencia de Protección de Datos pedí comparecer voluntariamente para exponer mi plan de actuación, lo que se llevó a cabo el día 27 de mayo del año pasado, y al concluir la memoria nuevamente volví a solicitar comparecer para rendir cuentas del primer año de mi mandato y recibir de SS.SS. las sugerencias pertinentes que me permitan un mejor desempeño de mis funciones.

La memoria de 1998, la que tengo en la mano, es ya conocida por SS.SS., toda vez que cumpliendo la exigencia legal fue remitida en su día a las Cámaras. Siguiendo la estructura de la misma, que viene establecida por el estatuto de la Agencia, comentaré a continuación los puntos más relevantes que posteriormente podré aclarar o ampliar a preguntas de SS.SS. En primer lugar, he de referirme a la actuación de la Subdirección General de los Registros de Protección de Datos.

La gestión de todo tipo de movimientos referentes a la inscripción de ficheros ha sido significativamente fluida, ya que el tiempo medio de respuesta desde que una notificación tiene entrada en el registro hasta que se emite la correspondiente resolución de inscripción al responsable del fichero no supera los tres días de media. Dentro de las actividades propias del registro se ha tramitado la inscripción de 3.253 nuevos ficheros, se han modificado 5.704 inscripciones y se han suprimido 1.234. Todo ello supone que al 31 de diciembre de 1998 el número de ficheros inscritos en el registro general era de 232.028, de los cuales 28.890 correspondían a inscripciones de titularidad pública y 203.138 a inscripciones de titularidad privada.

Se han mantenido diversas reuniones con responsables de determinados sectores a fin de conseguir un cumplimiento de la ley y, como consecuencia, una inscripción de los ficheros. Se pueden resaltar por su interés las reuniones mantenidas con el Consejo General del Notariado y otros colectivos profesionales, como son los sectores de los seguros, de la banca y del marketing.

En cuanto a inscripción de ficheros públicos, con el objeto de concienciar a los responsables de los ficheros de las administraciones públicas a lo largo del año se han mantenido diversas reuniones y se han realizado requerimientos de inscripción.

En el área específica de los ficheros de la Administración local se ha instado al vocal del Consejo Consultivo de la Agencia de Protección de Datos para que traslade a la Federación Española de Municipios y Provincias la necesidad de todos de cumplir con la ley.

En cuanto a la publicación del catálogo de ficheros inscritos, que es una obligación que la ley determina para la Agencia de Protección de Datos, hemos de decir que para cumplir con este precepto se ha mantenido una actualización mensual del catálogo de ficheros en la página web de la Agencia, lo que permite completar las publicaciones que se vienen realizando tanto en soporte papel como en CD-Rom.

Asimismo se han publicado los modelos de declaración de ficheros en la página web de la Agencia, facilitando de esta forma la obtención de los impresos establecidos como modelos normalizados, obteniéndose una media cercana a 20.000 accesos mensuales a nuestra página web. El próximo año 2000 la Agencia espera estar en condiciones de facilitar incluso la inscripción a través de Internet. En cuanto a la inscripción de ficheros de datos especialmente protegidos, he de significar que en relación con los datos de la salud, de origen racial y vida sexual, enumerados por el artículo 7.3 de la ley, se observa un incremento en la declaración de ficheros que contienen este tipo de datos. Se han inscrito 202 ficheros que declaran datos de salud, correspondiendo una parte de los mismos a ficheros cuya finalidad es la gestión de recursos humanos de empresas que mantienen políticas de prevención de riesgos laborales y vigilancia de la salud de sus trabajadores. Hay que aclarar a este respecto que estos datos son siempre tratados por los servicios médicos de la empresa y nunca por el empresario, al menos en las declaraciones.

También incluyen datos de salud los ficheros de entidades del sector asegurador que ofrecen seguros de vida y salud o gestionan pólizas de asistencia sanitaria o decesos. La Agencia de Protección de Datos analiza especialmente las declaraciones que contienen datos de este tipo antes de proceder a su inscripción, aunque como SS.SS. saben esta inscripción es meramente declarativa.

Una actividad importante de la Agencia es la autorización de transferencias internacionales de datos. Hasta diciembre de 1998 se han resuelto 101 expedientes de solicitud de autorización de transferencias internacionales, autorizándose durante el año 1999 doce expedientes iniciados ya en el año 1998. Además, durante este año 1999 se han iniciado 38 expedientes, encontrándose todos ellos resueltos a la fecha de hoy, lo que ha supuesto 36 autorizaciones de transferencia internacional y el archivo de dos expedientes por desistimiento de los solicitantes. La mayor parte de ellas son con destino a los Estados Unidos de Norteamérica, excepto dos que lo han sido con destino a Filipinas y a Marruecos. Hay que aclarar, señorías, que por supuesto las autorizaciones dentro de la Unión Europea no son necesarias por el principio de libre circulación que establece la directiva y porque todos los países de la Unión Europea tienen tanto ley de protección de datos como autoridad de control, aunque también es bueno decir que no se realiza este control con el rigor con que lo hacemos los españoles. Todas las autorizaciones de transferencias internacionales están amparadas en el consentimiento informado de los afectados, a excepción de cuatro que están amparadas en una solución contractual. La primera vez que se ha utilizado la solución contractual en el contexto de la transferencia internacional ha sido a fines de 1998, concretamente en el expediente de transferencia internacional masiva de datos de la entidad Reader_s Digest. Las cláusulas que se han exigido en esta autorización, en los términos que posibilita la Directiva 95/46, son las siguientes. En primer lugar, la obligación de las partes de la transferencia a garantizar que aplican íntegramente el principio de protección de datos.

En segundo lugar, la delimitación de la finalidad del tratamiento, garantía de que los datos de carácter personal no podrán utilizarse para fines distintos de los especificados en el contrato y de que no pueden ser cedidos a terceros en el país de destino de la transferencia, ni siquiera para su conservación, siendo necesaria su destrucción o devolución al responsable una vez cumplida la prestación contractual. En tercer lugar, la exigencia del cumplimiento de medidas de seguridad conforme a lo dispuesto en el artículo 9 de nuestra ley. Una condición especialmente significativa es la impuesta sobre el control de la aplicación de la legislación de protección de datos, así como la de realizar auditorías por parte de la propia Agencia o por un auditor externo independiente designado por ésta, incluida la de realizar inspecciones en el país de destino.

Es decir, la Agencia española podrá realizar en el país de destino los datos e inspecciones bien directamente o a través de un auditor independiente que pueda garantizar el cumplimiento de la ley.

Seguidamente también se exige, en relación con la atribución al remitente de la responsabilidad por los incumplimientos de las garantías legales, el que se responsabilice a la entidad que realice la transferencia internacional de cualquier infracción de las leyes de protección de datos por su parte o por parte de la entidad destinataria; es decir, se exige responsabilidad solidaria. Se deberá garantizar expresamente el cumplimiento por su parte y por parte de la entidad destinataria de todas las obligaciones y derechos dispuestos en nuestras ley y facilitar desde España, en su condición de titular responsable del fichero, los derechos de acceso, de rectificación y cancelación que en cualquier caso corresponden a nuestros ciudadanos. Se deberán aplicar cláusulas que garanticen al afectado, cuando resulte perjudicado, el pago de las indemnizaciones por el responsable del fichero y la posibilidad, en su caso, de imponer sanciones por la Agencia de Protección de Datos española. Conforme con las garantías exigidas por el director de la Agencia, se incluirá que la entidad remitente responderá solidariamente con la destinataria frente a la Agencia de Protección de Datos y a los tribunales españoles de los eventuales incumplimientos que esta última puede incurrir respecto de las obligaciones asumidas en este contrato. Se planteó el problema -vuelvo a repetir que es la primera vez que se realiza una transferencia contractual donde no está el consentimiento de los ciudadanos afectados- de si este fichero ya venía con todas las bendiciones o para los próximos que se incorporaran debía exigirse el consentimiento. La Agencia entendió que es un deber incorporar a este fichero informar a los nuevos clientes de que sus datos van a ser transferidos y el destinatario del fichero. Esta cuestión -vuelvo a repetir- ha sido muy discutida. Incluso otros países menos garantes que el nuestro no la aplican.

Pero yo he entendido que así como puede justificarse la transferencia masiva por las dificultades de la comunicación, siempre que existan garantías, en ningún caso puede obviarse el consentimiento cuando el ciudadano puede decidir previamente si sus datos van a un sitio u a otro. Todo ello ha supuesto, señorías, una felicitación a la Agencia de Protección de Datos por la Comisión de la Unión Europea. Somos el único país que hemos notificado las transferencias internacionales en este caso y, además, nuestro escrito, donde se autoriza la transferencia que he referido, se va a utilizar como alternativo al problema tan debatido del marco del puerto seguro que los Estados Unidos de Norteamérica están presionando para que sea aceptado por la Unión Europea. El Grupo del artículo 29, donde nos reunimos todas las agencias de protección de datos de los países de la Unión, se ha manifestado mayoritariamente a Estados Unidos en contra de esta transferencia porque consideramos que no se dan garantías, no hay ley de protección de datos, no hay autoridad de control; son sólo buenos principios sin ninguna garantía, lo que a mi criterio personal supondría la muerte de la propia directiva y la imposibilidad de exigir otras transferencias a otros países. Como consecuencia de que no se ha llegado al acuerdo, se ha propuesto como alternativa el modelo de la Agencia española para posibilitar estas transferencias que otros países consideraban que eran imprescindibles que había que autorizar sin ningún tipo de garantías.

Otro tema importante, señorías, es el de los códigos tipos, es la autorregulación. El año 1998 merece una especial consideración en la actuación de la Agencia de Protección de Datos porque se ha autorizado el primer código de comercio en Internet que propició la Federación española de comercio electrónico y marketing directo. Dentro de las dificultades que supone reglar las transacciones o las comunicaciones en Internet, un medio eficaz consiste en promocionar códigos éticos para proteger los datos de los ciudadanos en dicha red. Hemos sido el primer país de la Unión Europea en el que se ha inscrito un código ético de protección de datos sobre comercio electrónico en Internet. La finalidad del código es garantizar que las empresas asociadas proporcionen un marco apropiado de protección de la intimidad ante la promoción de productos a través de Internet. Sus aspectos más destacables son los que a continuación

se mencionan. La asociación que lo ha elaborado incluye empresas muy significativas de diversos sectores como el bancario, los medios de comunicación audiovisual y escrita, correos, telégrafos, grandes establecimientos comerciales, edición y distribución de libros, informática, telecomunicaciones, marketing, asesoría, etcétera. En la promoción del código ético han participado tres de las principales asociaciones de consumidores, así como la Asociación para el autocontrol de la publicidad, organismo de carácter privado que actúa como autorregulador en el ámbito de la publicidad ilícita. De este modo se ha pretendido que el contenido del código no se limite a tener en cuenta el criterio de las empresas, sino también la problemática e intereses de los consumidores. Su presencia no se ha limitado a participar en la elaboración del código, sino que tiene un carácter estructural y permanente.

El efecto de los diez miembros que integran el comité de protección de datos de la Asociación española de comercio electrónico, órgano que tiene atribuida la competencia de control del cumplimiento del código ético, es que cuatro son representantes de las asociaciones de consumidores y uno de la Asociación para el autocontrol de la publicidad. El derecho a la información de los afectados de que sus datos han sido recabados o capturados por los anunciantes encuentra su primera manifestación en la obligación que se impone a éstos de informar en su página web, mediante un aviso, de que se está produciendo dicho tratamiento de datos. El consumidor podrá oponerse total o incluso parcialmente al tratamiento de sus datos. El consumidor podrá también seleccionar o excluir las finalidades para las que consiente que sean destinados sus datos. En el caso de terceros deberá informársele sobre la identidad de los cesionarios y sobre las finalidades perseguidas por la cesión. El derecho de oposición puede ejercitarse mediante un sistema on line.

En las relaciones con terceros contratantes, las empresas involucradas en la cesión de datos para realizar ofertas por e-mail deberán garantizar que cumplen con los principios del código ético.

En relación al tratamiento de datos sobre menores, ante la dificultad de conocer cuando un menor facilita sus datos, se aplican garantías indirectas que tratan de evitar el riesgo que afectan a tales usuarios. Se concede a los padres la posibilidad de que preventivamente puedan ejercer los derechos de acceso, cancelación y rectificación, debiendo respetarse el aviso de los padres contrario a la solicitud de información o de publicidad. A tal efecto, los anunciantes deberán animar a los menores para que consulten a sus padres. Finalmente, no podrán cederse los datos ni utilizarse para campañas inadecuadas a la edad de los menores. Las recomendaciones que he tratado de resumir son muchos más amplias (y podré ampliar, si SS.SS. lo desean) y han sido pioneras en la protección de datos personales a través de Internet, habiendo constituido el modelo seguido en la actualidad por el Consejo de Europa y por las autoridades de protección de datos de algunos países, como es el caso de Francia.

Siguiendo con la estructura de la memoria, les informaré de las actividades realizadas por la Agencia a través de la Secretaría General. Éstas han ido dirigidas a posibilitar el funcionamiento de la Agencia de Protección de Datos en sus aspectos materiales, técnicos y de recursos humanos, así como al área de atención al ciudadano. Para ello se han realizado las siguientes tareas. En primer lugar, gestión y administración de personal funcionario y laboral. Tenemos un total de 55 personas que trabajan para la Agencia, incluido su director; todos son funcionarios a excepción de tres ordenanzas con vínculo laboral. En el año 1998 hemos conseguido que se nos amplíen tres plazas en la Agencia, toda vez que nuestro personal es evidentemente escaso. También se ha controlado la ejecución y seguimiento del presupuesto. Como SS.SS. saben, nuestro presupuesto no está dependiendo de ningún ministerio, sino que es autónomo dentro de los Presupuestos Generales del Estado. Se ha gestionado un presupuesto de 523 millones; como ven, es un presupuesto modesto. También es importante destacar la gestión de ingresos de la Agencia, que han tenido su procedencia, por un lado, de transferencias establecidas por los Presupuestos Generales del Estado y, por otro, del pago de las sanciones impuestas por la Agencia en el ejercicio de su potestad sancionadora. En el año 1998 se han producido unos ingresos en este concepto de 373 millones y se han reconocido derechos por el mismo concepto en cuantía de 986 millones de pesetas.

Se ha convocado por la Agencia la segunda edición del premio de protección de datos, que, como saben, existe desde hace ya dos años para premiar una obra en materia jurídica sobre el tema de la protección de datos, con lo cual estamos propiciando la investigación y el desarrollo de las garantías constitucionales. En este caso, el premio ha recaído en un profesor asociado de derecho procesal de la Universidad del País Vasco, don José Francisco Etxeberría Guridi, por un tema de máxima importancia y actualidad, la protección de datos de carácter personal en el ámbito de la investigación penal, y, dada la calidad de los trabajos presentados, el jurado, constituido por todos los miembros del Consejo Consultivo y por el director de la Agencia, por unanimidad accedió a conceder un accésit, dotado con 100.000 pesetas, a la obra titulada La responsabilidad civil del responsable del fichero en la Ley Orgánica 5/1992, de la que es autor el profesor titular de la Universidad de las Islas Baleares, don Pedro Grimalt.

Una actividad sumamente importante de la Secretaría General, de la que depende directamente, pero yo diría que también de la Agencia, es el área de atención al ciudadano. La obligación que nos impone la propia ley orgánica es en cualquier caso realizarlo con el máximo celo. Por un lado, hay campañas de difusión en los medios de comunicación social. Nuestro presupuesto en este caso es mínimo, 20 millones para publicidad, con los que normalmente hacemos una campaña de publicidad en medios de prensa en todo el territorio nacional.

Aparte de eso, distribuimos múltiples trípticos donde se informa a los ciudadanos de sus derechos, y por supuesto directamente, en el área de atención al ciudadano, se responden las consultas, las dudas o los problemas que tienen los ciudadanos. En el año 1998 se han resuelto 12.780 consultas telefónicas, un 30 por ciento más que en el año anterior, 1.300 consultas presenciales y 1.453 consultas por escrito, con un incremento del 44 por ciento respecto a 1997. Con independencia de la emisión de estas consultas, a lo que además viene obligado por la ley, la Agencia también ha producido 300 dictámenes, dentro de su carácter no obligatorio, para las administraciones públicas y para las empresas, para ayudarles, en definitiva, a un mejor conocimiento y a un mejor cumplimiento de la ley. Asimismo las consultas en

nuestra página web han sido importantes en 1998, ya que se han producido 216.000 accesos. A todo esto, hablando sólo de números, podría decirles que en cuanto a los inforrmes preceptivos que tiene que realizar la Agencia en materia de anteproyectos de ley, de proyectos de ley y de otras normas inferiores, en el año 1998 se han evacuado 22 informes preceptivos que a estas alturas, en 1999, han aumentado a 34, lo que en definitiva demuestra una mayor sensibilidad de todos por el tema de la protección de datos. Igualmente SS.SS., a través de preguntas parlamentarias, aumentaron su interés por la Agencia, ya que, frente a diez consultas o preguntas parlamentarias en 1998, en 1999, al día de hoy -y aún hay una por contestar-, van ya 22. Por los tipos de fichero, las cuestiones relativas a solvencia patrimonial y crédito constituyen el grupo más numeroso de las consultas de los ciudadanos, y siguen a continuación los de los ficheros relativos a la publicidad.

Paso seguidamente a comentarles las tareas realizadas por la Agencia en materia de inspección y de instrucción de expedientes sancionadores, que desgraciadamente tienen que existir porque no todos están dispuestos al cumplimiento de la ley. Hablando sólo en números muy generales, las reclamaciones y denuncias recibidas en 1998 fueron 493; las resueltas, 543 -había alguna pendiente del año anterior-; los procedimientos sancionadores resueltos han sido 147, en los cuales hay que incluir nueve referentes a administraciones públicas, de los que han sido resueltos seis; se han dictado resoluciones de archivo motivadas en número de 292 y se han practicado inspecciones en 182 casos, con independencia de las inspecciones sectoriales, cuya finalidad y número les referiré a continuación. Las sanciones por faltas muy graves han sido cuatro; graves, 72, y leves, 46. Durante el año 1998 se ha procedido a una revisión en profundidad de determinados sectores -es el caso de los sistemas de información de Telefónica de España- dentro de un plan que ha sido completado en el año 1999 con la inspección del resto de los grandes operadores en telecomunicaciones, Retevisión, Euskatel y Uni 2. Se ha ampliado este plan a partir de agosto de 1999 al examen del cumplimiento de la normativa específica de la protección de datos en el sector de las telecomunicaciones, conforme a lo establecido en el artículo 50 de la Ley General de Telecomunicaciones y en el Real Decreto 1.736/1998, que desarrolla aquel precepto. También se han revisado exhaustivamente los sistemas de las mayores entidades dedicadas a la información de solvencia patrimonial y crédito,de una muestra de las más grandes compañías aseguradoras españolas, e igualmente se ha revisado la oficina Sirene española, órgano de colaboración policial establecido en el marco del Convenio de Schengen, y asimismo se ha realizado una inspección sectorial a las salas de bingo repartidas por diversas provincias del territorio nacional.
La Agencia destina todo ello a la comprobación del cumplimiento de la ley, con la idea fundamental de ayudar a estas empresas al mayor respeto del derecho a la intimidad de los ciudadanos. Como resultado de estos planes de inspección, la Agencia ha elaborado un conjunto de recomendaciones dirigidas a las asociaciones más representativas de cada sector u organismo público correspondiente, encaminadas a la subsanación de aquellas deficiencias encontradas durante la realización del plan y su mejor adecuación a la Lortad.

En el caso de ficheros de solvencia patrimonial y crédito podemos destacar algunas recomendaciones significativas, con lo cual, señor presidente, a lo mejor estoy adelantado una pregunta parlamentaria que se formulará posteriormente, pero está dentro del plan de inspección que la Agencia ha realizado en el año 1998. Las recomendaciones a los titulares de los ficheros de solvencia patrimonial, de acuerdo con las deficiencias detectadas, han sido las siguientes: a) En el caso de que se realice una anotación por cada movimiento impagado, deberá diferenciarse el capital de los intereses; b) En el caso de que no se incluyan anotaciones que puedan referirse inequívocamente a una persona específica, deberá concretarse esto; c) que se respeten los plazos legales de actualización de oficio de los ficheros, es decir una semana como máximo; d) que se adopten las medidas necesarias para que cuando se distribuyan copias de los ficheros éstas sean idénticas, se eviten las versiones piratas y se dé a los afectados toda la información que la ley establece: destinatarios de los datos, complementos, evaluaciones, etcétera; e) Recordar a los responsables de este tipo de ficheros las obligaciones que impone el Real Decreto 994/1999, en materia de medidas de seguridad, que, como saben SS.SS., ha entrado en vigor el mes de junio pasado y tendrá efectividad a partir del día 26 de este mes, en que ya serán de exigencia a todos los ficheros existentes al menos las medidas de seguridad de nivel básico.

Por lo que respecta a las compañías aseguradoras, se hicieron recomendaciones en relación a la mejora de los procedimientos de actualización de la información que debe remitirse al Registro General de Protección de Datos; igualmente, al mantenimiento en los ficheros de los datos de las aseguradoras, con especial atención a los datos especialmente protegidos, y de estos, claro está, a la salud, que son los que más habitualmente manejan las compañías de seguros; también a la información que se ofrece a los tomadores y a los asegurados, a la formación de los empleados de la compañía y a las comunicaciones de datos entre las compañías y los mediadores de seguros. En relación con las inspecciones de oficio a las salas de bingo, las principales recomendaciones volvieron a hacer referencia a la necesidad de que se remita en tiempo y debida forma la información que la ley marca al Registro General de Protección de Datos; a la necesidad de solicitar el consentimiento de sus clientes para la remisión de publicidad y a los tipos de datos que pueden recogerse de los afectados -según el reglamento del juego del bingo: nombre, apellidos, domicilio, DNI y pasaporte- y a las fechas de las visitas. En algunos casos se producen algunos problemas respecto a las legislaciones autonómicas que permiten que esos datos estén mantenidos más de los seis meses que establece la legislación de protección de datos. Por lo que se refiere a la inspección llevada a cabo en la oficina Sirene, encaminada a evaluar las medidas de seguridad existentes, se constató que, aún siendo en general satisfactorias -yo les diría que una de las más satisfactorias de Europa-, sería conveniente no obstante incrementarlas en las áreas relativas a los estándares, gestión de soportes, aspectos formales de acceso a los sistemas y acceso a las instalaciones.

En lo que respecta a los ficheros de titularidad privada, ya he expuesto anteriormente el cuadro de procedimientos sancionadores incoados en 1998 y el número de sanciones impuestas, por un importe total de 975 millones de pesetas. De entre ellas cabe destacar cuatro que corresponden a infracciones muy graves, por infracción del artículo 11 de la ley: cesión de datos, sancionado con 50 millones 1 peseta. Recuerden SS.SS. que las cuantías previstas para las muy graves van de 50 millones 1 peseta a 100 millones, por lo que aquí no se apreciaron circunstancias especiales. Las entidades a las que se han impuesto tales sanciones son las cuatro siguientes: Gestión y Técnicas del Agua, S. A.;

Manipulat y Trameses, S. L.; Sumun Films, S. A. y Banco Bilbao-Vizcaya, S. A. Otra actividad que mereció la atención de la Agencia, en el ámbito de los ficheros de titularidad privada, fue la iniciativa de las empresas que recopilaban masivamente información detallada de los ciudadanos a través de las denominadas encuestas de consumo, con objeto de configurar sus bases de datos. Los procedimientos sancionadores incoados a las entidades VNU Marketing Information Service, S. A. y a Consodata España, S. A., fueron sobreseidos por entender que en ningún caso se vulneraba lo establecido en la Lortad. En ambos supuestos, el folleto remitido al destinatario dejaba bien claro que, salvo manifestación en contra del ciudadanos, sus datos personales podían ser cedidos a empresas comerciales del sector, que podían dirigir ofertas a su domicilio; en el propio impreso existía la casilla para poder decir: no, lo cual es importante. Otra importante actividad de la Agencia el año pasado comprendió la inspección a Telefónica de España en relación con la utilización de datos personales de abonados al servicio de telecomunicaciones.

Se impusieron dos sanciones a Telefónica y tres a Telefónica Publicidad e Información, por cesión de datos a terceros sin consentimiento de los afectados, tratamiento sin consentimiento y por no facilitar la información que exige la ley en la recogida de datos. Por su parte Telefónica de España, primero, en 1998, dirigió un escrito a todos sus abonados, firmado por su presidente, en el que anunciaba que la compañía iba a dejar de ceder sus datos. Al mismo tiempo, Telefónica Publicidad e Información solicitaba a la Agencia de Protección de Datos, compañía a la que en principio iban a ser cedidos los datos, la supresión de la inscripción del fichero, con lo cual este expediente terminó con la elevación a definitivas de las medidas cautelares y sin sanción. Afortunadamente, las medidas cautelares sirvieron para que Telefónica no llegara a ceder los datos y no hubo que sancionarla;se nos hizo caso. Es de señalar que el expediente abierto

Telefónica terminó sin sanción -como digo-, supuesto que es muy importante, puesto que la Agencia está utilizando cada día más el medio de las medidas cautelares, que es el campo adecuado para evitar sobre todo un daño que luego puede ser difícilmente reparable.

En cuanto a los procedimientos abiertos a las administraciones públicas, se iniciaron nueve expedientes sancionadores por infracciones a esta clase de ficheros, de los cuales se resolvieron en 1998, seis: los cuatro primeros declarando responsabilidad y los dos restantes decretando su archivo. Aeste respecto hay que señalar que a la Consejería de Hacienda y Economía de la comunidad autónoma de La Rioja se le declaró una infracción del artículo 11 de la Ley de Protección de Datos, en relación con el artículo 15.1 de la Ley de la Función Estadística, y, por tanto, fue sancionada. El Ayuntamiento de Vinalesa (Valencia) también fue sancionado por infracción del artículo 11, porque cedió datos del padrón municipal sin consentimiento previo del afectado. A la Dirección General de Tráfico se le sancionó por infracción del artículo 4.3 de la Ley, principio de veracidad de los datos, al constar en sus ficheros datos del titular de un vehículo que no respondían a la realidad. Al Ayuntamiento de Gavá (Barcelona), por infracción del artículo 4.2, por haber incorporado de forma masiva a sus ficheros de finalidad policial datos del padrón municipal, y también por infracción del artículo 20.2 de la misma ley orgánica, por haber registrado datos personales fuera de los casos permitidos por dicho artículo. En otro caso, a la Dirección General de la Policía se sobreseyó el expediente y se archivó por una denuncia por presunta infracción del artículo 10.

Al Banco de España también se le declaró sin responsabilidad en una especial problemática en relación con el fichero Firbe, que estimo merece una consideración aparte. Como resultado de la tramitación de diversos expedientes iniciados por denuncias presentadas ante esta Agencia, se decidió la apertura de un procedimiento de infracción de administraciones públicas al Banco de España en su calidad de responsable del fichero central de información de riesgos. El CIR o Firbe, como también se le conoce, contiene información sobre los riesgos financieros contraidos por personas físicas y jurídicas, fundamentalmente por estas últimas. Los datos son facilitados por las entidades bancarias y financieras y el Banco de España, tras consolidar la información recibida, remite a cada entidad los datos relativos a sus clientes. Durante la tramitación de los expedientes se constató que el citado fichero trata datos relativos a deudas transcurridos más de seis años desde la fecha de su incorporación. La resolución del director de la Agencia concluye que el CIR, por ser un fichero de titularidad pública, debe considerarse excluido del régimen que establece el artículo 28 de la Lortad, por cuanto que siendo una de sus funciones informar a las entidades de crédito de la totalidad del riesgo contraído por sus clientes en el sistema financiero tiene esta titularidad pública. No obstante, la similitud existente entre este hecho y las funciones previstas para los ficheros a los que se refiere el artículo 28 de la Ley Orgánica de Protección de Datos hizo conveniente aclarar que, por tratarse de un fichero de titularidad pública, debe entenderse el CIR excluido del régimen del artículo 28. No obstante lo anterior, con el objeto de evitar cualquier duda sobre la suficiente cobertura legal de la normativa vigente, el director de la Agencia realizó gestiones ante el Banco de España para que se promoviera un marco legal más adecuado.

En este sentido, a fin de regularizar la situación del Firbe, entre los consiguientes contactos con el Banco de España y la Agencia de Protección de Datos, se remitió el 28 de mayo de 1999 un proyecto de disposición, con rango de ley, para actualizar la regulación del fichero adaptándola a la regulación de la normativa vigente en materia de protección de datos. Hay que pensar que la regulación del Firbe es de los años sesenta. La citada disposición fue informada por la Agencia de Protección de Datos en un extenso informe, de fecha 15 de junio de 1999, en el que se hacía hincapié en muy diversas cuestiones referentes a la adecuación del fichero al régimen consagrado por la Lortad.

Otra resolución de especial relevancia, porque hasta ahora la Agencia de Protección de Datos no se había pronunciado al respecto, es una referente a los contratos de leasing. El leasing, por considerarse que es una actividad empresarial individual (el contrato de leasing, por su propia normativa, está concebido exclusivamente para empresarios), ha entendido la Agencia que no está bajo la protección de la Lortad. La Lortad protege el derecho personal y familiar del ciudadano a la protección de su intimidad. Los comerciantes, aparte de las personas jurídicas, en el ejercicio de su actividad están, por su propia idiosincrasia, sometidos a un régimen de publicidad. No obstante esto, habrá que distinguir en algunos supuestos cuándo el comerciante actúa como tal o como ciudadano, pero en el contrato de leasing no ofrece duda porque es un contrato sólo posible entre comerciantes. Otro tema que también requirió nuestra atención

son las tarjetas de identificación de las universidades. Se tramitaron algunos expedientes que al final resultaron archivados por no encontrar responsabilidad, pero se detectó que las universidades, en muchos supuestos, tienen la colaboración de los bancos para tramitar los carnés tanto de los estudiantes como de los profesores y personal administrativo. Esto no tiene ningún problema si se realiza dentro de un marco de colaboración como los que define el artículo 27 de la ley, pero no se podrán ceder esos datos para que la entidad bancaria haga ningún tipo de prospección. La Universidad sí podrá, en su propia información, facilitar, como existe en algunos casos, ventajas a los estudiantes y profesores que les ofrecen determinadas empresas bancarias.

No obstante ello, ante la problemática detectada y ante la posibilidad de incumplir por desconocimiento la ley, la Agencia ha dirigido un comunicado al Consejo de Universidades, a través del representante de esta institución que figura en el Consejo Consultivo, a fin de facilitar el cumplimiento de la ley, toda vez que la primavera pasada tuve una reunión con los gerentes de las universidades catalanas que estaban muy preocupados por el cumplimiento de la ley.

Finalmente, voy a referirme a otra de las actividades importantes de la Agencia y que cada día va teniendo mayor exigencia, como es la actividad internacional. En primer lugar, tengo que decir que a los pocos días de hacerme cargo de la Agencia de Protección de Datos, concretamente en abril pasado, se celebró en Dublín la conferencia de primavera de los comisionados europeos de protección de datos, compuesta por todos los equivalentes a nuestra

Agencia de Protección de Datos en la Unión Europea, además de los representantes de Islandia y Noruega. En ella, la delegación española, aparte de participar en los debates, presentó un proyecto de cooperación entre las distintas agencias para crear un sistema integrado de información, utilizando la red Internet y la tecnología web, con vistas a facilitar una mayor coordinación entre las propias agencias y ofrecer una mayor información a los ciudadanos europeos.

Un hecho que hay que resaltar en el año 1998 en el plano internacional es que a la Agencia española le correspondió el honor de organizar la 20.ª Conferencia internacional de autoridades de control de datos que se celebró en Santiago de Compostela. La Agencia española recibió este encargo y la conferencia se celebró los días 16 a 18 de septiembre de 1998. El objeto de cada conferencia internacional, que se celebra con una periodicidad anual, es la puesta en común de las distintas legislaciones en materia de protección de datos para profundizar en los problemas existentes en cada país y en el estudio de las incidencias de la nueva tecnología en la privacidad de los ciudadanos. En la 20.ª Conferencia internacional participaron 20 representantes de agencias de protección de datos de todo el mundo; además de las europeas, que estuvieron todas, estuvieron también otras como Canadá, Australia, Nueva Zelanda y Japón. No obstante, los Estados Unidos de Norteamérica, a pesar de su importancia capital en el tratamiento de datos personales -hay que señalar que carecen de legislación general en esta materia y de autoridad de control-, pidieron su participación como observadores. También asistieron a la conferencia 30 representantes tanto de otras administraciones que carecen de autoridad de control como del mundo empresarial y jurídico relacionado con la protección de datos, además de un representante del Consejo de Europa. La Agencia de Protección de Datos española presentó cuatro ponencias. La primera, relativa al derecho a la privacidad y su frontera con los demás derechos humanos, fue presentada por mí como director de la autoridad de control del país anfitrión.

Se trataba de dar una visión de conjunto de los derechos al respeto a la esfera privada en los cuatro aspectos contemplados por el artículo 8 del Convenio Europeo de Derechos Humanos (vida privada, vida familiar, domicilio y correspondencia) y del tratamiento recibido por parte de la jurisprudencia del Tribunal Europeo de Derechos Humanos. Por su parte, el subdirector general de la inspección intentó transmitir el enfoque general de la labor de investigación que se emplea en la inspección de la Agencia, proveniente, sobre todo, de la experiencia adquirida y de los problemas en las casi dos mil investigaciones realizadas en los cuatro años de existencia de la Agencia española, y que han llevado aparejadas casi mil inspecciones in situ en una gran variedad de sistemas de información. El jefe del gabinete jurídico de la Agencia estudió los problemas que se han planteado en la práctica de la Agencia de Protección de Datos en relación con las empresas dedicadas a la realización de informes de riesgo financiero. En las distintas sesiones se abordaron temas relativos al escenario internacional y a la Directiva europea de protección de datos, desarrollado por un miembro de la Comisión Europea, la aplicación de las reglas de protección a datos accesibles al público, la protección de datos, en el caso de las nuevas tecnologías, para vigilancia de carreteras, Internet, correo electrónico, venta electrónica, etcétera.

Por último, el 18 septiembre y en una sesión cerrada para las autoridades de protección de la Unión Europea, se abordaron los temas de determinación de estándares de inspección y de datos especialmente protegidos. Al finalizar la conferencia se aprobó una declaración conjunta de los asistentes en relación con un proyecto del gobierno de Islandia, consistente en la creación de una base de datos genéticos de todos los habitantes de Islandia. En dicha declaración expresamos nuestra seria preocupación acerca de este asunto y recomendamos a las autoridades de Islandia que reconsideraran su proyecto a la luz de los principios fundamentales consagrados por el Convenio Europeo para la protección de derechos humanos y libertades fundamentales, del Convenio 108 relativo a la protección de datos y la Recomendación 97/5, referente a datos médicos, ambos del Consejo de Europa, así como de la Directiva 95/46. Los asistentes adoptamos un acuerdo sobre la utilización de Internet. En dicho acuerdo se ponía de manifiesto que, sobre la base de los principios de protección de datos personales, ya establecidos en muchos países y aplicables a Internet, todos los Estados, y en particular aquellos que hacen un mayor uso de las nuevas tecnologías, deben adoptar y reforzar las medidas de protección de los datos personales y promover la cooperación internacional, basada en la recomendación de principios universales, para asegurar que el crecimiento del uso de Internet no produce consecuencias incompatibles con la protección de datos y la privacidad.

Dada la calidad de estas ponencias y las aportaciones de los participantes, la Agencia las ha publicado y se han presentado en un acto que tuvo lugar el 28 de abril en el Colegio de Abogados de Madrid, organizado conjuntamente por dicha corporación y la Agencia.

En él intervinieron ante un nutrido auditorio dos diputados pertenecientes a los grupos parlamentarios con mayor representación en el Congreso. Asimismo, intervino el profesor don Miguel Ángel Dabara, quien pronunció una conferencia sobre protección de la intimidad en la sociedad de la información, y la presentación del libro de la XX Conferencia estuvo a mi cargo como director de la Agencia, cerrando el acto el decano del Colegio de Abogados, quien resaltó la trascendencia del derecho a la intimidad y el importante papel de la abogacía en su defensa.

Otro tema que ha desarrollado la Agencia en el ámbito internacional se ha producido como consecuencia de la celebración de la Conferencia de Santiago. Se despertó un interés por la autoridad de control de los Países Bajos, por la Registratiekamer, en llevar a cabo una experiencia común para compartir las auditorías de privacidad y llegar a métodos de procedimiento para inspecciones comunes. La cada vez mayor internacionalización de los tratamientos de datos y la entrada en vigor de la Directiva 95/46, hace que sea previsible que, cada vez con mayor frecuencia, sea necesario recurrir a actuaciones coordinadas entre las inspecciones de varias autoridades. Los primeros trabajos fueron presentados en la Conferencia de primavera de este año, celebrada en Helsinki. Habrá un posterior desarrollo de los trabajos que serán presentados en la próxima Conferencia de primavera.

Una labor que tenemos obligación de realizar y que además llevamos a cabo con bastante buen nivel, es la relación con nuestros colegas de la Unión Europea a través del grupo del artículo 29 de la directiva.

Dicha directiva estableció en su artículo 29 la creación de un grupo de trabajo sobre protección de datos personales. Este grupo tiene la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de la protección de las personas físicas con respecto al tratamiento de sus datos, tanto en la Comunidad como en terceros países. El grupo de trabajo está compuesto por los representantes de las autoridades nacionales independientes, encargadas de la protección de la intimidad, y por un representante de la Comisión Europea. En un futuro incluirá un representante de la autoridad responsable de las cuestiones relacionadas con la protección de datos en la Unión Europea, que aún no ha sido nombrado. La Agencia española forma parte de este grupo de trabajo, participando activamente en los diferentes debates y trabajos preparatorios, así como en los diferentes subgrupos que ya se han establecido al efecto. Como fruto de este trabajo, y en el ejercicio de las competencias atribuidas por la directiva, el grupo de trabajo ha elaborado en 1998 seis documentos, sobre los que no me extiendo porque constan en la memoria, que van desde el tratamiento de la privacidad en Internet a temas como la privacidad en los sistemas de información, en el sistema SIR de las líneas aéreas, etcétera.

Asimismo, participamos en el Consejo de Europa como miembros del Convenio 108 para la protección de los individuos en relación con sus datos automatizados. Es también relevante nuestra participación en Schengen. La Agencia de Protección de Datos ha participado activamente como autoridad de control común y han sido precisamente ingenieros españoles los que han dirigido el examen del fichero de datos común de las policías europeas, sito en Estrasburgo, porque precisamente nuestros ingenieros en protección de datos eran los más capaces. Dentro de esta actividad, la autoridad española ha inspeccionado la oficina Sirene, la de la policía española, que se llevó a cabo en 1998, con las recomendaciones que antes mencioné.

También se ha llevado cabo una campaña de publicidad respecto a dar a conocer a los ciudadanos esta existencia del Convenio Schengen y la posibilidad de acceder, rectificar o cancelar sus datos.

También hemos sido nombrados autoridad de control en Europol. El Consejo de Ministros de 25 de septiembre ha nombrado a la Agencia de Control de Datos autoridad de control y en este grupo de Europol que se ha constituido recientemente incluso se ha establecido una cámara de recursos -una cámara administrativa, pero cámara de recursos- donde los ciudadanos europeos, en el caso de que tengan que hacer alguna reclamación, puedan recurrir; se trata de una autoridad administrativa, pero europea.

Finalmente, quiero destacar que también participamos en el grupo de datos de telecomunicaciones, más conocido por grupo Berlín, donde se estudian expresamente las cuestiones relativas al desarrollo, cada día más fulgurante, de las telecomunicaciones. Este grupo ha celebrado en el año 1998 dos reuniones, la de primavera en Hong-kong y la otra en Berlín, y fruto de ellas ha sido la aprobación de diversas posturas comunes, relativas a Internet, a la interceptación de comunicaciones privadas y a las tecnologías avanzadas en la protección de datos.

Señorías, no quiero entretenerles excesivamente en un día como hoy, pero sí quiero que comprendan que la exposición de la memoria no puede quedar reducida a cinco minutos. Por ello, les pido disculpas y quedo a su entera disposición.

El señor PRESIDENTE: Muchas gracias, señor Fernández López. Sus disculpas son innecesarias; al contrario, la Comisión le queda rendidamente agradecida por el rigor, la precisión y la exhaustividad en la exposición de la memoria, con independencia de los juicios que merezca a cada grupo parlamentario en el libre ejercicio de su juicio político. Entiendo, al menos así se deduce de la parte final de su exposición, que la muy activa presencia exterior de la Administración española, a través de la Agencia de Protección de Datos, en muy distintos sectores de colaboración europeos es altamente indiciaria del alto prestigio que ha alcanzado nuestra Agencia de Protección de Datos, a pesar de su bisoñez, de su corta experiencia administrativa en este ámbito internacional, en el que las tecnologías abren posibilidades inéditas, pero también riesgos, para conceptos fundamentales asociados a nuestras más profundas convicciones sobre la libertad personal y los derechos humanos. De suerte que, sin entrar en los puntos concretos del orden del día, sino a los solos efectos de comentar o formular alguna sugerencia o repregunta sobre la intervención general del señor director de la Agencia de Protección de Datos, abriríamos un primer turno de intervenciones, que podría llegar a ser hasta de diez minutos, aun cuando estoy seguro de que serán capaces de ser más sintéticos.

A tales efectos, por el Grupo Parlamentario Federal de Izquierda Unida, tiene la palabra el señor Castellano.

El señor CASTELLANO CARDALLIAGUET: Centrándonos en el punto 1.º del orden del día, exposición de la memoria, nuestro grupo quiere agradecer sinceramente la presencia del director de la Agencia de Protección de Datos. Valoramos muy positivamente la exposición que ha hecho de las actividades efectuadas por dicha Agencia, celebrando que, como ha señalado el señor presidente, una institución de tal importancia haya tenido esa preocupación en cuanto al cumplimiento de sus obligaciones de redacción, registro y vigilancia en la confección de los correspondientes ficheros, que ha culminado levantando las correspondientes actas de infracción. Nada más tenemos que añadir, porque pensamos que el resto de comparecencias solicitadas, que van a entrar en temas muy concretos, permitirá conocer cuáles son los criterios de la Agencia en el cumplimiento de sus obligaciones. Por tanto, pura y sencillamente, reiteramos nuestra felicitación al señor compareciente y expresamos la satisfacción de este grupo parlamentario por la exposición de la memoria.

El señor PRESIDENTE: Por el Grupo Parlamentario Socialista, tiene la palabra don Carlos Navarrete.

El señor NAVARRETE MERINO: Señor director de la Agencia de Protección de Datos, quiero, en primer lugar,manifestar el enojo de nuestro grupo porque esta sesión de trabajo de la Comisión Constitucional tenga lugar en una fecha como esta, cuando los acontecimientos inmediatos, tanto la anunciada disolución de la Cámara como las propias festividades navideñas, ponen de manifiesto que esta sesión de trabajo va a tener muy poca repercusión en los medios, y a las pruebas me remito. Siendo la Agencia de Protección de Datos un arbolito recién nacido, parece que debiera ser objeto de un cuidado muy especial por parte de los legisladores, cosa que más bien brilla por su ausencia; no se entiende muy bien el retraso en la comparecencia ni la propia demora en el señalamiento de la fecha para esta Comisión. Dicho esto, quiero disolver los escrúpulos del director compareciente, a quien agradecemos su presencia, porque el tiempo que ha invertido es el corriente en la exposiciones habidas en otras comparecencias similares de autoridades de la Administración del Estado.

Cabe pensar que las cosas han ocurrido de esta manera porque no han podido ocurrir de otra o porque se oculte una secreta intención. En este caso, habría que decir que esta reunión parlamentaria es como una metáfora de la vida, lo que importa es el sentido final, la tarea de las diferentes generaciones de seres humanos. Por consiguiente, aunque estemos al final de la legislatura y sea difícil convertir en criterios concretos las conclusiones que aquí pudiéramos sacar, el Grupo Socialista en la próxima legislatura seguirá poniendo el mismo empeño en que la labor de la Agencia de Protección de Datos sea cada vez más garantista de la intimidad de las personas y más cumplidora de los objetivos que tanto orgánica como constitucionalmente le están atribuidos.

Aclarado esto, nos parece que la exposición ha tenido una extraordinaria corrección en cuanto a sistemática y que ha abarcado de una manera elocuente y lógica los distintos ámbitos de actuación de la Agencia de Protección de Datos, las consultas, las inscripciones de ficheros, las actividades de denuncia, inspección y sanción y, finalmente, la repercusión de las tareas internacionales en el ámbito de trabajo de la Agencia de Protección de Datos.

Voy a hacer algunos comentarios muy breves al socaire de la memoria.

En la página 18 aparece algo referente al tiempo medio de respuesta desde que las notificaciones tienen entrada en el registro hasta que se emite la correspondiente resolución, que es de tres días. Me gustaría que la Administración del Estado y las administraciones autonómicas, así como las administraciones locales, tomaran ejemplo y los ciudadanos pudieran verse satisfechos en sus pretensiones con la misma rapidez. En la página siguiente se menciona el artículo 20. 10 de la Directiva, donde se establece un precepto de una extraordinaria importancia, que ha ocupado últimamente los trabajos de esta Comisión, que establece que los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados deberán ser examinados previamente, antes del comienzo de dichos tratamientos, por la Agencia de Protección de Datos. Como en esos trabajos que han conducido a la elaboración de una nueva, entre paréntesis, ley orgánica de protección de datos no aparece esta facultad de control previo, mi pregunta al señor director de la Agencia es si, en su opinión, queda viciada esta Ley Orgánica de Protección de Datos con la ausencia de un precepto de la Directiva que, como decimos, al menos para el Grupo Socialista tiene una extraordinaria importancia. Esta es la primera cuestión que le planteamos.

El buen hacer de la Agencia no solamente se refleja en el tiempo que invierte para la realización de sus cometidos, sino también en la forma en que lo hace. Hacía una alusión verbal el señor director de la Agencia a las medidas cautelares como alternativa o como complemento a las vías disciplinarias y sancionadoras y, evidentemente, no solamente en la medicina, sino también en el derecho tiene plena vigencia aquello que se dice de que es mejor prevenir que curar. Las reuniones con los colegios notariales, con el sector del seguro, la banca y el marketing, con la Federación de Municipios, así como trabajos concretos con colegios, hospitales, etcétera, demuestran que existe esta preocupación, normalmente acompañada de éxito, por dar a conocer los cometidos de la Agencia y porque las entidades tanto públicas como privadas contribuyan con su colaboración a esa misión constitucional que es la protección de la intimidad de las personas.

En la página 39 se expresa que hay un aumento extraordinario en 1998 de las declaraciones de inscripción de ficheros con finalidad de encuestas de opinión, prospección de mercado, publicidad propia y publicidad para terceros, aumento que puede estar basado en el desarrollo de nuevas técnicas en el ámbito del tratamiento de la información, como datawarehouse, data mining, data mart, Sistema de ayuda a la decisión, etcétera. Estas técnicas, concluye el párrafo, surgen por la necesidad de hacer más operativa la enorme cantidad de información almacenada en distintas bases de datos. Y en la página siguiente se nos recuerda que alguna de estas técnicas se emplean para recopilar la mayor

información posible sobre un tema o sobre un sujeto para, en base a ello, establecer perfiles o tomar decisiones.

El comentario que ha hecho usted en relación con este tema merece una dedicación por nuestra parte, puesto que le atribuimos una gran importancia. Primero, porque la directiva, y así se recogía en la Lortad con palabras parecidas a las que emplea la nueva ley, entre comillas, establece que ningún procedimiento automatizado podrá servir para la elaboración de perfiles o decisiones. Estamos viendo que con estas bases de datos que se utilizan en materia de prospección comercial u otras actividades semejantes precisamente a lo que se está contribuyendo es a lo que está prohibido por la directiva, estaba prohibido por la Lortad y un recto entendimiento de la Ley Orgánica de Protección de Datos continúa prohibiendo. Pero, paradójicamente, en la nueva ley se ha establecido la posibilidad de crear un censo promocional con base en el censo electoral, además de dar carta de naturaleza a la recogida de datos que aparecen recopilados en los listines telefónicos y en las relaciones de colegios profesionales.

Cuando hoy venía hacia acá he oído en Radio 5 la noticia de que es bastante habitual, bastante frecuente, y según el comentarista no tenía ninguna importancia, que exista una representación de intereses ante la Unión Europea, representación que yo creo que no solamente existe ante la Unión Europea, sino también ante otras instancias, siendo seguramente esta representación de intereses la que ha logrado que se incorporen a la legislación tres fuentes de datos bajo, digamos, el eufemismo de fuentes públicas para lograr con estas técnicas a las que me estoy refiriendo, y de las que trata la memoria en las páginas que he mencionado, violar clara, lisa y llanamente el espíritu de la directiva. El hecho de que estas comparecencias se produzcan, como es habitual, con una cierta demora nos plantea luego algunos problemas de metodología en nuestras intervenciones. Ahí tenemos la propia memoria del año 1998, que hace referencia a los necesarios trabajos de adaptación de la Lortad a la directiva vigente.

Tendríamos que hacer referencia a algunos temas siguiendo con el asunto de la representación de los intereses. Se ha logrado, precisamente en esta línea que estamos comentando, que Unespa incorpore una enmienda, que figura como sexta en la Ley Orgánica de Protección de Datos, por la cual se podrá tratar actuarialmente, con el fin de evitar el fraude y lograr una tarificación más adecuada, la incorporación a los ficheros comunes de todas las compañías aseguradoras en España de los datos personales de los asegurados.

Bien es verdad que a este grupo de presión y a los legisladores que se sentían más sensibles ante ello se les planteaba un doble dilema, puesto que a estos sectores se les reconocía, en línea con lo que dice la directiva, el derecho de oposición, que es preceptivo en todos los casos en que la información no se obtiene del interesado con su consentimiento. La primera propuesta de enmienda no mencionaba el derecho de oposición, y alguien debió advertir que se estaba incumpliendo tal directiva, por lo que llegó una segunda redacción al Senado, una propuesta de enmienda, en la que sí se reconocía el derecho de oposición, pero con una sanción que en el lenguaje más llano, el que utiliza el pueblo, se podría calificar de chantaje. Si el asegurado, cuyos datos personales se obtienen para incorporar a unos ficheros comunes, se opone, quedará privado de la posibilidad de concertar el contrato de seguro, lo cual, evidentemente, era una actitud de dominio, de monopolio, de oligopolio del mercado del seguro, porque estamos hablando del colectivo de todas las compañías de seguros en España. Pues bien, se eligió el mal menor, con lo que tenemos una sexta norma adicional con respecto a la cual me gustaría saber si el director de la Agencia de Protección de Datos comparte el criterio del Grupo Parlamentario Socialista, que es el de que dicha disposición adicional, independientemente de otros efectos colaterales, como es la aparición de una presencia monopolística en la práctica actuarial española, significa una radical contraposición y violación de la directiva al no reconocer el derecho de oposición.

Por último, se hace alusión a los 10 miembros, incluido el director de la Agencia de Protección de Datos, que no preside el Consejo Consultivo. El Grupo Parlamentario Popular ha tenido la genialidad de ampliarlo ad nauseam, de manera que al Consejo Consultivo, un órgano de carácter estatal, un órgano de consulta y de asesoramiento de la Agencia de Protección de Datos, se pueden incorporar 17 representantes de las comunidades autónomas. Se trata de un órgano estatal donde el Estado tiene un solo representante, este Congreso tiene un solo representante, el Senado tienen un solo representante y las comunidades autónomas pueden tener 17. Las preguntas que con respecto a este asunto le planteamos al señor director de la Agencia es, primera, si se va a resentir el carácter funcional de ese Consejo Consultivo, al tener una multitud tan grande congregada; segunda, si puede ocurrir que prevalezcan los criterios autonómicos más que los criterios de la Administración central o del Estado en las opiniones que emita el Consejo Consultivo; tercera, si vislumbra la posibilidad de que, cuando se constituyan en las comunidades autónomas órganos similares, los órganos de dichas comunidades autónomas le van a conceder a la Administración del Estado un número de representantes equivalentes a la multiplicación por 17 de los representantes que tenga la comunidad autónoma en ese órgano consultivo.

No quiero ser más amplio en mi exposición. Comprendo que sobre el ánimo de los diputados presionan los acontecimientos a que he hecho referencia y que van en directa contraposición a los intereses de la Comisión Constitucional y de la Agencia de Protección de Datos.

El señor PRESIDENTE: Gracias, señor Navarrete, por las consideraciones que ha hecho al hilo de la intervención del señor director general, así como por las otras, por ese tercer turno de enmienda a la ley recientemente aprobada, a las que obviamente el señor director general está facultado para responder o no, según su criterio, y mucho menos para el ejercicio de la profecía, al que también le ha emplazado, sobre cuál pueda ser la funcionalidad del nuevo órgano.

Por el Grupo Parlamentario Vasco (EAJ-PNV), tiene la palabra la señora Uría.

La señora URÍA ECHEVARRÍA: Muchas gracias, señor presidente. Una vez más debo dárselas sinceramente por permitirme intervenir en cualquier momento durante el desarrollo de las sesiones de esta Comisión, puesto que, como me ocurre casi siempre, en este momento estoy también asistiendo a la subcomisión para el estudio del modelo policial.

No tenía más deseo que cumplir con el deber de cortesía de saludar al señor director de la Agencia de Protección de Datos, organismo que sabe que goza de todo nuestro reconocimiento, al igual que él y su predecesor en la tarea que tienen encomendada, que, desde la óptica del grupo al que represento, tiene relevancia constitucional.

Si estamos hablando de la protección de un nuevo derecho fundamental, el llamado derecho a la autodeterminación informativa en relación con el ámbito personal de todos y cada uno de los ciudadanos, si estamos obligados a la protección de este derecho, y no sólo por lo que dice el artículo 18.4 sino que es más amplio que esto, según he manifestado, puesto que se habla de la protección de la esfera personal, más allá del uso de los datos informáticos, si lo ponemos en relación con el artículo 10.2 de la propia Constitución, podríamos hablar, y así lo ha sostenido el grupo al que represento, de que la Agencia de Protección de Datos es un órgano que tiene relevancia constitucional.

Desde la perspectiva del grupo al que represento, no hemos tenido grandes problemas con la Agencia, sino todo lo contrario. Con ocasión de una anterior comparecencia y también en la de su predecesor, manifestaron su alabanza hacia las autoridades del Gobierno vasco, con relación a cómo se había producido el proceso de actualización y de regularización de sus ficheros, incluidos los policiales. Eneste caso me corresponde a mí estar a la recíproca, puesto que en los últimos tiempos es el gran problema que ha afectado a la Administración policial vasca sobre cómo podía utilizarse el dato de los números de afiliación por cada uno de los sindicatos que funcionan en la Ertzaintza, en relación con su presencia en el Consejo Sindical, sin vulnerar la protección de los datos personales en relación con un dato tan sensible como es el de la pertenencia o no a una ideología, de la pertenencia o no a un sindicato.

Finalmente, los esfuerzos efectuados por las dos partes para llegar a una solución que pudiese cumplir con los requisitos que la Agencia exigía, no porque así se lo pareciese, sino porque creía que ésa era su obligación legal -y efectivamente así lo era-, y la solución dada desde la Administración vasca en relación con la disociación del dato de afiliación con el número correspondiente a cada uno de los ertzainas, parece que ha podido satisfacer los requisitos y que es la fórmula que se ha utilizado, siendo un ejemplo de cómo la buena voluntad en la utilización de los mecanismos que el ordenamiento permite puede llevar a soluciones satisfactorias.

Quizá, puesto que es previsible que vaya a tener que ausentarme, porque el modelo policial avanza, vaya yo también a excederme del contenido de la memoria respecto de la cual no tengo sino que decir que me parecen muy meritorias las tareas que la Agencia realiza, pero sí quisiera hacer alguna reflexión en relación con el suceso más importante ocurrido desde su última comparecencia, que es la aprobación de la Ley Orgánica de Protección de datos de carácter personal. El haber sido ponente de esta ley no me lleva a tener respecto de ella el complejo de madre, porque creo que realmente no es, de los textos legales de los que esta diputada haya sido ponente, del que se pueda sentir más orgullosa. Para empezar, es efectivamente lamentable, desde mi propia consideración, que se trate de una ley orgánica -orgánica referida al desarrollo de derechos fundamentales- que carece de exposición de motivos, que es un elemento esencial interpretativo de cualquier ley que se precie. Pero es que, además, derogamos la vieja Lortad, que tenía una muy buena exposición de motivos.

Sí quisiera preguntarle, por si pudiera hacer alguna consideración, el porqué de las suspicacias manifestadas desde la Agencia, o por lo menos así se nos han transmitido a determinados grupos, en relación con las pretensiones de asunción o de reconocimiento de determinadas competencias en manos de las comunidades autónomas referidas a la protección de datos. Ya existían las reconocidas en el artículo 40 y el haber querido ir algo más lejos ha creado -según pensamos- determinadas suspicacias, y me viene bien la argumentación anterior en relación con los datos policiales y cómo han sido tratados, o cómo ha respondido la Administración vasca al respecto, para decir que nunca se han intentado utilizar más allá de lo legalmente permitido, de lo que es el marco legal, estatutario y constitucional, las competencias que se detentan. Me gustaría saber por qué existen suspicacias al respecto.

Otra consideración es la de qué criterio le merece o cómo cree que se va a poder cohonestar el que mientras estaba tramitándose en esta Cámara el proyecto de ley que luego ha sido Ley Orgánica de Protección de datos de carácter personal, se produjese desde el Gobierno la publicación de un nuevo reglamento para la protección de los ficheros, aprobado por Real decreto 994/1999, y si cree que se adecua bien al propio contenido de la ley, que no fue una precipitación el dictarlo en una fecha como la del 11 de junio, en relación con la protección de los ficheros, y si no va a ser necesario no sólo el intento de interpretación de la ley sino también la adecuación de todas estas normas reglamentarias.

Hay una última consideración, que entenderé perfectamente que no me conteste le parece que si no es adecuada, que es por qué, si se considera inadecuado que las comunidades autónomas puedan solicitar de sus institutos de estadística, en el caso de que los tenga, como es el caso catalán o vasco, datos porque están protegidos por el secreto estadístico (esa virtualidad solamente se salva respecto del Estado), sin embargo sí se contenga en la ley una disposición que coloca a las compañías de seguros en una situación que para nosotros -y hablo como si yo fuese comunidad autónoma- los partidos que gobernamos en las comunidades autónomas los quisiéramos.

Alguno de los diputados intervinientes en el trámite final de la ley se permitía incluso llamar la atención del Defensor del Pueblo para que esta disposición fuese recurrida. No nos atrevimos otros, a tanto, pero sí me gustaría saber si no considera que esta disposición adicional, contemplada como sexta, que modifica el artículo 24.3 de la Ley de Ordenación y supervisión de los seguros privados no incurre en flagrante contradicción con lo que son los bienes y derechos que el proyecto de ley, en sí, debe cumplir.

Muchas gracias, y bienvenido a esta Comisión, como siempre, señor director general.

El señor PRESIDENTE: Por el Grupo Parlamentario Popular, tiene la palabra doña Sandra Moneo.

La señora MONEO DÍEZ: En primer lugar, y como no podía ser de otra forma, en nombre del Grupo Popular quiero agradecer al director de la Agencia de Protección de Datos, señor Fernández López, su solicitud de comparecencia ante esta Comisión para informar respecto al cumplimiento de los compromisos adquiridos por él mismo, y además mostrados en esta Comisión, al hacerse responsable de la Agencia de Protección de Datos. Recuerdo que en aquella comparecencia expuso ante los miembros de esta Comisión una serie de cuestiones que iban a constituir el hilo o los compromisos que pretendía cumplir al frente de la Agencia de Protección de Datos. Algunos de ellos hacían referencia a una mejor coordinación con otras instituciones, especialmente con el Defensor del Pueblo, que recibe quejas en cuanto al cumplimiento de esta ley orgánica. Hablaba usted también de los planes de inspección de ficheros, de la aplicación estricta de la ley a los infractores, especialmente a aquellos que eran reincidentes, de estimular al consejo consultivo, de una mayor participación de la Agencia de Protección de Datos en los foros internacionales y especialmente de una potenciación del servicio de atención al ciudadano. De la extensa y yo diría que brillante exposición que hemos escuchado hoy se deduce que la mayor parte de estos objetivos han sido cumplidos. Especial interés merece al Grupo Popular el que respecta a la atención al ciudadano. Creemos que el ciudadano debe estar perfectamente informado, y que la Agencia debe estar obligatoriamente comprometida en ello, respecto a los derechos que le asisten en cuanto a la privacidad de sus datos personales. Especial atención nos ha merecido también la exposición que ha hecho respecto a la consideración internacional que merece nuestra Agencia, tanto en la participación de foros internacionales como en lo que respecta a las transferencias internacionales o a la propia felicitación de la Comisión respecto a los códigos éticos utilizados por la propia Agencia.

Nos felicitamos también del seguimiento que hace tanto de empresas públicas e instituciones públicas como privadas para el cumplimiento de la ley. Por tanto, podemos decir que, en vista de ese cumplimiento de la mayoría de los objetivos planteados en su inicial compromiso, nos felicitamos de que estos hayan sido objeto de un seguimiento diríamos nosotros que muy muy interesante y nos ponemos -como así lo hacíamos en la anterior comparecencia- a su entera disposición en un absoluto compromiso de colaboración para el cumplimiento estricto de esta ley.

El señor PRESIDENTE: Con la mayor capacidad de síntesis de que sea capaz, doy la palabra al señor Fernández López, pero antes he de decir que es ocioso que reitere lo que hacía a propósito de la intervención del señor Navarrete. El señor director de la Agencia de Protección de Datos comparece aquí desde su condición de autoridad administrativa en una intervención de control. Sus opiniones o sus juicios son sin duda estimables pero no pueden pasar de ser opiniones o juicios sobre una responsabilidad que a nosotros como legisladores incumbe. Es decir, esos juicios de valor merecidos por la reciente reforma o por la nueva ley de protección de datos, en razón del principio legítimo de mayorías y minorías, tuvimos ocasión de explayarlos de forma cumplida con ocasión de la propia tramitación.

Pero innecesaria es esta apelación sin duda a la prudencia del señor director de la Agencia del Protección de Datos.

El señor Fernández López tiene la palabra.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Ante todo quiero agradecer las palabras de don Pablo Castellano por todos los elogios que ha hecho de la actuación de la Agencia. En definitiva, como él bien conoce, lo único que hacemos es cumplir con la misión que nos ha sido encomendada de proteger los derechos de los ciudadanos y está, creo yo, fuera de dudas que en el momento en que eso no lo pudiera hacer yo no estaría al frente de la Agencia.

Contestar al señor Navarrete es mucho más complicado, porque cada palabra del señor Navarrete dispara cuatro o cinco ideas; no obstante, voy a tratar de hacerlo. En primer lugar, comparto y tengo los mismos problemas que él por el día, pero todos los días son hábiles y todos estamos al servicio de nuestra misión y, como él bien ha dicho, lo que importa es el sentido final.

En cuanto a la referencia que ha hecho al artículo 20 de la directiva, sobre la comunicación en casos especiales, yo entiendo que está suficientemente cumplida, porque la directiva, a mi modo de ver, no debía ser de mínimos, como es, debía ser una directiva mucho más armonizadora, porque esto da lugar a que tengamos sistemas más proteccionistas como el español y otros mucho menos proteccionistas, lo cual coloca a todos los ciudadanos europeos en distinta situación y sobre todo a las empresas que han de cumplir con las obligaciones también en situaciones que nunca debieran ser de discriminación, pero la realidad es la que es. Creo que el artículo 20 queda suficientemente garantizado con nuestra ley porque, en definitiva, los datos especialmente protegidos tienen un tratamiento muy concreto y muy especial en nuestra ley, sin que en el resto de los supuestos se imposibilite el que los derechos de los ciudadanos puedan ser ejercitados con toda amplitud.

Comparto absolutamente con el señor Navarrete sus reticencias sobre las nuevas tecnologías del marketing como son el datawarehouse y el data mining. Evidentemente esto nos puede llevar a la obtención de perfiles que tal vez sea la más grave violación del derecho a la intimidad, en tanto en cuanto esos perfiles sean generales y no vayan relacionados con el fin de los datos y con una promoción comercial relativa exclusivamente a ese fin.

La Agencia se ha visto en la necesidad muy reciente de imponer medidas cautelares a Telefónica de España porque estaba tratando datos de los ciudadanos de forma inversa; es decir, si bien la normativa específica en materia de telecomunicaciones habilita para que las empresas de telecomunicaciones traten los datos de los ciudadanos que hayan dado su consentimiento y sólo los datos de facturación para ofrecerles mejores promociones, nos hemos encontrado con la sorpresa, en la actuación que personalmente dirigí en el mes de agosto para ampliar la inspección que se estaba realizando a las compañías de telecomunicación en el específico caso de las telecomunicaciones, de que Telefónica

estaba obteniendo los datos de los ciudadanos de los números que le llaman y a los que llaman y, señorías, creo que esto no se necesita para ninguna promoción comercial. Se podrá tener necesidad de conocer los datos a los que llamo por cuanto que se va a establecer la factura telefónica, ante la que yo tendré también durante un tiempo la posibilidad de reclamar, pero los datos de que me llame alguien a mí no sé para qué se necesita.

Como consecuencia de estos procedimientos modernos, la Agencia de Protección de Datos ha impuesto a Telefónica medidas cautelares y, aún sin terminar el procedimiento sancionador, ya he recibido la visita de su secretario general diciéndome que van a empezar de cero, que van a pedir nueva autorización y que se van a concretar a los datos que habilita la ley.

Vuelvo a repetir, la obtención de perfiles es algo muy grave si está fuera de los ámbitos de la ley. Siempre diré que un banco es el que más datos nuestros tiene: sabe lo que ganamos, sabe en lo que lo invertimos, sabe si tenemos hijos, si no tenemos, si van a un colegio religioso, si no van a un colegio religioso, y es necesario, porque, ¿quién va a ir hoy día a la compañía de la luz a pagar su recibo o va a ir a cualquier otro sitio con el dinero en efectivo? Es una necesidad de la vida que nos ha tocado vivir. Pero -y ahí está lo importante- el banco no debe nunca utilizar esos datos fuera de la relación contractual que le liga con sus clientes. Con lo cual el que tenga esos datos es necesario; el que emplee esos datos sería establecer perfiles que irían a una vulneración grave de nuestra Ley de protección de

datos, tanto la aún vigente, como la que lo estará en el próximo mes de enero.

En cuanto al tema del censo promocional, ya conoce el señor Navarrete mi opinión al respecto y la hice patente en esta Cámara en mi primera comparecencia en el momento de tomar posesión como director de la Agencia. Teníamos el problema de que, por un lado, la Ley General Electoral establece que los datos del censo electoral deben utilizarse sólo para lo que dice la ley, para que los ciudadanos puedan ejercitar su derecho al sufragio activo. Por otro lado -y es una ley que también se ha aprobado en esta Cámara-, está la Ley de Comercio minorista -que no es orgánica, pero es una ley-, que establece que las empresas que se dediquen al marketing y a la publicidad podrán obtener del censo los nombres, apellidos y domicilios de los ciudadanos para esta función. Esto, como fácilmente comprobarán SS.SS., es una contradicción legal que nunca debió existir, pero ahí está. Como consecuencia de eso, la Agencia se ha visto con diversos expedientes sancionadores sobre la materia. Para resolver la controversia se consultó a la Junta Electoral Central, que dijo claramente -y no podía ser de otra forma- que los datos del censo electoral sólo pueden aplicarse para lo que aquella ley dice, por lo que una serie de empresas se han visto sancionadas por aplicar la Ley de Comercio minorista. Esto había que solucionarlo, y creo que es una magnífica solución la que proporciona el censo promocional. El censo promocional, permítame, señor Navarrete, que le diga que no es el censo electoral camuflado, no. El censo promocional va a ser el formado por los nombres, apellidos y domicilios de aquellos ciudadanos que se tomen del censo electoral y que decidan no apartarse de él, es decir, que deseen recibir ofertas publicitarias.

Pero es que, además, el ciudadano podrá -en el caso de que, en un principio, haya decidido no estar en el censo promocional- estarlo en un futuro o dejar de estarlo cuando autorizó al principio, por lo cual está previsto que esto pueda actualizarse anualmente.

El otro día me encontré con la presidenta del INI y me dijo que había que trabajar en el reglamento, y la Agencia de Protección de Datos no va a ser la que escurra el bulto en este aspecto; vamos a trabajar en el reglamento que lo desarrolle, de forma que puedan cohonestarse ambos derechos: el legítimo de las empresas para realizar una actividad de lícito comercio que, por otro lado, existe en la totalidad de los países de la Unión Europea y sin las garantías que nosotros le vamos a dar y, por otro lado, el derecho del ciudadano a poder preservar su intimidad y decir no al censo promocional o poder decir hoy sí y mañana no, y poder al año siguiente decir lo contrario. Creo que el censo promocional es una buena solución y es una solución más garantista que la que establecen nuestros colegas de la Unión Europea, porque, señor Navarrete, si nosotros a las empresas de publicidad y marketing -las que actúan lícitamente, vuelvo a repetir- les ponemos las cosas imposibles, lo único que ocurrirá es que estas empresas se irán a otros países de la Unión Europea y desde allí podrán realizar sus mismas promociones sin sanción de ningún tipo. Eso nos llevará a que las empresas españolas vayan cerrando, vayan destruyéndose puestos de trabajo y, en cambio, el que quiera ganar dinero y quiera hacerlo de una forma menos controlada, lo pueda hacer. Con lo cual -repito- creo que el censo promocional es una buena solución.

Me ha preguntado también sobre la posibilidad -promocionada por Unespa, a través de una disposición adicional-, de que las compañías aseguradoras tengan registros compartidos. Aunque mi misión no es, por supuesto, alabar ni criticar la ley, sino aplicarla, sí tengo que decir una cosa y es que a mí, en principio, esta disposición no me gusta que esté en la ley porque es una disposición sectorial y debería estar, en su caso, en la ley de seguros y no en esta. Por otro lado entiendo (también es legítimo el interés de las compañías de seguros) que la represión del fraude en materia de seguros es importante, pero en este momento no puedo decirle si esta es la forma adecuada o no. Tal vez si yo lo hubiera tenido que establecer lo hubiera hecho de otra forma. En cualquier caso, tenga la tranquilidad de que hay bastantes compañías de seguros, por lo menos por lo que yo conozco, que no comparten esta necesidad y que van a funcionar por libre, no van a verter sus datos a ficheros comunes, con lo cual, mientras esto ocurra, los ciudadanos podrán exigir la posibilidad de estar en unas u otras. Lo importante -y eso sí se mantiene en la ley- es el derecho de informar a los ciudadanos de que sus datos van a ser o no comunicados a un fichero común.

Estoy totalmente de acuerdo con S.S. en que 17 representantes de las comunidades autónomas en el Consejo consultivo son excesivos o, en cualquier caso, no es proporcionado con la representación de la Cámaras, que, como es bien conocido, es de un diputado y un senador.

Pero ahí están y bienvenidos sean. Como también S.S. conoce, yo al Consejo Consultivo trato de mantenerlo activo,

trato de aprovecharme de él y de que me informen, y si esto va a ser para bien, bienvenido sea. Estoy de acuerdo en que la representación es absolutamente desproporcional tanto en cuanto a las Cámaras como a los otros implicados, ya sean consumidores o empresas.

Se dice también al respecto si prevalecerán los criterios de la autonomía. Como también conoce S.S. el Consejo es puramente consultivo y, para bien o para mal, el director de la Agencia es unipersonal y es alguien que, para bien o para mal, tiene que tomar sus decisiones con todas sus consecuencias. Oirá al Consejo Consultivo, por supuesto lo oirá y tratará de que le aporte lo más posible, pero al final, en la soledad de la decisión, el director de la Agencia, como el juez, tiene que tomarla. No creo que haya dejado ningún tema sin tratar, si no me lo dice y con mucho gusto le contestaré.

Respecto a las observaciones de la señora Uría, quiero, en primer lugar, agradecer tanto sus palabras como su cooperación siempre abierta a la Agencia, lo cual es absolutamente cierto, como también es cierto que la Agencia ha mantenido unas excelentes relaciones con el Gobierno vasco. La Ley de Policía se ha hecho teniendo en consideración los criterios de la Agencia y ha habido diversas reuniones al respecto.

No me produce ninguna suspicacia las competencias de las comunidades autónomas, lo que no me gustan nada son las competencias difusas o indefinidas y, desgraciadamente, señorías, el texto que salió de esta Cámara no había por dónde cogerlo, porque no se sabía verdaderamente qué competencias se daban a las autonomías o qué competencias se le quitaban a las autonomías. Y esto es muy serio, cuando estamos hablando de los derechos de los ciudadanos. Fíjense ustedes que si ya es complicado para los ciudadanos tener que ir a la Agencia de Protección de Datos para averiguar en qué ficheros están sus datos, si eso ocurre en relación con 17 comunidades autónomas, si, además, la infracción no sabemos dónde se produce, porque alguien recoge los datos en una comunidad pero los transfiere a otra -estamos hablando de medios de comunicación telemáticos-, ¿quién es el competente, quién es el que tiene que sancionar, quién es el que puede perseguir? Esto sería muy grave, podríamos crear una situación que el ciudadano no llegara a comprender nunca. Yo siempre estoy de acuerdo con las transferencias a las comunidades autónomas, siempre que las reglas del juego sean precisas y cada uno sepa lo que tiene que hacer, y no estoy de acuerdo en cómo salió de esta Cámara el proyecto de ley de protección de datos que, por otro lado, nunca he entendido cómo cuando el Gobierno mandó un anteproyecto que iba muy circunscrito a unas reformas, que eran las necesarias, que en caulquier caso se podían haber mejorado, la Cámara decidió hacer una nueva ley.

En cuanto a si el reglamento de las medidas de seguridad que tuvo su luz en el mes de junio se adecua bien a la nueva ley, yo entiendo que sí. Quizá yo aquí tengo que ser demasiado partidista porque el borrador del reglamento fundamentalmente nació de la Agencia y los méritos -que indudablemente los tiene- no se deben a mí, sino a mi antecesor y a los funcionarios de la Agencia. El reglamento se trató como una cuestión técnica, además -según la información que tengo- se convocó a especialistas universitarios, tanto del mundo tecnológico como del mundo del derecho, y se elaboró ese reglamento que es bastante bueno y que no hace nada más que desarrollar las previsiones que ya se contienen en el artículo 9 de la propia ley. Creo que no habrá problemas con el reglamento.

En cuanto a la referencia que hace a la situación discriminatoria y que las compañías de seguros van a poder pedir datos y que las comunidades autónomas, en cambio, no podrán pedirlos debido al secreto estadístico, yo creo que son situaciones absolutamente distintas. Habrá que analizar en profundidad el artículo (yo lo he visto hace sólo unos días y no he tenido tiempo de pensar sobre ello), pero creo que tienen fundamentalmente dos funciones: por un lado, establecer datos actuariales, es decir, los grandes números y, por otro, controlar el fraude. Lo que habrá que tener muy en cuenta -y les aseguro que la Agencia va a estar muy vigilante- es que no se rebasen las competencias que atribuye la ley. La Agencia, por supuesto, las acatará, pero nunca se podrá ir más allá.

En relación con la intervención de la señora Moneo, ante todo quiero agradecer sus palabras, responderle a algunas cuestiones que ha formulado sobre lo establecido en mi comparecencia anterior ante esta Comisión y reiterarle mi compromiso de conseguir una mejor coordinación con el Defensor del Pueblo. Por razones que desconozco, cuando yo llegué a la Agencia al parecer las relaciones eran tirantes. Últimamente he visitado tanto al Defensor como a los dos adjuntos. Creo que nuestra relación es de lo más fluida y no creo que haya presentado ninguna queja contra la actuación de la Agencia, porque se le ha contestado cumplida y puntualmente.

También se ha referido S.S. al consejo consultivo. Creo que para el director de la Agencia el consejo consultivo es algo muy útil, puesto que lo constituyen personas que aportan visiones distintas desde diferentes sectores de la sociedad, con lo cual el director va a estar mejor informado de qué es lo que está ocurriendo, y también puede colaborar a una mejor difusión de un ámbito determinado de la ley, a proyectar los problemas que acontecen en un sector, etcétera.

Aunque pueda parecer que el consejo consultivo es un órgano de adorno, yo les aseguro que no es así, y además los miembros lo saben porque yo al menos trimestralmente les convoco, les pido su consejo y les planteo cuestiones porque, aunque sea yo el que deba adoptar la decisiones, su conocimiento sobre los temas, sus consejos e incluso las posibilidades de transmitir las opiniones de la Agencia me son de una gran utilidad.

En cuanto a nuestra presencia internacional, creo que es una presencia importante y que en la Unión Europea se tiene a la Agencia de Protección de Datos española un poco como modelo. Hay que tener en cuenta que, aunque nuestra ley sea un poco tardía, hemos sido de los más activos en la intervención. Piénsese, por ejemplo, que un país como Italia, que tiene una ley nueva y que lleva actuando dos años, aún no realiza planes de inspección, mientras nosotros llevamos ya 4.000. Y en otros países, como Holanda, con una tradición mucho mayor en la protección del derecho a la intimidad, la tradición va más en el conocimiento y en el respeto por los ciudadanos pero no, en cambio, en la actuación de la agencia, y lo hemos visto a través del taller que hemos realizado con los holandeses, donde se ha puesto de mani-

fiesto la mayor capacitación de nuestros inspectores y el mayor conocimiento de las funciones en el desarrollo de la misión. Los inspectores holandeses sólo intervienen en casos últimos y después de que dos abogados -no vale el requerimiento de los ciudadanos-, uno representando al ciudadano y otro a la empresa, les hayan requerido expresamente para que hagan algo porque las cosas no van bien.

Creo que tenemos (por supuesto no es mérito mío, porque yo no he hecho ni esta ley ni la anterior) un marco legislativo adecuado y creo que nuestra Agencia, desde el principio, ha funcionado adecuadamente y ha dado respuesta a las inquietudes y a las necesidades de los ciudadanos. Lo que ocurre es que la demanda cada vez es mayor y nuestro dispositivo humano se queda cada día más pequeño, y por ello este año he solicitado una ampliación de plantilla en 15 personas, que es el mínimo para poder subsistir y poder dar una respuesta mínima porque, como efectivamente hemos visto, no se puede improvisar sino que tiene que haber gente atendiendo, y a mi modo de ver tendríamos que hacerlo aún más eficazmente. Alo mejor ahora ya comunica demasiado la línea y tendríamos que tener más líneas telefónicas. En cualquier caso, creo que podemos estar seguros de que nuestro nivel en la Unión Europea es uno de los más tuitivos en la protección de los ciudadanos.

El señor PRESIDENTE: Muchas gracias, señor Fernández López.

Nos adentramos en la consideración conjunta de los puntos 2 y 3 del orden del día... (El señor Navarrete Merino pide la palabra.) ¿Señor Navarrete?

El señor NAVARRETE MERINO: Señor presidente, cuando hay una comparecencia, es habitual que los diputados hagamos uso de la palabra para decir si nos han satisfecho o no los informes que se nos han dado sobre las distintas cuestiones propuestas. Por mucha prisa que tengamos, por lo menos vamos a tratar de aprovechar el tiempo.

El señor PRESIDENTE: No tenemos otra, señor Navarrete, que la que determina lo denso del orden del día que nos convoca.

Tiene la palabra, señor Navarrete.

El señor NAVARRETE MERINO: Lo primero que quiero decir, con el afecto que sabe el señor presidente que le tengo desde hace muchos años, es que el buen éxito de la actividad parlamentaria consiste en que cada uno de los vértices de la trilogía que interviene en las comparecencias cumpla su función correctamente: las mesas y las juntas de portavoces organizan la actividad de la Cámara, los diputados plantean propuestas y cuestiones con respeto y el compareciente contesta hasta donde su ciencia llegue. Eso es lo que yo he pretendido con mis preguntas.

En cuanto a las respuestas que el ilustrísimo señor director de la Agencia me da respecto al asunto de las compañías de seguros, yo soy un poco más pesimista en mi comentario porque se habla de cálculos actuariales y los cálculos actuariales son estadísticos. Se trata de datos que no se obtienen con consentimiento del interesado, luego dan lugar al derecho de oposición, según la directiva. Es más, en el anexo 9 de la memoria, donde aparece una recomendación del Consejo de Europa para los datos estadísticos, se dice que siempre se tiene que informar al interesado y éste podrá ejercitar el derecho de oposición; derecho que la adicional sexta la niega. En este aspecto, me parece que el análisis del ilustrísimo señor director general de la Agencia no ha sido todo lo exhaustivo que pretendíamos que fuera.

Con respecto al censo promocional quiero aclarar que no he partido de la base de que se va a utilizar la totalidad del censo, sino de que, dadas las tendencias que la propia Agencia reconoce en sus memorias, que tiene la recopilación de datos para fines comerciales, es presumible que se va a utilizar el censo electoral con cruce de los datos que se obtengan de los colegios profesionales y del listín de teléfono para conseguir una finalidad fraudulenta que está expresamente prohibida por la directiva.

Para terminar, quiero agradecer este turno de palabra al que creía tener derecho, que, en todo caso, no ha discutido la Presidencia.

El señor PRESIDENTE: Señor Fernández López, brevísimamente, por favor.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Discrepo cordialmente, como siempre, en este caso del señor Navarrete.
Ami modo de ver, no es cierto que la disposición adicional sexta no posibilite el derecho oposición. Fíjese usted que dice: La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable. Si hay una indicación previa antes de la cesión yo me podré oponer. ¿Sí o no? Entiendo que sí.

- SU CRITERIO SOBRE SI LOS DATOS EXIGIBLES PARADETERMINAR EL CÁLCULO DEL TIPO DE RETENCIÓN APLICABLE SOBRE LOS RENDIMIENTOS DEL TRABAJO RESPETA EL DERECHO A LA INTIMIDAD DE LOS AFECTADOS. ASOLICITUD DEL GRUPO PARLAMENTARIO FEDERAL DE IZQUIERDA UNIDA. (Número de expediente 212/001869.)

- CONTENIDO DEL DICTAMEN EMITIDO EL 23 DE DICIEMBRE EN RELACIÓN AL MODELO OFICIAL «IRPF RETENCIONES DEL TRABAJO PERSONAL. COMUNICACIÓN DE DATOS AL PAGADOR». A SOLICITD DEL GRUPO SOCIALISTA DEL CONGRESO.

(Número de expediente 212/001872.)

El señor PRESIDENTE: Tiene la palabra don Pablo Castellano para explayar la petición de comparecencia que versa sobre si los datos exigibles para determinar el cálculo del tipo de retención aplicable sobre los rendimientos del trabajo respeta el derecho a la intimidad de los afectados.

El señor CASTELLANO CARDALLIAGUET: Entendía esta representación que, al tratarse de una comparecencia cuyo motivo conoce ya el señor director, podría empezar él contestando y a continuación se le diría si está uno o no satisfecho, porque de la otra forma cambíabamos la técnica parlamentaria en forma de pregunta. Yo preguntaría unos antecedentes, él contestaría, yo tendría que volver a intervenir y luego intervendría él, con lo cual se dilataría más; sin embargo, si es comparecencia, no sé si según el artículo 202, el compareciente explica, interviene el solicitante, contesta y aquí paz y después gloria.

El señor PRESIDENTE: ¿Comparte el señor Navarrete el criterio expuesto por don Pablo Castellano? (Asentimiento.)

En consecuencia, el señor director de la Agencia de Protección de Datos tiene la palabra para responder a las cuestiones suscitadas por los grupos parlamentarios Federal de Izquierda Unida y Socialista del Congreso, que aparecen reseñados como puntos 2 y 3 del orden del día de esta comparecencia.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Ante todo tengo que señalar que la Agencia de Protección de Datos no recibió solicitud de información en relación con las consecuencias que, para la protección de datos personales, sepudieran derivar de la Ley 40/1988, de 9 de diciembre, reguladora del impuesto sobre la renta de las personas físicas ni de los reales decretos de desarrollo reglamentario de aquélla. (El señor vicepresidente, Vera Pro, ocupa la Presidencia) Únicamente se recibió solicitud de informe por parte de la directora del Departamento de Gestión Tributaria de la Agencia Tributaria en relación con el proyecto de resolución del Departamento de Gestión Tributaria por el que se aprobaría el modelo de comunicación de la situación personal y familiar del perceptor de rentas de trabajo o de su variación ante el pagador y se determina la forma en que debe efectuarse dicha comunicación.

El citado informe fue solicitado, con carácter urgente, el 22 de diciembre de 1998, siendo emitido el informe de la Agencia el día 23 siguiente. El informe emitido formuló diversas observaciones sobre la adecuación del proyecto de la resolución a las exigencias de la Lortad, cuyo contenido fue sintéticamente el siguiente, y repito, señorías, que el informe sólo se refiere al proyecto de resolución, que es lo que se nos consulta: A) La existencia de deficiencias respecto del deber de información previsto en el articulo 5 de la Lortad, al no existir en el modelo de declaración una cláusula de información, la Agencia de Protección de Datos entendió que no cabía admitir la omisión del deber de información por deducirse ésta claramente de la naturaleza de los datos solicitados ni de las circunstancias en que se recaban (artículo 5.3 de la Lortad), al menos en lo relativo a la identificación del responsable del fichero y de su dirección, elementos básicos para ejercer los derechos de acceso, rectificación y cancelación. El informe apuntaba como posible solución la inclusión de una cláusula informativa en la que adicionalmente se recabara el consentimiento para el tratamiento de datos.

B) La necesidad de obtener el consentimiento expreso de los afectados para el tratamiento de datos especialmente protegidos, como son los relativos a la salud, puesto que el modelo de declaración prevé el tratamiento de información sobre discapacitados, tanto si es el propio contribuyente como los miembros de la organización familiar.

El informe apuntaba como posible solución la inclusión de una cláusula en el modelo de declaración para la prestación del consentimiento expreso exigido por el artículo 7.3 de la Lortad.

C) La falta de claridad sobre quién es el responsable del fichero, la Agencia Tributaria o las empresas retenedores, a los efectos de exigir garantías de la Lortad, respecto de los tratamientos de datos, creíamos que debían ser concretados. La exigencia como documentación que debe acompañar a la declaración del certificado de minusvalías y testimonios literales de las resoluciones judiciales sobre pago de anualidades por alimentos en favor de hijos o de pensiones compensatorias en favor del cónyuge, lo que supone poner en conocimiento de retenedores, ajenos a la relación jurídico-pública del impuesto, informaciones que afectan a la intimidad protegida por la Lortad, privándose de los correspondientes beneficios fiscales en el supuesto de no atender a estas peticiones. El informe proponía que se habilitara un sistema alternativo de acreditación directamente ante la Administración tributaria. La resolución que se nos envió para informar fue aprobada el 28 de diciembre de 1998 y publicada en el BOE del 30 del mismo mes.

El 18 de febrero de 1999, la directora del Departamento de Gestión Tributaria remitió a la Agencia de Protección de Datos un escrito en el que se analizaba el informe de ésta y se exponían los criterios que sirvieron de base para la elaboración de la resolución aprobada. Después de mantener diversas conversaciones sobre la cuestión, el 25 de febrero de 1999, la Agencia de Protección de Datos solicitó aclaraciones sobre diversos extremos antes de proceder a la emisión de un informe definitivo. Las aclaraciones fueron contestadas por el Departamento de Gestión Tributaria el 23 de marzo. El 5 de abril de 1999, la Agencia de Protección de Datos emitió el informe definitivo y sus conclusiones afectan a las siguientes cuestiones: A) La exigencia de proceder al tratamiento automatizado de los datos declarados a efecto de retenciones, circunstancia que determina la aplicación o no de las garantías de la Lortad. En esta materia, el informe de la Agencia manifiesta que ni la resolución aprobada, ni el software facilitado por la Agencia Tributaria, que pone a disposición de las empresas para efectuar el cálculo de la retención, implican una exigencia normativa de proceder al tratamiento automatizado de datos. La falta de exigencia normativa no excluye que exista una alta probabilidad de dicho tratamiento automatizado, toda vez que un número elevado de contribuyentes han declarado ficheros inscritos en el registro de protección de datos que tienen por objeto la gestión de retenciones. Por ello, la resolución

debe facilitar el cumplimiento de las obligaciones de la Lortad, aunque haya casos en los que la normativa no sea exigible.

B) En cuanto al responsable del fichero, circunstancia que afecta al sujeto obligado a cumplir con las exigencias en materia de protección de datos, hemos de manifestar lo siguiente: Siendo el tratamiento automatizado, conforme se ha expuesto, decisión autónoma del retenedor, éste tendrá la condición de responsable del fichero. La obligación de las administraciones públicas de informar a los ciudadanos sobre sus derechos y obligaciones, (artículo 35.g) de la Ley 30/1992, artículo 96 de la Ley General Tributaria y artículo 5 de la Ley de derechos y garantías de los contribuyentes) se cumple insuficientemente por la mera inclusión en la resolución de un apartado 9 que se limita a reiterar las exigencias de los artículos 5, 9, 10 y 11 de la Lortad.

Ajuicio de la Agencia de Protección de Datos, la forma más conveniente de facilitar el cumplimiento de la norma citada implicaría incluir en el modelo de comunicación una cláusula tipo con la información del artículo 5 de la Lortad, incluir en el mismo modelo un apartado que facilite la presentación del consentimiento expreso de los afectados para el tratamiento de datos de salud, como son los relativos a la declaración de minusvalías y pueden ser otros especialmente protegidos por el artículo 7 de la misma ley en los supuestos de pensiones compensatorias y anualidades por alimentos. La ausencia de tales previsiones en el modelo de declaración puede dar lugar al incumplimiento o al cumplimiento inadecuado de la Lortad, con las consiguientes e innecesarias consecuencias sancionadoras.

Finalmente, aclarado y admitido por el Departamento de Gestión Tributaria que los medios para acreditar la existencia de pensiones compensatorias o por alimento son los que facilitan al contribuyente una cómoda acreditación de los hechos, pero no los únicos válidos para realizarla, sería conveniente, a juicio de la Agencia, que la resolución advirtiera expresamente sobre tales posibilidades alternativas, que puedan evitar a los retendores el incurrir en infraccciones de la Lortad. Con posterioridad a la aprobación de la resolución sobre retenciones de IRPF, no se han producido denuncias sobre el incumplimiento de la Lortad que hayan exigido la actuación de la Agencia.

Por otro lado, quiero señalar, señorías, que en el año 1999 la Agencia de Protección de Datos ha realizado una inspección de oficio a la Agencia Tributaria respecto de los ficheros que la misma gestiona en relación con el IRPF, inspección que está aún pendiente de finalizar.

El señor VICEPRESIDENTE (Vera Pro): Tiene la palabra el señor Castellano.

El señor CASTELLANO CARDALLIAGUET: Nos hubiera gustado -y al decir nos hubiera gustado casi debería decir le hubiera gustado a don Pedro Antonio Ríos Martínez, a quien yo sustituyo en este acto, que ha mantenido con usted correspondencia sobre este tema, porque con fecha 18 de febrero usted le contestó a un escrito del día 17 de febrero, día en que también pidió esta comparecencia- que ese informe que ha remitido usted a la Agencia Tributaria lo hubiéramos podido tener, porque incluso a lo mejor hubiéramos retirado esta comparecencia. En todo caso, es evidente que aquí se produce una situación muy peculiar por la contestación que usted da a la Agencia Tributaria en cuanto a la valoración de los datos que se recaban de los contribuyentes, de cuyo cumplimiento se deducirán las posibilidades de desgravación o no y cuál sea la cantidad que le es objeto de retención, porque al tratarse de instituciones públicas, como es la que usted tan dignamente preside y la Agencia Tributaria, lógicamente tiene una cierta facilidad de coordinación. (El señor presidente ocupa la Presidencia.) Pero el problema se complica cuando resulta que los receptores iniciales de todos estos datos son empresas que lógicamente puden alegar que están actuando por delegación de la Administración y que se les encomienda, ni más ni menos, que la carga de tener que ser ellas incluso las que apliquen la legislación y digan cuáles son las retenciones a practicar y hagan casi, valga la expresión, una autoliquidación.

El hecho es que esta consulta que le efectuó don Pedro Antonio Ríos, su contestación y aquel conjunto de trámites que usted ha realizado y de los que nos acaba de informar, no nos han sacado de una situación de absoluta inseguridad jurídica. Vemos, por lo que usted nos informa, que los datos que son objeto de conocimiento por las empresas pagadoras no tienen ninguna garantía de ningún tipo que nos pueda permitir saber si, efectivamente, están siendo objeto de cualquier clase de abusos, teniendo en cuenta además -fíjese usted- la dificultad de control de todo un conjunto de entidades pagadoras.

Será el ciudadano el que a lo mejor, dando esos datos, pensando en que con ello facilita el cumplimiento de sus obligaciones fiscales, ha de confiar y para cuando quiera conocer si ha sido objeto ni más ni menos que de una arbitrariedad o de un abuso será ya en una situación que casi lo colocarán en la más absoluta indefensión.

Por ello, no sé hasta qué punto es suficiente y bastante el informe al que usted ha hecho referencia, evacuado el día 5 de abril como consecuencia de los datos del día 23 de marzo, porque no nos ha sacado en modo alguno de una situación de total inseguridad. A lo mejor sea necesario -esta es la sugerencia, señor director- que por parte de la Agencia, en combinación con la Agencia Tributaria, se establezca clarísimamente cuál es el modelo que ha servido a la retención. Alo mejor es mucho más dificultoso para la actuación de la Administración, pero se debe evitar esta actitud de delegación por parte de la Agencia Tributaria a las empresas pagadoras y se debe recurrir a un sistema en el que haya una relación muchísimo más directa, porque la Administración está amparada por una presunción de legalidad y la Administración está amparada por una presunción de utilización de los datos a los fines exclusivos que se les exige, pero esa presunción no ampara a las entidades pagadoras que van a conocer unos datos de enorme importancia. Y la solución, que puede ser no contestar a esos datos, ni más ni menos que lleva aparejada una situación absolutamente perjudicial para el contribuyente, porque, al no contestar a esos datos, se le van a aplicar de inmediato las máximas retenciones, con lo cual, además de la inseguridad jurídica, hay no voy a decir una sanción, pero sí la colocación por parte del contribuyente de una situación, la menos favorecedora, y sin ninguna clase de garantías.

La pregunta que yo le formulo, en sustitución de mi compañero don Pedro Antonio Ríos, que, repito, se dirigió a usted el mismo día que conoció este modelo para la declaración a efectos de retención de trabajo personal y solicitó esta comparecencia, la damos por satisfecha desde el punto de vista de la Agencia, me refiero de la Agencia de Protección de Datos, y entendemos perfectamente su contestación. Lógicamente, pone de manifiesto una situación en la que, por muchas que sean las precauciones que quiera tomar la Agencia de Protección de Datos y por muchas que sean las exigibilidades que quiera tomar la Agencia Tributaria en el cumplimiento de sus funciones y por mucha que sea la lógica predisposición del contribuyente a cumplir con sus obligaciones, sigue dependiendo de unas entidades no sometidas a ninguna clase de medidas de control ni más ni menos que la observación de lo que es la finalidad de nuestra propia legislación en materia de protección de datos y protección de la intimidad. Estamos a expensas del buen criterio que puedan tener las entidades pagadoras, sin ninguna clase de mecanismos de tutela ni de garantía. Hemos hablado a lo largo de lo que va de tarde muchas veces de la garantista ley que nos hemos dado, pero, llegada una situación como la presente, en la que no es la Agencia de Protección de Datos la responsable ni es la Agencia Tributaria, es la forma de hacer las cosas, se está a expensas, repito, ni más ni menos de cuál sea el grado de respeto que puedan tener las entidades retenedoras de estas cantidades con respecto a estos datos, lo cual nos lleva a solicitar del director de la Agencia de Protección de Datos que, en el seno de su propia Agencia, trate de articular, de acuerdo con la Agencia Tributaria, un mecanismo que evite por completo que podamos seguir en esta situación de inseguridad.

El señor PRESIDENTE: Señor Navarrete.

El señor NAVARRETE MERINO: En primer lugar, tengo que adherirme a bastantes de las manifestaciones hechas por mi compañero don Pablo Castellano en cuanto a la corrección y satisfacción que nos producen las respuestas dadas por el director de la Agencia de Protección de Datos, puesto que en nuestra petición de comparecencia solicitábamos que informara del contenido del dictamen emitido el 23 de diciembre en relación con el modelo oficial «IRPF, retenciones del trabajo personal. Comunicación de datos al pagador». Nos ha transmitido su informe y, desde ese punto de vista, tenemos que expresar nuestra satisfacción.

La segunda cuestión que queremos plantear, que también coincide tangencialmente con algo que don Pablo Castellano ha sugerido, es que tenemos que partir de la realidad de que, por ser la protección de la intimidad una materia relativamente nueva en nuestro derecho, queda un largo camino por andar y una extensa necesidad de profundizar en el respeto a la intimidad. Esto, en principio, es bueno desde el punto de vista de la actuación administrativa, pero a veces se adopta como criterio el del mínimo esfuerzo de la Administración, y no puede convertirse en regla áurea del comportamiento administrativo, que en aras de esa rapidez y mínimo esfuerzo de la Administración pública, se violenten otros intereses constitucionalmente protegidos, como es el caso de la intimidad. La figura de la retención fiscal es necesaria; pero cuando la retención fiscal entra en contacto con la intimidad de las personas quizás habría que transitar por un camino de circunvalación. Es decir, la Administración tributaria podría requerir al particular que le presente aquellos datos personales que van a modalizar su cuota tributaria, y una vez conocidos, sin pasar por el eslabón intermedio del que retiene los pagos o deduce las cuotas correspondientes, es decir, sin pasar por ese conocimiento de la intimidad del sujeto, lo único que tendría que aplicar automáticamente serían los criterios fiscales que, en función de esos datos personales, le suministre Hacienda. Retendría, calcularía correctamente la cuota; pero la intimidad sólo sería visible para la Hacienda pública.

La situación es todavía más risible desde el punto de vista legislativo si se tiene en cuenta que nosotros habíamos planteado una enmienda, que fue rechazada, a la Ley orgánica de protección de datos personales, en la que decíamos, más o menos, que, debiendo contribuir todos los poderes públicos en la persecución de la evasión fiscal, se debería facultar a la Administración tributaria para que, a los efectos de evitar esa evasión fiscal o el fraude a los derechos sociales, o para provocar la emergencia de la economía sumergida o perseguir el delito, pudiese cruzar los datos públicos con aquellos que obran en archivos de particulares. Aesto se dijo que no, aunque, como en este caso se pone de manifiesto, es algo que viene ocurriendo, permitiéndose y facilitándose que una persona interpuesta en la relación tributaria entre la Administración fiscal y el ciudadano se entere de cosas de las que no tenía que enterarse.

A la vista de esto, y teniendo en cuenta la reflexión que hacía mi compañero de tareas parlamentarias y de algunas otras cosas, don Pablo Castellano, lo que sugeriría con todo el respeto a cualquier otro criterio mejor fundado es que, para zanjar este asunto, la Agencia de Protección de Datos pueda proponerle a la Administración tributaria que requiera los datos personales que afectan a la intimidad del sujeto pasivo para que se le comuniquen a la Agencia, que ésta practique las operaciones fiscales que deben ser tenidas en cuenta por el que va a retener la cuota o descontar el pago correspondiente y así se lograría que las cuotas se correspondan con la situación personal de los sujetos y preservar la intimidad. Esto debería salir de la propia Administración tributaria. Como no ha sido así, como parlamentario representante de mi grupo y como persona que en estos momentos tiene la relación correspondiente con la Agencia de Protección de Datos, me permito sugerírselo así.

El señor PRESIDENTE: ¿Grupos distintos de los solicitantes de la comparecencia que quieran fijar posición sobre este debate. (Pausa.) Por el Grupo Parlamentario Popular, tiene la palabra el señor Martínez-Pujalte.

El señor MARTÍNEZ-PUJALTE LÓPEZ: Con absoluta brevedad, como se merece el tema y la hora.

Este asunto viene ya de hace tiempo, es una derivación de la reforma del IRPF y de la voluntad manifestada en este Parlamento de ajustar la factura fiscal final a las retenciones que se van practicando. De todos es conocido que en España se estaba produciendo una situación de tremenda injusticia, que castigaba fundamentalmente a las rentas más bajas y a los asalariados. Con el modelo de retenciones que se estaba practicando en España desde hace un tiempo se producía una sobrefinanciación de la Administración, porque se retenía por encima de la factura fiscal final no en cantidades pequeñas, sino en cantidades que se acercaban al billón de pesetas. Eso a la Administración le iba muy

bien, porque era una financiación con coste cero, pero era una situación de tremenda injustica, fundamentalmente para los más débiles, porque los asalariados eran los que cargaban sobre sus espaldas esas mayores retenciones. Por eso, en este Parlamento, con la reforma del IRPF, hubo una voluntad política, yo creo que consensuada por amplia mayoría, de ajustar retenciones y factura fiscal final, de tal manera que las retenciones fueran la determinación de lo que cada sujeto iba a pagar. Como en el nuevo IRPF hay una serie de conceptos para llegar a la base imponible, que configuran el impuesto, como son el mínimo personal y familiar, etcétera, es lógico que en el decreto de retenciones los retenedores pidan una serie de datos a los trabajadores, datos que, por otra parte, no exceden en absoluto de los que se estaban pidiendo hasta ahora. Siempre hay que tener, por una parte, ese objetivo de ajustar factura fiscal y retenciones y, por otra, la legítima defensa de la intimidad de las ciudadanas y ciudadanos españoles, por lo que se les pedía una serie de datos.

Sólo se modificaban, respecto a lo que venía funcionando con anterioridad, dos datos: se solicita a los retenidos información de las rentas del cónyuge y certificado de la discapacidad propia o familiar, porque, como es de todos sabido, la discapacidad configura una menor tributación y, por tanto, una exigencia de menor retención.

El artículo 82 del Real Decreto 214/1999, establece el carácter voluntario de la comunicación de datos por parte del contribuyente a su retenedor, no estamos hablando de una obligatoriedad, sino de un carácter voluntario en la aportación de esos datos. Si no se suministran unos datos que lo que conllevan es una menor retención, se aplican unas retenciones mayores, que no es una mayor imposición, porque luego se produce la devolución, como sucedía hasta ahora.

Ciertamente, el dato de la discapacidad ya era solicitado por las empresas para tener algún tipo de beneficios sociales o laborales.

Tampoco aporta nada excepcional. También quiero manifestar la firme voluntad de mi grupo de trabajar, sin olvidarnos de ese objetivo prioritario de ajuste factura-retención, para no desproteger la intimidad de nadie, que es un bien, y más en esta Comisión Constitucional, que mi grupo defiende a capa y espada. Bien es verdad que la solución que en su día se nos planteó en las enmiendas de algún grupo parlamentario -y no es el foro para discutirlas- nos parecía un procedimiento que no llevaba aparejada una solución definitiva, porque era una complicación administrativa enorme y además no se podía establecer una retención adecuada, porque la retención depende de las retribuciones, y eso sólo lo conoce el retenedor.

PRESIDENTE:

El señor ¿Algún comentario, señor director ?

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Solamente, como punto final de este tema, quiero decir que la Agencia no ha detectado ningún tratamiento de datos ilícito. Lo único que hizo fueron unas recomendaciones que, a nuestro entender, la Agencia Tributaria debió trasmitir a los ciudadanos y lo hizo.

Tambien quiero señalar que las medidas de seguridad que se han aprobado van a contribuir en una mayor preservación de los datos.

Nada más, señor presidente.

- INFORMAR, A LA VISTA DE LO SUCEDIDO CON LA GENERALIDAD VALENCIANA EN LA PREPARACIÓN DE UNA FIESTA DE LA TERCERAEDAD, DE LAS MEDIDAS YACTUACIONES QUE VA A ADOPTAR ENCAMINADAS A GARANTIZAR EL CUMPLIMIENTO POR LAS ADMINISTRACIONES PÚBLICAS DE LOS PRECEPTOS DE LA LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL (LORTAD). A SOLICITUD DEL GRUPO PARLAMENTARIO MIXTO. (Número de expediente 212/001901.)

- ACTUACIONES REALIZADAS POR LAAGENCIA PARA ESCLARECER LA PRESUNTA UTILIZACIÓN ILEGAL DE DATOS DE ORIGEN DESCONOCIDO EN LA CONVOCATORIA DE LA LLAMADA «GRAN FIESTA DE LA TERCERA EDAD», ORGANIZADA POR LA CONSEJERÍA DE BIENESTAR SOCIAL DE LA GENERALIDAD VALENCIANA, ASÍ COMO SU ENTREGAAUNAEMPRESAPRIVADA. ASOLICITUD DEL GRUPO SOCIALISTA DEL CONGRESO. (Número de expediente 212/001911.)

El señor PRESIDENTE: Nos adentramos en la consideración conjunta de los puntos 4 y 6, que versan sobre el mismo incidente, y para explayar las respuestas sobre los mismos, el señor director de la Agencia tiene la palabra.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Para contestar a estas dos preguntas tengo que referirme a las actuaciones que la Agencia ha realizado al efecto. A tal respecto debo decir que en el mes de enero de 1999 se presentaron ante la Agencia de Protección de Datos diversas denuncias relativas a una cesión ilícita de datos personales por parte de la Generalidad Valenciana, para la convocatoria de la gran fiesta de la tercera edad.

La Agencia realizó las oportunas actuaciones inspectoras, que dieron lugar a la iniciación de un expediente de infracción de administraciones públicas en el mes de marzo de 1999. En este procedimiento ha quedado acreditado lo siguiente: La Generalidad Valenciana remitió el 15 de octubre de 1998 a 558.454 personas mayores de 65 años, residentes en la Comunidad Valenciana, una invitación para asistir a la gran fiesta de la tercera edad, utilizando para ello los ficheros de la Consellería de Bienestar Social. Para la realización de estos envíos se contrataron los servicios de la

empresa Meydis. Los datos entregados a Meydis proceden de los ficheros de pensiones no contributivas, centros base, bonos de residencia, fondo de asistencia social, amas de casa y termalismo.

Asimismo, se entregó a Meydis un número indeterminado de disquetes, que obraban en la Subsecretaría de Bienestar Social, de los cuales no se puede precisar su origen ni su contenido. Meydis devolvió a la Consellería ocho disquetes ya normalizados, que contenían información sobre nombre, apellidos, domicilio, código postal, población, provincia, número de registro y año de nacimiento. En consecuencia, la actuación de la empresa, de Meydis, es una mera prestación de servicios informáticos, amparada por el artículo 27. Es alguien que realiza un trabajo para alguien.

La Lortad exige que los datos personales sean tratados por las administraciones públicas, de acuerdo con la finalidad para la que se obtuvieron, artículo 4.º 2. Esta previsión se ha considerado incumplida por la Generalidad Valenciana, ya que en las normas de creación de los ficheros utilizados no se concreta la posibilidad de utilizar los datos para el acto convocado.

En consecuencia, se ha declarado la existencia de una infracción del artículo 18 de la Lortad, que debe ser calificada como leve, conforme al artículo 43. Asimismo, se ha requerido a la Generalidad Valenciana para que regularice el nuevo fichero derivado del servicio contratado a Meydis, mediante la publicación de la correspondiente norma habilitante y su posterior inscripción en el registro de protección de datos, o, en caso contrario, para que proceda a su destrucción.

Finalmente, se dio cuenta de la resolución, como es preceptivo, al Defensor del Pueblo.

Nada más, señor presidente.

El señor PRESIDENTE: Por el Grupo Parlamentario Mixto, tiene la palabra el señor Peralta.

El señor PERALTA ORTEGA: Doy las gracias al señor director de la Agencia de Protección de Datos por su comparecencia y por la información que nos ha proporcionado.

Me va a permitir que, de cara a poder comprender exactamente la situación, amplíe algunos de los datos a los que usted, lógicamente, por la acumulación de trabajo que hay hoy, no ha hecho referencia o la ha hecho muy brevemente.

Tal como ha dicho, en octubre de 1998, la Generalitat Valenciana convoca lo que denominó el primer encuentro de mayores de la Comunidad Valenciana y, en el marco de ese encuentro, prácticamente como único contenido del mismo, lo que llamó la gran fiesta de mayores, que se celebró en el estadio Mestalla y para la cual se cursaron, tal como ha dicho usted, 800.000 invitaciones.

Ha habido duda de si la cifra era 800.000, como ha dicho usted, o 560.000, como en algún momento se dijo.

El señor PRESIDENTE: Discúlpeme, señor Peralta.

A esta Presidencia le ha parecido entender que la cifra dada por el señor director de la Agencia era 500.000.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): 558.454, algunos de los cuales se depuraron en el tratamiento, con lo cual, aunque no hay constancia, serían menos.

El señor PERALTA ORTEGA: Gracias, señor presidente, por su intervención.

Sin entrar en este detalle, que me parece relativamente irrelevante, creo, señor Fernández, que la cifra inicial que se entregó a Meydis, la empresa que se contrató, era de 800.000 y la que Meydis entregó finalmente es de 560.000. En todo caso, me parece que son datos sin relevancia; estamos hablando de centenares de miles de ciudadanos de la Comunidad Valenciana.

Se plantea el problema del origen de esos datos, de dónde han salido, y qué uso se ha hecho de ellos. No ha dicho usted, y creo que es bueno tenerlo en cuenta, que la Agencia de Protección de Datos dice por escrito que se requirió a la Generalitat valenciana información y documentación relativa a la campaña. La Generalitat responde con un fax indicando que se realizaron 560.000 envíos, utilizándose para ello la base de datos propia que la Consellería de Bienestar Social posee por las competencias que tiene asumidas. Esta es la respuesta literal de la Consellería.

Con muy buen criterio, la Agencia de Protección de Datos que usted preside, dice que, dado lo sucinto de la información remitida y la necesidad de comprobar el carácter y volumen de los datos incluidos en las bases propias de la Consellería, resultó preciso realizar una acción inspectora. Se lleva a cabo una acción inspectora en la sede de la Consellería de la Generalitat valenciana y se encuentra allí un número indeterminado de disquetes cuyo origen y contenido no puede precisar el subsecretario, de los cuales dispone y, a tenor de lo que había manifestado por escrito, disponía de ellos por las competencias que tenía asumidas. Esta es la realidad; me falta completarla diciendo que públicamente se declaró que estos disquetes los había dejado el Gobierno anterior.

Una Administración pública tiene esos disquetes, conoce su contenido, no los legaliza, no los registra y los entrega a una empresa de fuera. Esta es la realidad, señor director de la Agencia de Protección de Datos. Me falta decirle que en el debate que se plantea en relación con este tema hemos oído las interpretaciones más variopintas, como la de una consejera que insiste en que son exclusivamente datos que ella tiene registrados, y que es evidente que no se corres-

ponde con la verdad, porque las bases de datos que la Consellería tiene registradas en la Agencia de Protección de Datos lde ninguna manera justifica la cifra de 560.000 ciudadanos valencianos a los que se remitió la invitación; ese es un dato perfectamente comprobable. En ningún momento la Consellería informa de que tiene a su disposición y usa unos disquetes cuyo contenido ignora, cuyo origen ignora y que sin embargo entrega a una empresa para que prepare un acto determinado, lo cual es realmente inaudito e increíble. Si uno desconoce cuál es el contenido y el origen de unos disquetes no los entrega para la preparación de un acto determinado.

Finalmente, tal como usted ha dicho, se utilizan todos esos archivos y todos esos datos -algunos de ellos registrados, otros no registrados y que se han obtenido no sabemos cómo- para un acto que no tiene nada que ver, absolutamente nada que ver, con la razón por la que se constituyeron esos pocos archivos que están registrados.

Esta es, señor director, en nuestra opinión, la situación real. En esta situación real, señor director, permítame que le diga que no cabe duda de que es verdad que se ha cometido una falta, y es que se han utilizado datos para un objetivo que nada tenía que ver con eso; estamos de acuerdo en eso. Pero dígame, señor director de la APD, ¿no es ninguna ilegalidad que una administración pública disponga de unos datos y haga uso de unos disquetes con datos de los que afirma desconocer su contenido y su origen? ¿Es que es admisible en nuestro país, desde el punto de vista de protec - ción de datos, que una administración pública tenga a su disposición unos archivos de datos de los que no es capaz de precisar su origen, su contenido y que, sin embargo, los entrega, para la preparación de un acto muy concreto, a una empresa? En nuestra opinión, no; estamos convencidos de que eso no es admisible y de que si la legislación española permitiera, que por supuesto no lo permite, esa actuación, usted debería pedir que se modificara urgentemente; pero no hace falta que lo pida, no lo permite la legislación española, no puede permitir que circulen libremente datos y que además sean utilizados por una administración pública y se pueda hacer irresponsablemente.

Creo, señor Fernández, que además debería hacer una reflexión sobre cómo es posible que la Agencia de Protección de Datos no tenga la capacidad de conseguir que una administración diga de dónde procede eso. ¿Cómo puede usted aceptar o cómo puede aceptar la Agencia de Protección de Datos que una administración pública actúe de esa manera y a continuación usted no haga nada cuando le dicen que no se puede precisar ni el contenido ni el origen de los disquetes, pero que sí los tienen y los entregan para la preparación de un acto muy concreto? ¿Es que es posible tragarse -permítame la expresión- bolas tan grandes, señor Fernández? Está en juego la credibilidad de la Agencia, señor Fernández. Si usted le permite eso a una admi nistración pública, ¿por qué a otro tipo de entes no? Dicen: no lo sabíamos, mire usted, nos hemos encontrado aquí los datos, no sabemos ni el origen ni el contenido. Imagínese si es burda la mentira, pero, según dice usted, no pasa nada. Según usted, lo único que se ha producido es una falta leve consistente en que se han utilizado un conjunto de datos, unos conocidos por la Agencia y legalizados, otros no, para un fin que no era el adecuado. Yo comprendo que, en ocasiones, los temas no se plantean sólo por los procedimientos exclusivamente legales, se utilizan también los procedimientos políticos, que por supuesto son legales, pero que no se limitan a los que se siguen ante la Agencia de Protección de Datos. Este, sin lugar a dudas, ha tenido una resonancia política, pero eso, señor Fernández, no puede ser de ninguna manera una razón para que se dé carpetazo al asunto; al contrario, para reconocer la enorme trascendencia de los temas que están en juego. Cientos de miles de ciudadanos valencianos tienen datos que son manejados, al margen de la legalidad, sin registrar, por una Administración pública para un fin que no es el previsto, y eso, me dice usted, que es simplemente una falta de carácter leve.

Sinceramente, no es ésa nuestra opinión. Ysi es esa la conclusión que se desprende con la legislación vigente, debería usted pedir inmediatamente que se modificara, porque resultaría absolutamente insuficiente.

Por tanto, señor Fernández, en opinión de Nueva Izquierda, la comparecencia que usted ha hecho hoy aquí, que noso - tros le agradecemos por estar en sede parlamentaria y por los datos que nos da, es ciertamente insuficiente. Desea - ríamos -y queremos creer, señor Fernández- que de esta comparecencia de hoy aquí pueda sacar reflexiones y puntos de vista que le lleven a concluir que los hechos sobre los que ha tenido ocasión de llevar a cabo una investigación hasta la fecha, merecen un tratamiento distinto del que usted ha dado. En nuestra opinión, aquí se han producido infracciones muy serias, muy graves, de una legislación que tiene trascendencia constitucional y por eso está en esta Comisión. Estamos hablando de temas muy importantes y nosotros desearíamos que la Agencia de Protección de Datos cumpliera y tuviera en cuenta la importancia de esos datos.

El señor PRESIDENTE: Tiene la palabra el señor Navarrete.

El señor NAVARRETE MERINO: Señor presidente, señoras y señores diputados, no tendría nada de extraño que la Administración penitenciaria difundiera determinados antecedentes penales de varios centenares de miles de ex reclusos convocados por la propia Administración penitenciaria para la celebración de la gran fiesta de ex internos de cualquier prisión provincial.

El señor Peralta manifestaba su convencimiento de que la normativa legal está en contra de este tipo de actuaciones. No tengo más remedio que darle la razón, porque el artículo 19 de la Lortad dice que los datos de carácter personal recogidos por las administraciones públicas para el desempeño de sus atribuciones no serán cedidos a otras adminis - traciones públicas para el ejercicio de competencias diferentes o que versen sobre materias distintas, salvo cuando la cesión hubiera sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango.

Estamos una vez más ante el descubrimiento de un nuevo monumento erigido a la hipocresía política. Porque, con el objeto de agravar la situación de las administraciones públicas, este artículo ha sido reformado posteriormente en la ley que ha sustituido a ésta, diciendo que sólo sería posible por disposición de superior rango. Pues bien, aquí ni la de igual rango ni la de superior rango. Libérrimamente ha decidido la Generalitat Valenciana tirar de los archivos públicos

de otros departamentos de la propia Generalitat para organizar una gran fiesta, cuyo alcance político no se le escapa a nadie que tiene que ver con los casi ocho millones de afiliados al sistema de pensiones que existe en nuestro país. Esa finalidad, la finalidad de organizar grandes fiestas no está en los ficheros de las administraciones públicas sobre esta materia.

Hay otra cuestión que nos preocupa, y es el tema de los trabajos que terceros privados pueden realizar para las Administraciones públicas, que están legalmente permitidos como en su informe nos decía el director de la Agencia de Protección de Datos, es verdad, eso es lícito, pero también hay una figura muy clásica en el derecho administrativo que es la desviación de poder cuando se utilizan determinadas facultades establecidas por el ordenamiento jurídico para el ejercicio de unas funciones que de ninguna manera están contempladas por el ordenamiento jurídico, y el caso de las grandes fiestas evidentemente no constituye algo contemplado por el ordenamiento jurídico y la adaptación de los datos para otras finalidades que están en poder de las administraciones públicas con ese concreto propósito constituye al menos una desviación de poder, además de una violación flagrante del artículo 19.

Me gustaría saber quién ha calificado la sanción, porque la verdad es que la redacción del artículo 45 da pábulo a cualquier tipo de legitimación, la de la Agencia o la de la propia Administración pública. Lo que manda el artículo 45 es que la Agencia notifique al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados, si los hubiera, las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción, además de poderse iniciar -no dice qué sujeto la inicia- la correspondiente actuación disciplinaria. Que sepamos, del informe de la Agencia no se desprende que se haya dado cumplida noticia a los afectados de la arbitrariedad que se ha cometido con sus datos personales, y yo desearía que se estableciera el compromiso de la Agencia de subsanar esa notificación a los afectados.

Por otra parte, siendo válido que determinados datos sean tratados por particulares, también sería bueno que la Agencia estableciera un criterio de prudencia, porque a pesar de las obligaciones de guardar el secreto, de someterse a las instrucciones que pueda dar el mandante, etcétera, es evidente que siempre se establece una situación de riesgo para la intimidad de los datos personales cuando el tratamiento se realiza por un tercero de naturaleza privada. Por consiguiente, este debiera ser un recurso excepcional al que recurrieran las Administraciones públicas, pero no me quiero explayar mucho sobre este asunto porque luego nosvamos a ocupar del asunto de las historias clínicas, que tiene evidente parentesco con cuanto estoy expresando en estos momentos.

Por tanto, nos parece que en la actuación administrativa que se ha seguido se ha omitido el requisito de la notificación a los afectados de lo decidido por la Agencia en relación con el comportamiento irregular de la Generalidad Valenciana, y creemos que cuando se multiplica por 568.000 o por 800.000 un hecho que individualmente y con un criterio benigno podría ser calificado como falta leve, evidentemente desborda el marco de las faltas leves, y aunque lo cuantitativo no tenga siempre el mismo relieve jurídico, me parece que en este caso la calificación de la infracción y la sanción aplicada han sido extraordinariamente benévolas y poco acordes con el mandato del artículo 18 de la Constitución.

El señor PRESIDENTE: ¿Grupos no solicitantes de la comparecencia que desean fijar posición sobre la misma? (Pausa.) El señor Castellano tiene la palabra.

El señor CASTELLANO CARDALLIAGUET: Es evidente que asiste plena razón a los grupos que han solicitado la comparecencia para conocer cuál ha sido la actuación de la Agencia de Protección de Datos en el posible abuso cometido por una institución como la Generalitat Valenciana, en la utilización de unos determinados datos de domicilio y circunstancias personales de unos ciudadanos, que evidentemente no fueron obtenidos para la organización de fiestas y saraos, dado que ni en el Estatuto de Autonomía de la Comunidad Valenciana ni en ningún otro figuran estas cosas.

A mí me produciría cierta violencia que la posible actuación de la Generalitat Valenciana y su juicio fueran a recaer en esta comparecencia en responsabilidad del señor director de la Agencia de Protección de Datos. Me parecería algo así como el intento de sancionar a un ciudadano por haber redactado un panfleto insultante y descalificador por el simple hecho de que carecía del pie de imprenta. Sinceramente, es verdad que podemos excitar, y debemos hacerlo, a la Agencia de Protección de Datos -que no actúa de oficio, que siempre actuará a petición de parte- para que lleve adelante la protección de esos datos y para que instruya los expedientes. Ignoro el contenido del expediente, por tanto no me encuentro con fuerza suficiente para saber si había atenuantes o eximentes y de qué tipo y si eso era merecedor o no de una calificación de gravedad o levedad en cuanto a esa utilización.

En todo caso, no voy a mesarme los cabellos, porque estoy acostumbrado a saber que las administraciones, desde el más modesto ayuntamiento hasta el Gobierno de turno, utilizan el conocimiento de ciertos datos con carácter político. Obviamente, al no haber sido peticionario de esta comparecencia me tengo que quedar aquí.

Procuraré conocer a través de la diputada en Valencia, doña Presentación Urán, qué actividades se han realizado en el Parlamento de Valencia, en la exigencia de control a las autoridades políticas valencianas sobre este tema. Una vez que conozca este dato, nuestro grupo parlamentario -colocando lógicamente los bueyes delante de la carreta-, podrá en primer lugar exigir las responsabilidades políticas de quién haya hecho esto, y en segundo lugar una vez que aquellas hubieran sido exigidas, penetrar en cuáles pudieran ser las funciones de la Agencia de Protección de Datos.

Repito, no me escandaliza que en Valencia se haya organizado una fiesta de mayorcitos, pero sabemos que es frecuente que los presidentes de las comunidades autónomas dirijan cartas, en unos casos a los pensionistas, en otros a las madres solteras, en otros a los soldados sin graduación y, en otros a aquellos que les parece conveniente, con la intención, por otra parte lícita, de recabarles el voto. Evidentemente, me parece que los ciudadanos deberían ser más

merecedores de respeto. No soy muy dado a la utilización de citas bíblicas, porque no pertenecen a mi acervo cultural, pero quién esté libre de pecado que tire la primera piedra.

El señor PRESIDENTE: Tiene la palabra la señora Díez de la Lastra.

La señora DÍEZ DE LA LASTRA BARBADILLO: Esta petición de comparecencia forma parte de otras iniciativas que tuvieron lugar, una en las Cortes Valencianas, y otra en el Congreso de los Diputados. Yo creo que con la contestación que dio en las Cortes Valencianas el presidente del Consell quedaba bastante clara la situación, pero incluso cuando se inició el expediente el Grupo Socialista seguía preguntando todavía sobre la misma cuestión. La contestación que dio el señor Zaplana fue precisamente que no se trataba de una gran fiesta y un gran sarao, como ha dicho coloquialmente el señor Castellano. No. Es que, siguiendo la recomendación de la Asamblea de Naciones Unidas sobre la celebración del Año Internacional de las Personas Mayores, se debatieron durante una mañana las nuevas necesidades y carencias por especialistas, representantes de los jubilados y otras personas, y se acabó con una reunión en sentido lúdico, pero no fue una gran fiesta exclusivamente. Aquí se ha obviado que hubo una serie de discusiones y una serie de actos que se hicieron siguiendo las directrices de la Asamblea de Naciones Unidas.

Para mí, la intervención del señor Peralta o la del señor Castellano tienen su sentido, aunque su compañera de partido, la señora Marcos, ha aceptado otras situaciones en otros tiempos. Parece ser que se han acostumbrado a una serie de actuaciones en la época del Gobierno socialista y cargan sobre todos los grupos políticos la misma actuación que hicieron ellos; pero eso no es así. Todos recordamos perfectamente, cuando gobernaba el señor Lerma en la Comunidad Autónoma Valenciana, las fiestas de los mayores, de los jóvenes e incluso las cartas de Felipe González, el ex presidente del Gobierno a todos los jóvenes que cumplían 18 años para darles la enhorabuena y aanimarles a votar. Sinceramente creo que las dos comparecencias del presidente del Consell aclararon bastante la situación, se dijo allí incluso lo que había costado, eran 65 millones que provenían de la Consellería de Bienestar Social, y que en el ámbito de su competencia la Consellería tiene que tener una serie de datos para conocer la población que debe atender, sus necesidades, sus demandas, razón por la cual existen unos ficheros dedicados a la tercera edad. Se ha dicho que los datos utilizados se entregaron a una entidad Meydis, y que se firmó un contrato de confidencialidad que aquí también se ha obviado decirlo. Creo que es buscar tres pies al gato.

Parece que a los grupos que han pedido la comparecencia les molesta el éxito que tuvo aquel foro. Yo he estado 13 años en la oposición, y en una democracia la oposición es tan importante como el Gobierno; pero hay que ejercerla siempre con seriedad, rigor y buena fe y yo creo que por parte del Grupo Socialista y del señor Peralta no ha habido ninguna de las tres cualidades.

Tengo que hacer muy brevemente el resumen de las actuaciones de la Agencia de Protección de Datos y de la resolución dictada por la Agencia. La actuación de la Generalidad valenciana no ha supuesto menoscabo ninguno de los derechos de las personas invitadas en su día al acto convocado; no existe indicio alguno de delito en las actuaciones desarrolladas por la Consellería de Bienestar Social; no se aprecia la existencia de infracciones graves o muy graves. Es curioso que cuando se pide una comparecencia y se hace una denuncia lo menos que se puede es esperar a que se abra el expediente y no calificar a priori, como hace el señor Zamora en su denuncia, que aquellos hechos son graves o muy graves. La Consellería de Bienestar Social no ha pedido ningún dato de forma fraudulenta al margen de la legalidad, la Agencia sólo ha estimado la existencia de irregularidades de tipo formal que no invalidan en ningún momento las actuaciones desarrolladas por la Generalidad y se ha subsanado claramente las deficiencias formales que había en el registro de datos. Por eso, vuelvo a repetir, porque cuando se ha estado en la oposición y se está apoyando al Gobierno parece que uno tiene más visión total de cómo se debe ejercer eso, que el Grupo Popular cree que ha faltado seriedad, rigor y buena fe; parece que es una pataleta y el señor Navarrete no tiene ninguna autoridad moral para hablar como ha hablado. (Los señores Navarrete Merino y Peralta Ortega piden la palabra.)

El señor PRESIDENTE: Recuerden señores Navarrete y Peralta, que no se trata de una iniciativa de carácter contradictorio, pero han sido reiteradamente aludidos, por lo que tienen un minuto. En primer término, tiene la palabra el señor Peralta.

El señor PERALTA ORTEGA: Gracias, señor presidente, por su en mi opinión acertada interpretación de lo que ha ocurrido. De hecho se ha hablado de que nos falta rigor, seriedad y buena fe. No sé cuantos años lleva la señora diputada.

El señor PRESIDENTE: Muchísimos.

El señor PERALTA ORTEGA: Créame, señor presidente, que casi tantos como yo.

Desde esta labor nos parece que hay leyes y ésta que hoy nos ocupa tiene una fecha de nacimiento determinada. Antes se podía hacer oposición, no sé si con rigor, seriedad y buena fe, pero no se podía hacer con fundamento en la ley, ahora afortunadamente la podemos hacer con fundamento en la ley. Quiero recordarle a la señora diputada que el director de la Agencia de Protección de Datos ha sancionado a la Generalidad Valenciana, no le he oído a la señora diputada decir que se ha sancionado a la Generalidad Valenciana. Ése es un hecho que como diputado debería merecer una condena; a mí me la merece, sin lugar a dudas. Creo que lo significativo en ese caso es que una Administración pública ha infringido la ley, y la señora diputada considera más importante decir que los diputados carecemos de rigor, de seriedad y de buena fe y callar que la Generalidad valenciana, una administración pública ha sido sancionada.

Créame, no pretendo juzgar a la Agencia de Protección de Datos, pero si no sabe cumplir su papel, esa actuación que

acabamos de ver de que considera que lo grave es quienes hemos denunciado con acierto una actuación ilegal de la Generalitat valenciana, se convertirá en norma de conducta. No creo que podamos dar por buenas las infracciones legales, por amplias que sean; yo no comparto ese criterio. Lo que tenemos que hacer es, por más que cueste, lograr que se cumpla la ley, y en esa tarea, la Agencia de Protección de Datos tiene un papel fundamental. Qué duda cabe que la responsabilidad del incumplimiento es de quien incumple; la Generalitat Valenciana gestionada por el señor Zaplana, del Partido Popular, pero la Agencia de Protección de Datos tiene un papel esencial en conseguir que se respete la ley. En este caso, y le he dado datos y argumentos, entender que sólo se ha producido una utilización de datos para un fin no adecuado, no es suficiente. Tendría usted que preguntarle a la Generalitat valenciana por qué tenía esos disquetes y de dónde los ha sacado y no dar por buena la afirmación de que no puede justificar su origen, ni admitir que una Administración pública pueda utilizar unos disquetes con datos personales de manera absolutamente irresponsable y al margen de la ley. En nuestra opinión...

El señor PRESIDENTE: Señor Peralta, le he dado la palabra para replicar a la señora Díez de la Lastra, no al señor compareciente.

El señor PERALTA ORTEGA: Termino, señor presidente, y agradezco su benevolencia. Desde Nueva Izquierda nos gustaría que esta comparecencia sirviera para que usted nos informara a nosotros, pero también para que escuche nuestras valoraciones, políticas sin duda, que tienen la incidencia que deben tener en un expediente, porque son valoraciones políticas y pueden servir para que avance el imperio de la ley en nuestro país, y evitar hechos tan sonrojantes como que una Administración pública utilice, al margen de la ley, datos de cientos de miles de ciudadanos.

El señor PRESIDENTE: Tiene la palabra el señor Navarrete.

El señor NAVARRETE MERINO: Me voy a defender de las alusiones que se han hecho, sin incurrir en el mismo tipo de argumentos ad hominem que ha empleado la señora diputada, porque como nos sobran las razones no precisamos recurrir a los adjetivos calificativos. La democracia, lo digo por si hay alguna persona del Grupo Parlamentario Popular que todavía no se ha enterado, es algo dialéctico. A la calidad democrática contribuimos todos los que estamos en la vida política con más o menos preeminencia, criticando los defectos del adversario, sin que los defectos que otro adversario pueda haber cometido sirvan de alibí. A ver si se enteran ustedes de que en el derecho penal, y con la misma legitimidad en la vida política, los malos precedentes no constituyen ninguna patente de corso. Ustedes están en su derecho, cuando consideren que cualquier autoridad o funcionario de cualquier comunidad autónoma actúa incorrectamente, de poner las denuncias que procedan; pero es verdaderamente torticero recurrir a difuminadas responsabilidades para exonerarse de las propias. Ustedes han infringido el artículo 19, y no sólo eso, sino que han hecho una ceremonia teatral en la reelaboración del artículo 19, que no se compagina con lo que está ocurriendo en algunas administraciones públicas, y ponemos por caso el que estamos comentando esta tarde.

Por consiguiente, expreso mi opinión. Me parece que la sanción leve no se compagina con la naturaleza de la infracción que se ha cometido, digan lo que quieran sobre este asunto otros compañeros de la Cámara. Desearía que se adoptaran las medidas pertinentes por parte de la Agencia de Protección de Datos, la Generalitat, otras comunidades autónomas y la Administración central del Estado, para que los ciudadanos no se sientan manejados cada vez que convenga a cualquier instancia política poco escrupulosa.

El señor PRESIDENTE: Señora Díez de la Lastra.

La señora DÍEZ DE LA LASTRA BARBADILLO: Sólo un minuto, para decirle al señor Peralta que tenía conciencia de que había una infracción leve, pero ante la acusación en la denuncia por el señor Zamora, compañero suyo, de que la infracción era grave o muy grave, se me ha pasado, pero yo le tengo que decir que la Agencia resuelve declarar la ausencia de responsabilidad respecto a la imputación de infracción del artículo 6 de la Lortad.

Señor Navarrete, le ha tocado a usted jugar ese papel, como nos toca a veces a muchos. Es raro que no haya ningún diputado de la Comunidad Autónoma Valenciana de su grupo, que está más en comunicación con las Cortes valencianas, y supongo que le habrán pasado fichas, pero es raro que no haya venido ninguno aquí a hablar de la Comunidad Autónoma Valenciana siendo de esa comunidad. Claro que la oposición tiene que contribuir a la calidad democrática. Ya le he dicho que yo he estado 11 años en la oposición en el Ayuntamiento de Alicante y mantengo lo que he dicho. Quizas usted querría que la falta fuera gravísima y que se hubiera formado un escándalo. No es así; acate lo que se ha dicho. Ustedes están de acuerdo con la justicia cuando les va bien para ustedes, ahora con la protección de datos, y cuando no está a favor de ustedes protestan. Eso no es seriedad, rigor, ni buena fe.

El señor PRESIDENTE: Señor director de la Agencia, ¿algún comentario sobre el debate y sobre las manifestaciones que se han realizado?

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Sí, señor presidente, y lo más brevemente posible.

Quiero dejar aquí muy claro es la actuación de la Agencia de Protección de Datos. Señor Peralta o yo me he explicado mal o usted no me ha entendido. En primer lugar, hay que dejar muy claro que los datos que al final se depuran y por los que se envían las cartas son 558.454, que son los que la Generalidad valenciana remite el 15 de octubre de 1998 con cartas a personas mayores de 65 años; no hay 800.000. En segundo lugar, ¿de dónde han salido los datos? Salen, también creía que lo había explicado, de una serie de ficheros que tenía la Consejería de Asuntos Sociales. Son ficheros relativos a pensiones no contributivas, centros base, bonos residencia, fondo de asistencia social, amas de casa y termalismo. ¿Y dónde aparecen esos otros datos que usted dice? Estamos hablando de que la inspección la hacemos

pasado enero, que es cuando se denuncia. Se envían las cartas en octubre, en enero es cuando se denuncian y me parece que cuando nosotros inspeccionamos es en el mes de febrero. El mes de febrero nos enteramos de que existen esos otros datos en unos disquetes por la candidez del viceconsejero de Bienestar Social, que dice había por allí unos disquetes desde hacía mucho tiempo, que estaban en la Consejería y los entregó para que los depuraran. Se trataba de buscar unas personas de una edad y además que estuvieran vivas. Por eso nos enteramos, no por la perspicacia de mis inspectores, que a toro pasado difícilmente podrían averiguar nada; de ahí es de donde proceden los datos. Por tanto, en principio son datos que están en la Consejería de Bienestar Social, que no se han utilizado de otro departamento de la Administración autonómica, sino que en principio hay que presumirlo del mismo, puesto que no tenemos otras pruebas.

A pesar de eso, la Agencia entiende que esos datos no tienen cobertura en los ficheros y por eso se sanciona, pero se sanciona precisamente como una falta leve, que por otro lado no tiene mayor trascendencia porque a las administraciones públicas, como saben SS.SS, no se les impone como a los particulares 100.000 pesetas o 100 millones, sino que es el agravio público de haber infringido la ley. Lo que pasa es que la Agencia tiene unos criterios cuando va a calificar una falta como leve, como grave o como muy grave y esos criterios los tiene que aplicar para todos, sea una Administración, sea un particular o quien sea.

En cuanto a que se entregan a una empresa privada, sí se entrega a una empresa privada, pero a una empresa privada que se dedica a este tipo de tratamientos, con un contrato donde hay confidencialidad y donde no se ha detectado ninguna infracción por parte de la empresa, sino la devolución a la Consejería de Bienestar Social de los datos ya depurados. O sea que no hay en ningún caso utilización por particulares.

Estoy absolutamente de acuerdo con el señor Navarrete en que cuando además estos datos van a ir en algún supuesto a una empresa privada, hay que ser muy celosos de ellos. Fíjese si lo seremos que en algún caso, aprovechando las facilidades que da el artículo 27, no en temas de administraciones públicas sino de entes privados para hacer cesión de datos, han tratado de enmascarar una cesión hablando de alquiler de datos, se ha descubierto la cesión y se ha sancionado.

Por supuesto que en este tratamiento de datos la Agencia es especialmente celosa y vigilante.

Nos han dicho también que no hemos hecho nada aparte de esto, y yo tengo que decir que además de declarar la infracción se ha requerido a la Generalitat valenciana para que regularice el nuevo fichero derivado del servicio contratado a Meydis mediante la publicación de la correspondiente norma habilitante y posterior inscripción en el registro, y en caso contrario para que proceda a la destrucción. Es decir, la Agencia sí ha hecho algo más.

Me han dicho también que no lo hemos comunicado a los afectados, y tengo que decir que yo aplico las normas del derecho administrativo, notifico a los que están presentes en el procedimiento como afectados. No puedo hacer una notificación general; pero a todo el que pide la comparecencia en el procedimiento, si acredita las funciones apropiadas para ser parte en él, por supuesto se le reconoce, se le notifica y se le habilita la vía de recursos. Además, en cualquier caso serán los tribunales los que, corrigiendo la posible equivocación en la calificación de la Agencia, tendrán la última palabra. Sí les puedo garantizar que la Agencia ha actuado con los criterios que tiene para enjuiciar un tipo de conductas y que en este caso, además, si no es por el viceconsejero ni nos hubiéramos enterado de la existencia de las cintas porque nadie nos habló de ellas. Nadie, señor Peralta, nadie nos habló de ellas, y cuando los inspectores fueron, que no pudieron ir antes de recibir la denuncia, allí ya no había ningún fichero porque ya se habían envíado las cartas y se habían depurado. La Agencia de Protección de Datos actuó dentro de la más estricta legalidad y actuó además con prontitud.

Piense que tenemos 12 inspectores para atender a todo el territorio nacional, y actuamos con total prontitud. En el mes de febrero estaban los inspectores en Valencia, y se nos habían denunciado en enero unos hechos que ocurrieron en el mes de octubre y que mientras tanto a nadie se le ocurrió denunciar.

El señor PRESIDENTE: Gracias, señor director de la Agencia de Protección de Datos.

Vamos a hacer un breve receso de cinco minutos y entraremos inmediatamente en el punto 5 del orden del día, señor Peralta, en el que aparece la solicitud de comparecencia suscrita por el grupo al que pertenece S.S. (Pausa.)

- ACTUACIÓN DE LA AGENCIA EN DEFENSA DE LOS DERECHOS DE LOS CIUDADANOS AFECTADOS POR SU INCLUSIÓN ILEGÍTIMA EN LOS LLAMADOS «FICHEROS DE MOROSOS», ASÍ COMO DE LAS REFORMAS LEGISLATIVAS NECESARIAS PARA SU MAYOR EFICACIA EN ESTE ÁMBITO. A SOLICITUD DEL GRUPO PARLAMENTARIO MIXTO. (Número de expediente 212/001910.)

El señor PRESIDENTE: Se reanuda la sesión. Punto 5 del orden del día.

Señor Peralta, tiene S.S. la palabra en relación con el punto 5 del orden del día.

El señor PERALTA ORTEGA: Quiero manifestar que, habiéndose modificado la ley que regía cuando pedimos esa comparecencia, renunciamos a la misma.

El señor PRESIDENTE: En consecuencia, el señor director queda eximido asimismo de dar respuesta.

- MEDIDAS QUE PUDIERAN ADOPTARSE PARA PREVENIR LA CESIÓN ILÍCITA DE DATOS PERSONALES

ARCHIVADOS POR LAS ADMINISTRACIONES PÚBLICAS. A SOLICITUD DEL GRUPO SOCIALISTA DEL CONGRESO. (Número de expediente 212/001933.)

- ADECUACIÓN DE LAS MEDIDAS ADOPTADAS POR EL MINISTRO DE SANIDAD YCONSUMO, A LA LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL (LORTAD). A SOLICITUD DEL GRUPO SOCIALISTA DEL CONGRESO. (Número de expediente 212/002141.)

- VALORACIÓN DE LA AGENCIA ACERCA DE LA CESIÓN DE HISTORIALES CLÍNICOS DE LOS CENTROS DEL INSALUD A EMPRESAS PRIVADAS. ASOLICITUD DEL GRUPO PARLAMENTARIO MIXTO. (Número de expediente 212/002403.)

El señor PRESIDENTE: Pasamos al punto 7 del orden del día, comparecencia suscrita por el Grupo Socialista del Congreso en relación con las medidas que pudieran adoptarse para prevenir la cesión ilícita de datos personales archivados por las administraciones públicas. (El señor Navarrete Merino pide la palabra.) Señor Navarrete.

El señor NAVARRETE MERINO: Por aligerar el debate, y dado que los puntos 7 y 8 están estrechamente relacionados, por nuestra parte no habría ningún inconveniente en que se analizaran de forma conjunta.

No sé si el grupo que ha solicitado el punto 9 del orden del día (no soy el titular de la comparecencia) estaría dispuesto a incluirlo en el bloque.

El señor PRESIDENTE: Señor director, ignoro si el señor Peralta se va a reintegrar o no en el transcurso de la sesión, pero le ruego que dé respuesta a los puntos 7, 8 y 9 de forma conjunta, con independencia de que después demos voz a los grupos para expresar sus posiciones.

El señor CASTELLANO CARDALLIAGUET: Si el punto 9 es pedido por el Grupo Parlamentario Mixto y no hay nadie para sostenerlo, no entiendo por qué razón tiene que ser objeto de tratamiento.

El señor PRESIDENTE: Porque versa sobre el mismo tema que el punto 8.

El señor CASTELLANO CARDALLIAGUET: Pero, señor presidente, la más elemental coherencia impone que si el grupo que solicita una iniciativa no está, se dé por decaída.

El señor PRESIDENTE: Señor Castellano, si el señor director va a responder al punto 8, entendemos que el señor Peralta in absentia se dará por satisfecho.

El señor CASTELLANO CARDALLIAGUET: El señor Peralta antes de irse podía haber dicho si mantiene la iniciativa del punto 9 o no.

El señor PRESIDENTE: Esperemos que se reintegre. Estoy protegiendo la ausencia del señor Peralta, señor Castellano.

El señor CASTELLANO CARDALLIAGUET: Me parece muy bien, señor presidente, pero proteja usted también la presencia de los que nos quedamos.

El señor PRESIDENTE: Señor director.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): En relación con estos puntos que ahora se agrupan, en primer lugar, procede hacer alguna reflexión sobre la transmisión de datos entre administraciones públicas. Todos sabemos que es necesario y que en algunos supuestos se abusa de ello. El principio de finalidad, aquel para el cual fueron recogidos los datos, es el que debe imperar en las transferencias de los datos entre administraciones públicas.

En aquellos supuestos en los que no esté previsto por una norma o una ley de creación de fichero los datos entre administraciones públicas no deberán comunicarse a no sea que sea para una misma finalidad.

La Agencia está atenta a los problemas que puedan derivarse de la transmisión de datos entre administraciones públicas. Buena prueba de ello son los procedimientos de administraciones públicas, cada día más numerosos, y que tienen un especial relieve en el presente año, 1999. Así podemos comprobar que se ha declarado una infracción muy grave de cesión de datos sin consentimiento del afectado de la Dirección General de Instituciones Penitenciarias. Este procedimiento fue un poco curioso porque era un funcionario de la propia Dirección, cuyos datos se comunican al registro de altos cargos. En principio era un dato público porque su nombramiento y su cargo figuraban en el Boletín Oficial del Estado, pero luego se cambia la titularidad del cargo sin decir el funcionario y entonces se le cambia en el fichero de altos cargos, con lo cual la cesión no pudo venir de ninguna fuente accesible al público y por eso se sanciona a la Dirección General. Se ha declarado una infracción muy grave de la Agencia Estatal de Administración Tributaria por cesión de datos sin consentimiento a la Cámara de Comercio, Industria y Navegación y a ésta una infracción grave por tratamiento de datos personales sin consentimiento del afectado.

En otra resolución, se declara una infracción grave por vulneración del deber de secreto -artículo 10 de la Ley- de la Dirección General de Coste de Personal del Ministerio de Hacienda. También se declara una infracción muy grave por tratamiento de datos especialmente protegidos, en relación con el artículo 20 de la Lortad, del Ayuntamiento de Alco-

bendas; además aquí hubo que decretar una medida cautelar. Este tema fue verdaderamente bochornoso porque se estaban recabando datos de los ciudadanos por la Policía municipal sin la exigencia de la ley: que sea para una investigación concreta, donde se establecían referencias de origen racial, de enfermedades -no sé para qué servirá esto en la investigación policial-, creencias, etcétera. Afortunadamente, se adoptó una medida cautelar y el procedimiento ha terminado con una declaración de sanción muy grave. Asimismo se declara una infracción muy grave por cesión de datos al departamento de Servicios Sociales de la Diputación Foral de Guipúzcoa por esta transferencia a diversos ayuntamientos. Se declara una infracción leve por vulnerar el principio de finalidad a la Consejería de Bienestar Social de la Generalidad Valenciana, a la que nos hemos referido antes, la fiesta de la tercera edad. También se declara una falta grave por vulneración del deber de secreto a la Agencia Estatal de Administración Tributaria, en un procedimiento distinto al que me he referido antes. Se declara infracción muy grave por cesión de datos sin consentimiento del Ayuntamiento de Palma de Mallorca y del Ayuntamiento de Santa Cristina de la Polvorosa. Se declara una infracción grave por tratamiento de datos sin consentimiento del Ayuntamiento de Albacete. Por falta de inscripción han sido sancionados como falta leve los ayuntamientos de Ciempozuelos, Llanes, Fuentelamo, Rivas-Vaciamadrid, Marbella, etcétera.

Por la misma causa de no inscripción, pero ya como falta grave ante la reiteración y el incumplimiento, se sanciona al Ayuntamiento de Bujalance y al Ayuntamiento de Torreperogil. Por último, se han archivado diversas resoluciones en principio dirigidas contra el Ayuntamiento de Motril, el Banco de España, la Agencia Estatal de la Administración Tributaria, dos resoluciones de archivo. Éste es el panorama de actuación de la Agencia de Protección de Datos en cuanto a administraciones públicas en lo que va de año. Como verán, hay, por un lado, una preocupación de los ciudadanos en denunciar y, por otro lado, de la Agencia en tratar de conseguir que los datos no se cedan entre administraciones sin habilitación legal suficiente y, sobre todo, no se empleen para finalidades distintas. Vuelvo a insistir en que la finalidad es la que nos puede dar la pauta del buen actuar de las administraciones públicas. En algunas comunidades, tengo pensado organizar algunas jornadas para un mejor conocimiento por los funcionarios de las administraciones públicas de la Ley de Protección de Datos, que desgraciadamente aún sigue siendo desconocida en muchos aspectos y, por ello, en algunos casos infringida sin actitud especialmente dolosa.

En relación con estos temas de las administraciones públicas, a los que se refieren dos de las preguntas importantes, se encuentra el sistema TAIR, que ha sido especialmente analizado por la Agencia de Protección de Datos. En abril de 1998 se presentó ante la Agencia una denuncia relativa al incumplimiento de la Ley de Protección de Datos en la implantación por el Insalud del denominado

TAIR (Terminal Autónomo Identificativo del Paciente en las Recetas).

A ella se añadieron ulteriores denuncias presentadas en febrero y marzo de 1999. Tras la recepción de la primera denuncia, la Agencia inició las siguientes actuaciones para el esclarecimiento de los hechos: requerimiento al Insalud de información detallada sobre el amparo legal, objetivos y principales magnitudes del proyecto TAIR, incluidas sus fases de implantación; requerimiento de aclaraciones adicionales respecto de la confidencialidad de los datos a tratar y de las personas autorizadas para acceder a los mismos; tratamientos previstos por parte de los colegios farmacéuticos y especificación de los cesionarios; práctica de actuaciones inspectoras in situ en el Insalud, en el Colegio de Farmacéuticos de Madrid y en las empresas contratadas para la grabación de recetas, Cipsa y Veridata.

De las actuaciones practicadas se desprende que a partir del TAIR se generan dos flujos de información: a) Interno del Insalud, relativo a la actividad asistencial y recetas médicas, sin que se recoja en ellas el medicamento prescrito. En los centros de salud se realiza una explotación de dichos datos para la gestión asistencial y administrativa de los mismos; pacientes atendidos por consulta; pacientes derivados a especialidades; recetas entregadas a pacientes; partes de incapacidad laboral transitoria; solicitud de pruebas diagnósticas, etcétera, no saliendo dicha información fuera del entorno de dichos centros. El circuito interno de Insalud está implantado parcialmente, recogida de datos mediante el TAIR y volcado en los ordenadores de los centros de salud. Hay una implantación sólo parcial, encontrándose en fase de diseño y no operativa el resto del proyecto, que es el más relevante desde la perspectiva de la protección de datos. Sobre la implantación de las fases no operativas, la Dirección General del Insalud ha solicitado formalmente la colaboración de la Agencia de Protección de Datos, asumiendo el compromiso de mantenernos permanentemente informados. En cumplimiento del mismo, en diciembre de este año, el Insalud ha requerido la colaboración de la Agencia de Protección de Datos sobre nuevas aplicaciones que están siendo analizadas para garantizar la adecuación de la normativa de la protección de datos.

El otro flujo al que me refería, el apartado b), es externo al Insalud, relativo a la información generada por la receta médica, su grabación por los colegios farmacéuticos y su remisión posterior al Insalud. Este circuito está en funcionamiento y constituyó el objeto principal de la denunciada formulada, por lo que voy a centrar en él mi intervención. El TAIR genera una etiqueta para adherir a la receta que contiene datos del paciente, del médico, número de orden de la receta y la fecha de prescripción. Dado que el TAIR no recoge el dato relativo al medicamento prescrito, este es incluido en la receta de forma manual por el médico. Las oficinas de farmacia dispensadoras de los medicamentos recogen las recetas agregando físicamente el cupón precinto que contiene otro código de barras que corresponde al medicamento, así como los datos relativos a la propia farmacia.

Posteriormente las recetas son enviadas a los respectivos colegios farmacéuticos, donde generalmente a través de terceras empresas contratadas al efecto se graban en un CD-ROM para su envío mensualmente al Consejo General de Colegios Farmacéuticos.

Una de las innovaciones que ofrece el nuevo proyecto respecto de la grabación de recetas que se viene haciendo desde hace años, es la incorporación de la identificación del paciente mediante el código de identificación personal, CIP, incluido en la tarjeta sanitaria, identificación que con anterioridad se efectuaba escribiendo el nombre del paciente.

La única información identificativa personal que se puede grabar en los colegios farmacéuticos es el código de identificación personal -el CIP- de los pacientes y el código de identificación del área sanitaria -CIAS- que pertenece a los médicos.

La actuación de los colegios farmacéuticos se rige por el concierto firmado con fecha 17 de noviembre de 1998, concierto por el que se fijan las condiciones para la ejecución de la prestación farmacéutica a través de las oficinas de farmacia, que fue suscrito entre el presidente ejecutivo del Insalud y el director general de la Tesorería de la Seguridad Social, por una parte, y el presidente del Consejo General de Colegios Oficiales Médicos por otra. El concierto se rige por sus condiciones particulares, siendo de aplicación directa la normativa sanitaria por la que se regula la prestación farmacéutica en general y, en su caso, la de la Seguridad Social en particular, así como la Ley Orgánica 5/1992 de Protección de Datos, y resulta aplicable subsidiariamente la legislación reguladora de la contratación del Estado. La cláusula sexta del convenio garantiza la confidencialidad de los datos de carácter personal. Cualquier uso distinto de la facturación deberá ser autorizado por el Insalud. Los datos se graban en un CDROM por cada uno de los colegios farmacéuticos que, a través del Consejo General los entregarán a las dependencia del Insalud señaladas por éste. En algunos casos los colegios farmacéuticos proceden a contratar la grabación de datos, obligando a las empresas a salvaguardar la identidad y el secreto de los mismos, de acuerdo con las instrucciones de cliente y lo que establece al respecto la legislación vigente.

En la resolución del director de la Agencia de Protección de Datos de 24 de abril de 1999, se acuerda el archivo de las actuaciones en relación con el tratamiento de datos de las recetas. Los fundamentos de la resolución de archivos son sintéticamente los siguientes: A) Norma habilitante para realizar el tratamiento automatizado de datos.

Según se desprende de las actuaciones practicadas por la inspección, las únicas novedades derivadas de la introducción del TAIR consisten en la incorporación a la receta del código de identificación personal del paciente, CIP, en texto y en código de barras y en la impresión en código de barras del código de identificación de asistencia sanitaria, CIAS, correspondiente al médico, dato que ya se incluía con anterioridad en la receta. La norma habilitante para la creación de ficheros automatizados del Ministerio de Sanidad y de sus organismos autónomos es la Orden Ministerial de 21 de julio de 1994.

En ella se contempla un fichero específico de usuarios nacionales de la tarjeta sanitaria, inscrito en el Registro General de Protección de Datos que comprende, en el apartado relativo a finalidad y usos, el correspondiente a la gestión y control sanitarios. Las personas o colectivos afectados son todos los usuarios del Sistema Nacional de Salud y los organismos oficiales de estadística. De lo expuesto se desprende que la novedad del TAIR, en lo que se refiere al tratamiento de nuevos datos del usuario del Sistema Nacional de Salud y, en particular, de personas con derecho a prestación farmacéutica, se limita a la incorporación relativa al CIP -código de identificación personal-, contenida en la TSI, tarjeta sanitaria individual. El nuevo tratamiento de datos de titulares del TSI tiene habilitación normativa, puesto que es subsumible en el fichero de usuarios nacionales de tarjetas sanitarias, incluidos en la Orden de 21 de julio de 1994 a la que me he referido.

B) El consentimiento de los afectados, otro de los temas que trata a la resolución. En lo que se refiere al consentimiento de los afectados para la obtención de datos personales, la regla general del artículo 6 de la Lortad es la exigencia del mismo, salvo que la ley disponga otra cosa. Sin embargo, el apartado 2 de dicho precepto exceptúa la obtención del consentimiento de los afectados cuando los datos se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias. Dado que el artículo 85 de la Ley de Medicamento exige que la receta contenga los datos básicos de identificación del paciente y que tales se han asociado a los contenidos en el TSI, debe estimarse que la Administración sanitaria está actuando en el marco de sus competencias y que la recogida y el tratamiento de datos que figuran en la TSI son adecuados, pertinentes y no excesivos en relación a aquéllas, conforme al artículo 4 de la Lortad, por lo que cabe prescindir del consentimiento del afectado, de acuerdo con lo que señala el artículo 6.2 de la Lortad.

C) Tratamiento automatizado de datos. El artículo 8º de la Ley de Protección de Datos habilita para proceder al tratamiento automatizado de datos personales relativos a la salud de las personas que acudan a las instituciones y centros sanitarios o hayan de ser tratadas en los mismos, siempre que dicho tratamiento se realice de acuerdo con la normativa sanitaria. Dado que los aspectos actualmente operativos del proyecto TAIR se limitan a la grabación de los datos incorporados en las recetas, con la finalidad de efectuar su facturación y el control de ésta, y no a otros desarrollos pendientes en los términos expuestos en los antecedentes de hecho de la resolución, la habilitación para el tratamiento de datos por parte de la Administración sanitaria encuentra su fundamento en los artículos 85, 95, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento.

D) El concierto suscrito entre el Insalud y la Tesorería de la Seguridad Social y el Consejo General de Colegios Oficiales de Farmacéuticos. El artículo 97 de la Ley del Medicamento, que regula la colaboración farmacia-Sistema Nacional de Salud, destaca la calificación de las oficinas de farmacia como establecimientos sanitarios, el deber de colaboración que se les impone para garantizar el uso racional de los medicamentos y la posibilidad de ser objeto de concertación en cuestiones distintas de las obligaciones legales que se les imponen. Por su parte, la Ley 21/ 1974, de 13 de febrero, de Colegios Profesionales, configura a estas corporaciones como de derecho público, y se les atribuye la representación de la profesión y el ejercicio de las funciones que les sean encomendadas por la Administración.

La Ley de Colegios Profesionales regula los consejos generales de los colegios como corporaciones de derecho público con personalidad jurídica propia y plena capacidad. Entre sus funciones incluye la de los propios colegios en cuanto tengan ámbito o repercusión nacional, artículos 1, 5 y 9. Atendiendo a las normas citadas, debe estimarse que las actuaciones que el concierto exige de los colegios profesionales en las recetas constituye un supuesto de cesión de

datos entre administraciones públicas, conforme al artículo 19 de la Lortad.

E) Participación de empresas privadas en la grabación de datos. Esta actividad se encuentra amparada en el artículo 27 de la Lortad, que prevé la posibilidad de realizar el tratamiento de datos personales por cuenta de terceros, siempre que cumplan las garantías de dicha norma y, en particular, la confidencialidad.

Para concluir, he de señalarles que la Agencia de Protección de Datos tiene una especial sensibilidad en el tratamiento de datos especialmente protegidos, como son los relativos a la salud. Como manifestaciones concretas de dicha preocupación, la Agencia iniciará a principios del próximo año actuaciones inspectoras sobre la ejecución del convenio en relación con el tratamiento de datos personales. Asimismo velará, como señalé al principio, para que continúen desarrollándose las actuaciones de colaboración con el Insalud para el desarrollo posterior del proyecto TAIR, a fin de que este se adecue a las exigencias derivadas de la normativa de protección de datos.

Esto es, en resumen, lo que puedo informar de un tema que es complejo, como es el sistema TAIR, que, como ven SS. SS., sólo tiene desarrollada una parte. Esa parte es absolutamente correcta. En cuanto a próximos desarrollos, tenemos el compromiso del Insalud, que ya nos ha pedido la colaboración para que velemos por la protección de la intimidad en esos desarrollos.

El señor PRESIDENTE: Tiene la palabra el señor Navarrete.

El señor NAVARRETE MERINO: Señor director de la Agencia de Protección de Datos, la obtención, el tratamiento de datos, y en su caso, la cesión de los datos por parte de las administraciones públicas dista de ser un tema pacífico, lo cual no nos exonera a los legisladores ni a los que forman parte de las administraciones públicas de aplicar criterios de racionalidad en la interpretación de los preceptos legales. Desde el punto de vista de la racionalidad, se ha querido convertir algunas veces a las administraciones públicas en rehenes de la Ley Orgánica de Protección de Datos Personales. Las administraciones públicas tienen al menos tantos derechos como los titulares de ficheros privados, yo diría que algún derecho más que estos últimos. Lo reconocía el proyecto de directiva, lo reconocía la Lortad y lo viene a reconocer actualmente la Ley Orgánica de Protección de Datos, con un sistema que a veces produce una cierta ambig¸edad o una cierta perplejidad. Por supuesto, hay una serie de funciones, como bienestar, Seguridad Social, represión de los delitos, etcétera, que constituyen títulos habilitantes para las administraciones públicas parala recogida y el tratamiento de datos.

En las dos leyes que ha habido sobre esta materia en nuestro país se exceptúa del consentimiento la recogida de datos por las administraciones públicas, cuando son precisos para el cumplimiento de sus finalidades. La cesión de datos entre las administraciones públicas también se trata con benevolencia por todas las disposiciones normativas, incluidas las de la Unión Europea, cuando se trata de finalidades legítimas de las administraciones públicas.

Por consiguiente, habría que ir elaborando unos criterios que faciliten la cooperación interinstitucional. Yo apunto uno de estos criterios, que por otra parte se reconoce en el ámbito del derecho privado: que las administraciones públicas, al menos las de la misma naturaleza, tienen la misma personalidad jurídica, lo que convierte en un exceso ling¸ístico que un ministerio ceda a otro un dato, porque en ese caso no nos hemos salido de la misma personalidad jurídica.

Por otra parte, habría que ser restrictivos en una serie de cuestiones. En mis anteriores intervenciones apuntaba una idea: Los tratamientos por cuenta de un tercero, realizados por particulares, cuando el tercero son las administraciones públicas, debieran ser contemplados restrictivamente por éstas y por la misma Agencia de Protección de Datos.

Es más, las ciencias administrativas vienen buscando desde hace tiempo distintas fórmulas para que las actuaciones sean lo más ágiles y lo más eficaces posibles y el ciudadano no sea como un paciente que es sometido a inyecciones cada quince minutos. En ese sentido, figura en multitud de programas electorales la idea de que no se moleste al ciudadano pidiéndole datos que ya están en poder de las administraciones públicas, lo cual comporta la legitimidad de ciertas cesiones, introducidas alguna vez de una manera más universal en nuestro derecho, como la aportación de documentos que figuran en ficheros de las administraciones públicas.

Estos temas, por el carácter de sensibles o de especialmente protegidos que tienen los datos de salud, requieren una actuación mucho más meticulosa por parte de las administraciones públicas y por parte de la autoridad de control que existe en el derecho español, que es la Agencia de Protección de Datos. Incluso habría que decir que, desde el punto de vista del tratamiento que experimentan algunos datos sanitarios, estamos ante una administración primaria, instintiva o casi zoológica; no voy a emplear el término cateta, porque tengo una gran consideración a las personas que habitan en los pueblos. La administración reduce el problema de las historias clínicas a un puro problema de almacenamiento. ¿Para qué sirven las historias clínicas? A mí me gustaría que la administración sanitaria fuera al menos tan consciente como yo, que soy un profano en esta materia, de que las historias clínicas sirven para muchas más cosas que para guardarlas en unos almacenes en los que se espera que la polilla termine dando cuenta de ellas. Excepcionalmente, de vez en cuando se piden a esos remotos almacenes, en poder de particulares, tres o cuatro historias clínicas.

Las historias clínicas son extraordinariamente relevantes desde el punto de vista del seguimiento de la eficacia de los medicamentos, desde el punto de vista de la investigación de las relaciones concomitantes que existen entre las características de determinadas personas y el efecto que sobre ellos producen determinados medicamentos y desde el punto de vista de control sanitario.

No hay problemas de espacio en la era de los ordenadores. Resulta ridículo que la polémica que existe se monte sobre la cuestión de que la administración sanitaria en los hospitales no tiene el suficiente número de metros cuadrados para

guardar las historias clínicas. Como estoy tratando de indicar desde el principio, las historias clínicas sirven para algo más que para ser conservadas. Son como la propia historia de la vida y del futuro, y no es concebible una administración sanitaria moderna que no exprima, no saque todo su jugo a esas historias clínicas que alguna persona lúcida en un momento determinado decidió que valía la pena conservarlas. Desde el punto de vista del grupo parlamentario al que represento, aunque no estén presentes mis compañeros de otros territorios del Estado, debo decir que nos gustaría que las historias clínicas fueran informatizadas, conservadas dentro de los ordenadores, y así sería extraordinariamente fácil que pudieran ser tratadas y sacar multitud de consecuencias beneficiosas para la salud, tanto individual como colectiva de los españoles.

Respecto a vista de las recetas, hay que decir que los colegios profesionales -yo pertenezco a alguno de ellos también- no sólo tienen una finalidad de carácter público, sino también privado.

Algunos son muy mercantiles. Durante mucho tiempo se ha considerado que el tema de la distancia entre farmacias afectaba a centros sanitarios y, por tanto, debían ser objeto de una contemplación restrictiva y verdaderamente excepcional por el derecho; restricciones que no se aplican, por ejemplo, a los bufetes de los abogados ni a los estudios de los arquitectos, pero existía esa consideración sanitaria. Algunos sostenían que simultáneamente era muy importante la finalidad mercantil, no despreciable, no lo digo en un sentido despectivo, que coexiste con lo anterior.

Entre estos criterios que estoy intentando defender, que debieran aplicar las administraciones públicas, está no sólo el tema de la contemplación restrictiva de los trabajos encargados a terceros, sino también la transmisión de los datos nominales, que según la legislación son de carácter personal. Si la Administración quisiera estar más de acuerdo con la tónica de nuestro tiempo, la eficacia igualmente se podría conseguir en multitud de casos sanitarios mediante la disociación del contenido, por ejemplo, de las recetas respecto del nombre y apellidos del que va a ser el destinatario de sus efectos farmacológicos. Desde luego no puedo dar por válido el argumento de que no hay dato personal, porque los mismos han sido reconducidos a un código de barras, a la mención más o menos crítica del CIF o del área sanitaria correspondiente.

Debo recordar que el artículo 3 de las dos leyes de protección de datos que ha habido en nuestro país, al definir los términos, considera como datos personales la información que hace a la persona no sólo identificada sino también identificable. El número del carnet de identidad, el número del CIF, el número del área sanitaria o cualquier otro jeroglífico descifrable hace a la persona identificable, por lo que estamos en el ámbito de lo que prohibe o permite, según los casos, la Ley Orgánica de Protección de Datos.

Quiero apuntar un tercer tema y con esto voy a concluir, que es el de los datos genéticos, que de vez en cuando aparecen en la polémica periodística. Son de extraordinaria importancia, y como la técnica susceptible de un doble uso: uno, adecuado y, otro, inadecuado.

De momento, el Grupo Parlamentario Socialista en esta comparecencia lo que quiere hacer es una llamada de atención sobre la necesidad de que la administración sea más cauta en el manejo de las recetas y de los historiales clínicos, que estudien a fondo el tema de los datos genéticos. Por último, mostrarnos nuestra insatisfacción por el sistema de recetas implantado, más o menos totalmente, tanto en el ámbito interno de Insalud como en el ámbito público, puesto que las comunidades autónomas -que algunos tan recientemente han vituperado- no siguen el mismo sistema que el Insalud, porque además se puso en marcha un procedimiento sin la oportuna cobertura legal. Como consecuencia de ello se dictó una orden ministerial que ha sido modificada en dos ocasiones. Por tanto reprobamos , en la forma que podemos hacerlo en esta sesión, los procedimientos que se están siguiendo por el Insalud, tanto en materia de historiales clínicos, como en materia de recetas.

El señor PRESIDENTE: ¿Grupos no solicitantes de la comparecencia que desean manifestar su punto de vista? (Pausa.) Tiene la palabra el señor Castellano.

El señor CASTELLANO CARDALLIAGUET: Con toda brevedad, porque nuestro grupo puede exigir de la Agencia de Protección de Datos, que hoy comparece a través de su digno director, aquello que la ley le faculta, pero evidentemente no creemos que podamos exigir de la Agencia que tenga capacidad para reformar las pautas de comportamiento del resto de las administraciones. Como mucho podrá tener una capacidad de sugerencia. En consecuencia, no nos queda más que agradecer al director de la Agencia de Protección de Datos, en lo que se refiere a estos últimos tres puntos del orden del día, que no se haya dado cuenta de cuáles son las medidas que puede tomar y que evidentemente no pueden tener un carácter previsor; tienen más bien, como es lógico y natural un tratamiento a posteriori y una vez que se haya descubierto cuál es el uso que se hace.

Acabo pura y simplemente, señor presidente, manifestando la satisfacción que este diputado ha tenido, en nombre de Izquierda Unida, de pertenecer a una Comisión Constitucional como ésta, tan sabia y rectamente presidida por don Gabriel Cisneros. Agradezco también al letrado que la asiste el conjunto de inmerecidas deferencias de que por lo menos a mí me ha hecho objeto, así como a todos y cada uno de los miembros de la Comisión Constitucional y a sus portavoces la colaboración con la que han podido suplir las indudables e inocultables deficiencias que han guiado la actitud de esta parlamentario. Tengo que culminar, como es lógico y natural, no faltaría más, deseándoles a ustedes, primero, que tengan unas felices fiestas, que tengan un soberbio milenio y, a ser posible, lleguen ustedes al año 3000 y, como dicen en tono coloquial, larga vida y mejor fortuna. Si las listas de las respectivas organizaciones no les han dado a ustedes la suficiente hospitalidad, cual sería exigible por sus méritos, que se las dé a ustedes la del Servicio Nacional de Loterías que sería mucho más productiva.

El señor PRESIDENTE: Muchísimas gracias, don Pablo. Pensaba dar término a mi intervención con una referencia tan

cumplida como S.S. merece en torno a su indeseable abandono de las tareas parlamentarias, desde luego de esta Comisión Constitucional, que se ha honrado contándole entre su miembros y ha auxiliado a la Presidencia con tanta eficacia como amistad en la rectoría de la Mesa de esta Comisión. ¿El Grupo Parlamentario Popular va a fragmentar el breve tiempo de que dispone con dos intervenciones? (Pausa.) Don Cesar Villalón tiene la palabra.

El señor VILLALÓN RICO: Señor presidente, voy a intentar ser breve.

Quiero agradecer al director de la Agencia de Protección de Datos su comparecencia y también alegrarme de que se hayan debatido estas tres comparecencias, una que era de la cesión ilícita de datos personales por parte de las administraciones públicas y las otras dos de lo que podía ser el ámbito sanitario.

El director de la Agencia ha puesto de manifiesto lo que han sido ciertas irregularidades por parte de las administraciones públicas, tanto locales, como autonómicas e incluso de la Administración central del Estado -ha hablado de centros penitenciarios y otros datos- y ha puesto de manifiesto que la Agencia funciona conforme está establecido en la ley y con el control que los ciudadanos requerimos de la misma.

Me voy a remitir casi escuetamente a lo que ha sido un poco la intervención del portavoz del Grupo Socialista sobre temas de datos en el ámbito sanitario. La intervención que ha tenido el director de la Agencia sobre el TAIR creo que ha quedado clara. Ha acudido a los datos, a todo el estudio que se ha hecho. Me gustaría decir que estas dos solicitudes de comparecencia sobre temas sanitarios y controlados por la Agencia de Protección de Datos ya habían sido debatidas en esta Cámara, tanto en la Comisión de Sanidad como en el Pleno del Congreso, a través de varias interpelaciones, y en su momento por el ministro de Sanidad y por los altos cargos del Ministerio ya se dieron las respuestas oportunas. Como me da la sensación de que a la hora de hablar del TAIR el director de la Agencia ha dado unos datos que son una referencia explícita de cómo se han llevado a cabo por parte del Insalud, que es un servicio de salud de una parte del Sistema Nacional de Salud, tiene razón el señor Navarrete cuando decía que no se hace en todos los sitios igual. Esa es la autonomía de gestión que hace el Insalud y que otros servicios de salud no consideran oportuno. Pero le tendría que hacer una matización, y es que no hay posibilidad de utilizar los datos a través de este sistema del TAIR, de la misma forma que a lo largo de muchos años no ha habido la posibilidad de utilizar los datos con las clásicas recetas de la Seguridad Social, donde figura el diagnóstico, el nombre del paciente, el número de la Seguridad Social, y nadie se

había planteado hasta este momento que por esas recetas normales se pudiera utilizar, que es lo que pasa en otros servicios de salud.

Dicho esto, que además, como ha dicho el señor Fernández, por parte del Insalud ha habido una buena predisposición para seguir trabajando en hipotéticas cuestiones que puedan afectar a lo que son los derechos constitucionales de los ciudadanos españoles, a mí me parece que hay que hacer una referencia explícita al último punto, que era a solicitud del Grupo Mixto -el portavoz del Grupo Socialista también ha hecho referencia a él-, que es el de las historias clínicas. Aquí hay que decir dos cosas: si hay una preocupación, que podría ser por parte del Grupo Socialista, por mantener los derechos constitucionales que marca el artículo 18 de la Constitución, nosotros somos los primeros y estaremos seguramente al mismo nivel que el Grupo Socialista, no queremos ser ni más ni menos defensores de los derechos constitucionales; pero si la preocupación es por la custodia en sí misma de las historias clínicas, por si es una empresa privada fuera de un ámbito público, como puede ser un centro hospitalario, la intervención del señor Navarrete está algo equivocada. Lo digo porque los datos que nosotros tenemos son de algunas inspecciones que ha hecho la Agencia en relación con varios hospitales que tienen estas historias clínicas en depósito a través de empresas privadas, pero no son patrimonio de los hospitales del territorio Insalud, en este caso de los hospitales más conocidos por todos en Madrid, como puede ser el Doce de Octubre o el Ramón y Cajal, sino que hay hospitales en Andalucía que hacen lo mismo; los hospitales de Granada y Córdoba hacen lo mismo que estos hospitales.

¿Por qué? Entiendo que, aunque guiado de buena fe y de ese afán de reservar los derechos constitucionales de los españoles, usted ha cometido algunos errores, seguramente por un desconocimiento de lo que es el ámbito sanitario. Las historias clínicas sirven para muchas cosas. Pero ¿qué historias clínicas son las que están reservadas y se archivan en alguna empresa privada, con la seguridad de la Agencia de que hay confidencialidad de datos, según está establecido en el contrato? Las que se llaman historias clínicas pasivas. ¿Qué quiere decir eso? Que seguramente hace ya bastantes años los enfermos no han ido a ese centro por muchas circunstancias, porque han fallecido, porque en un momento dado acudieron a él y ya no han vuelto. La relación puede ser diversa, esa es la gran mayoría, no todas, bien es verdad.

Por otra parte, en todos los sitios se ha puesto eso de manifiesto.

Ya le ponía el ejemplo del hospital de Córdoba y el clínico de Granada, que hacen lo mismo que en los hospitales del Insalud; dos servicios de salud, el Insalud por un lado, que depende directamente del Ministerio de Sanidad, y un servicio de salud, el SAS de Andalucía, que hace lo mismo, que depende de un gobierno de una comunidad autónoma de distinto color político. Por lo tanto, vea usted lo que es la gestión en las historias clínicas.

Le voy a leer también lo que la junta técnico-asistencial del hospital Doce de Octubre dice: Hay que mejorar el archivo de las historias clínicas. Yfirman varios miembros de la junta técnico- asistencial del hospital. Y el presidente de la comisión de historias clínicas dice: Mejorar la situación del archivo. Insistimos y deseamos que este proyecto se realice lo antes posible, dada la vital importancia del archivo en el funcionamiento del hospital. Incluso, esta comisión elabora un documento donde dice cómo podrían archivarse estas historias clínicas. Las historias clínicas se pueden archivar, como usted ha dicho, a través de los sistemas modernos de los ordenadores, pero también son unos documentos

-porque hay historias clínicas desde hace muchos años- difíciles de archivar. Imagínese usted los años que lleva funcionando, por ejemplo, el hospital La Paz.

Aquí no hay un debate propiamente dicho de lo que es la preocupación por los derechos constitucionales, el derecho de todos los españoles a tener la confidencialidad de los datos; el debate se plantea sobre si es una empresa privada o una empresa pública, en este caso un centro hospitalario, quien archiva esos documentos. A mí me parece que si se mantienen los controles que la Agencia de Datos establece, los ciudadano podemos estar tranquilos. Todo aquellos objetivos para los que se usan las historias clínicas, van a estar asegurados, no sólo desde el punto de vista de los tratamientos, sino de la investigación, de lo que pueden ser estudios epidemiológicos. Todos esos temas están asegurados si las historias están bien archivadas y bien ordenadas, cosa que en algunos hospitales es difícil porque no tienen espacio material para hacerlo. Son algunas de las cuestiones que había que puntualizar para tranquilidad del señor diputado y del grupo al que representa.

El señor PRESIDENTE: ¿Algún comentario, señor director?

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Por mi parte, como también estaba entre las previsiones de mi comparecencia que lo fuera para explicar el tema de las historias clínicas, si quiere, brevemente lo explico, porque también ha sido analizado por la Agencia de Protección de Datos.

El señor PRESIDENTE: Tiene tres minutos.

El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Atendiendo iniciativas parlamentarias y noticias de los medios de comunicación social y algunas denuncias, se ha examinado el tema de las historias clínicas inspeccionando el hospital Doce de Octubre, de Madrid; el hospital de Cabueñes, de Gijón; el hospital provincial de Castellón; el hospital Clínico Universitario, de Valencia; el hospital universitario, La Fe, de Valencia; el hospital Nueve de Octubre, de Valencia, el hospital de Sagunto; el hospital psiquiátrico provincial Padre Jofré, de Betera, el complejo hospitalario provincial de Pontevedra y el Servicio gallego de detección precoz de cáncer de mama. Excepto el hospital Clínico de Valencia, el complejo hospitalario provincial de Pontevedra y el Servicio gallego de detección precoz de cáncer de mama, las otras inspecciones han quedado terminadas. Ello ha dado motivo a resoluciones de archivo, por cuanto que las historias clínicas se encuentran documentadas en soporte papel, sin que se produzca tratamiento automatizado dedato alguno, por lo cual es ajeno a la protección de la Lortad en cuanto a la no existencia de datos informatizados. Las empresas adjudicatarias de la gestión se limitan a establecer un sistema de control de entradas y salidas de las historias clínicas. No manipulan las historias clínicas y el tratamiento automatizado que realizan se limita a la gestión de acceso y control de las historias, es decir, nombre apellidos y números de la historia clínica, sin que traten datos de salud . Esta actividad de estas empresas está totalmente acorde. En los concursos públicos está así garantizada la confidencialidad y es acorde con el artículo 27 de la Lortad. Por eso los expedientes han sido archivados.

El señor PRESIDENTE: Muchas gracias, señor director.

Señora Uría, señor Navarrete, señor Villalón, señor López-Medel, señor Vera, señor letrado, lo reducido del elenco de asistentes nos permite despedirnos nominativamente de todos y cada uno de las señoras y señores diputados presentes en la sala. Ya don Pablo Castellano ha puesto un punto de emoción en sus palabras de despedida, de suerte que a mí no me cabe sino subrayarlas, poniendo de manifiesto que ha sido para esta Presidencia un gran honor el poder presidir los trabajos de la Comisión Constitucional a lo largo de esta legislatura que ya se extingue. Deseo la mejor fortuna a todos ustedes. A los señores funcionarios de la Cámara, al señor letrado y a los señores taquígrafos que nos han asistido con su trabajo, quiero desearles muy felices pascuas, y obviamente a los señores parlamentarios que encuentren, como nos deseaba el señor Castellano, la más hospitalaria acogida en las listas de nuestros respectivos partidos o, en su defecto, que Dios reparta mañana suerte.

Muchas gracias y muy felices pascuas.

Se levanta la sesión.

Eran las nueve y treinta minutos de la noche.

MEMORIA DE 1999 - ANEXO V - COMPARECENCIA DEL DIRECTOR DE LA AGENCIA EN EL SENADO

CORTES GENERALES
DIARIO DE SESIONES DEL SENADO
COMISIÓN ESPECIAL SOBRE REDES INFORMÁTICAS

Presidencia del Excmo. Sr. D. Pedro Calvo Poch

Celebrada el jueves, 29 de abril de 1999

COMPARECENCIA DEL DIRECTOR DE LA AGENCIA DE PROTECCION DE DATOS (713/000766).

El señor PRESIDENTE: Reanudamos la sesión dando la bienvenida a don Juan Manuel Fernández López, Director de la Agencia de Protección de Datos, a quien quiero agradecer especialmente su comparecencia en la medida en la que, primero, le avisamos con poco tiempo de antelación y no puso ningún problema y luego le cambiamos el día de la comparecencia y tampoco puso ningún problema. Sabemos de sus múltiples ocupaciones y, por lo tanto, quería agradecerle especialmente el esfuerzo que ha realizado.

Sin más, para informar sobre la materia objeto de esta Comisión, tiene usted la palabra.

El señor DIRECTOR DE LA AGENCIA DE PROTECCION DE DATOS (Fernández López):

Muchas gracias, señor Presidente.

Buenos días a todos, señorías. Es para mí una satisfacción el poder comparecer ante esta Comisión porque ello demuestra la sensibilidad de sus señorías por la protección del derecho a la intimidad, que garantiza la Agencia Española de Protección de Datos.

Como conocen sus señorías, el artículo 18 de la Constitución proclama el derecho a la intimidad y el 18.4 señala especialmente que ésta se ha de mantener ante los peligros que supone el tratamiento por parte de los nuevos medios informáticos y telemáticos.

En el ámbito europeo, el Convenio 108 del Consejo de Europa y posteriormente la Directiva 95/46 vienen a recoger toda una normativa detallada en la que se establece el desarrollo de la protección de la intimidad de los ciudadanos. La Ley española que desarrolla el artículo 18 de la Constitución, la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, nace ya con los principios de protección de datos que proclama la Directiva comunitaria, pues si bien la Ley española es anterior en el tiempo a la Directiva, se tuvieron en cuenta los trabajos llevados a cabo en el seno de la Unión Europea y además las propuestas que contenía la propuesta de directiva, de ahí que prácticamente nuestra Ley nazca con la mayor parte de los principios y garantías ya incorporados. Como saben, ahora se encuentra tramitándose en el Congreso el proyecto de ley que terminará de incorporar, aunque son sólo cosas de matiz, la Directiva comunitaria.

Los principios en la recogida de datos personales contenidos tanto en la Directiva como en la Ley española son --resumiéndolo mucho-- los siguientes. En primer lugar, la calidad de datos, que éstos han de ser adecuados, pertinentes y no excesivos, y su uso deberá ser exclusivamente para las finalidades para las que fueron recabados; los datos han de ser exactos, puestos al día y se cancelarán cuando dejen de ser necesarios.

El segundo principio es el derecho a la información en la recogida de datos. Aquellos a los que se les soliciten datos deberán ser informados de la existencia de ficheros, del carácter obligatorio o facultativo de sus respuestas, y de la posibilidad del ejercicio de los derechos de acceso, rectificación y cancelación de los mismos.

El tercer gran principio trata del consentimiento del afectado. Salvo excepciones tasadas, no se recogerán datos sin dicho consentimiento. En cuanto a las excepciones, se refieren a la relación negocial y al supuesto de que los datos se recojan de fuentes accesibles al público.

Nuestra ley, al igual que la directiva, se ocupa de los datos especialmente protegidos, de los datos sensibles, como la ideología, religión, creencias, origen racial, salud y vida sexual, para los cuales se exige, sin lugar a dudas, el consentimiento expreso y escrito del afectado.

Unicamente deberán incorporarse a la nueva ley los datos referentes a los sindicatos, que no estaban contemplados en la ley vigente, pero sí, en cambio, en la directiva comunitaria, como datos especialmente sensibles.

Un tema de gran trascendencia es el relativo a la cesión de esos datos.

En este sentido, sólo se podrán ceder para el cumplimiento de los fines directamente relacionados con las funciones del cedente y el cesionario.

Para ello se precisará el consentimiento del afectado, no siendo preciso el mismo cuando una ley prevea otra cosa, se trate de datos de fuentes accesibles al público, o si la cesión se deriva de una relación jurídica o negocial. Y también de

forma excepcional, no será necesario cuando se dé traslado de los datos al Defensor del Pueblo, los fiscales o los jueces, en el ejercicio de sus funciones.

En cuanto a la cesión de datos entre las administraciones públicas, no podrán cederse de unas a otras para el ejercicio de competencias diferentes o relacionadas con materias distintas. Por excepción, también contemplada en el artículo 19 de nuestra vigente ley, la cesión se podrá llevar a cabo cuando esté prevista en la disposición de creación del fichero o en otra disposición posterior.

Estos son, en general, los principios fundamentales del tratamiento de los datos que se recojan de los ciudadanos.

En el marco de la Unión Europea, y por mandato del artículo 29 de la propia directiva, todas las autoridades encargadas de la protección de datos en estos países nos reunimos con el fin de establecer posiciones comunes para el desarrollo de los principios que les he señalado, y que constan en la directiva.

Señorías, las nuevas tecnologías están formando parte de nuestra realidad social, y eso es algo que el Derecho no puede desconocer. No podemos permitir que no se encuentren soluciones satisfactorias para los problemas jurídicos nacidos de la falta de adecuación del Derecho a las normas de comportamiento de la sociedad de la información. En un sistema mundial, la aplicación territorial del Derecho puede quebrarse. Cualquier hecho que ocurra en la red tiene consecuencias en cualquier parte del mundo. La frontera entre los aspectos públicos y privados de la información que se encuentra en una red es difícil de diferenciar y a veces muy fácil de confundir. Por tanto, será necesario establecer medidas técnicas que garanticen la confidencialidad de los datos. La tecnología digital, a diferencia de la analógica, permite aplicar una serie de sistemas para identificar, cifrar, y con ello preservar, los derechos de cada ciudadano o usuario de la red que tengan relación con su intimidad.

En este aspecto, la Directiva 97/66, relativa al tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones, en particular, en la red digital de servicios integrados y las redes móviles digitales públicas, considera que ante la aparición de las redes digitales públicas avanzadas de telecomunicaciones se tienen que crear normas específicas en materia de protección de datos.

Por lo que se refiere a nuestro Derecho interno, la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la citada Ley, vienen a incorporar la directiva comunitaria en materia de telecomunicaciones a la que me he referido.

No voy a aburrir a sus señorías con una descripción completa de la ley, por lo que simplemente me voy a limitar a señalar aquellos aspectos que puedan tener más trascendencia. Así, el artículo 14, relativo a las guías telefónicas, restringe la publicación del número del abonado que haya manifestado su oposición a figurar en la misma. El artículo 55, sobre el servicio de información de la guía telefónica, establece que no se incluirán los datos de los abonados que se hayan opuesto a figurar en las guías telefónicas.

En cuanto al Título V de la ley, sobre la protección de datos personales en la prestación de los servicios de telecomunicaciones, es donde más ampliamente se desarrollan los principios protectores. El artículo 62 establece las normas de carácter técnico en relación con la protección de datos en las explotaciones de redes y la prestación de servicios en telecomunicaciones. Y el artículo 63, sobre el régimen jurídico, señala que la protección de los datos personales vinculados a las redes y servicios de telecomunicaciones se regirá por lo dispuesto en la Ley Orgánica de Protección de Datos, de conformidad con el artículo 50 de la propia Ley General de Telecomunicaciones. Los operadores con licencia individual o con autorización general para la prestación de servicios de telecomunicaciones disponibles al público, o los que exploten redes públicas de telecomunicaciones, deberán garantizar la protección de los datos personales en el ejercicio de su actividad. Los operadores prestadores de servicios deberán tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios. Estas medidas se tendrán que adoptar en colaboración con el operador de la red pública.

Por lo que respecta al ámbito de aplicación de toda esta normativa, se contiene en el artículo 64, y hace referencia al tratamiento de datos personales en la prestación de los servicios de telecomunicaciones disponibles al público y en la explotación de las redes públicas de telecomunicaciones.

Por otro lado, el artículo 68, relativo al supuesto de llamadas no solicitadas para fines de venta directa, establece que no podrán realizarse llamadas automáticas --es decir, aquellas sin intervención humana-- o por fax con fines de venta directa a aquellos abonados que no hayan dado su consentimiento al efecto.

El artículo 69 se refiere a la prestación y restricción de la línea llamante y la línea conectada. Y el artículo 70 trata de la supresión en origen de llamada a llamada, lo que ha sido desarrollado por una resolución de 2 de diciembre de 1998, por la que se atribuye el código 067 al servicio de supresión en origen llamada a llamada, de identificación de la línea llamante. Esto aún no se ha puesto en funcionamiento, por lo cual, la Agencia de Protección de Datos se ha dirigido al respecto al Director General de la Compañía Telefónica de España, y está previsto que comience a funcionar en el próximo mes de julio.

Un artículo también interesante --y no les canso más, es el último que les cito-- es el 79, que trata de la responsabilidad de los operadores que tengan sus redes interconectadas. La relación de países a los que puede ser enviada información sobre la identidad de la línea llamante se establecerá por la Secretaría General Técnica de Comunicaciones, previo informe de la Agencia de Protección de Datos, pendiente también de desarrollo.

Por lo que respecta a las actividades llevadas a cabo por las autoridades europeas en materia de control de datos a través de la reunión del Grupo del Artículo 29, respecto a Internet, se han elaborado ya varios documentos que me he atrevido a traer para dejar a disposición de sus señorías porque creo que pueden ser útiles. Les resumo los siguientes.

En la XII reunión del Grupo del Artículo 29 se acordó la creación de un grupo de trabajo denominado «Task Force Internet» con objeto de estudiar la aplicación de las Directivas 95/46 y la 97/66 al tratamiento de datos en Internet. El Grupo del Artículo 29 ha comenzado también a tratar cuestiones relacionadas con la aplicación de los principios de protección de datos, cuestiones relacionadas con Internet de modo práctico y en función de la urgencia de los problemas surgidos en el ámbito europeo e internacional. Aquí se trata, principalmente, de lo siguiente: del anonimato en Internet, de un primer informe sobre el proyecto P3P del Consorcio de World Wide Web, del administrador de la red de Internet, y de los trabajos en curso sobre los problemas planteados por los programas que permiten la utilización de Internet.

En el contexto de la participación en la conferencia de comisarios europeos de protección de datos, que tuvo lugar en Dublín los días 23 y 24 de abril del año pasado, ya se puso de manifiesto el deseo de que el Grupo pudiera tratar estas cuestiones de manera más sistemática para precisar las posturas y soluciones con vistas a contribuir a un desarrollo de Internet y los servicios conexos que respeten el derecho a la vida privada.

Como consecuencia de los trabajos llevados a cabo en el Grupo «Task Force Internet», una de las novedades ha sido la aprobación de tres documentos en la XIV reunión. El primero, referido al tratamiento de datos de carácter personal en Internet; el segundo, la recomendación sobre el tratamiento automático e invisible en Internet y, el tercero, sobre el respeto a la privacidad durante las interceptaciones. Me voy a referir a ellos brevemente.

La finalidad del documento sobre el tratamiento de datos de carácter personal en Internet es que quede claramente establecido que tanto la Directiva 95/46, relativa a la protección de datos de carácter personal, como la Directiva 97/66, relativa al sector de las telecomunicaciones, se apliquen sin lugar a dudas a Internet. Este documento, como les digo, ya ha sido adaptado y lo tengo a su disposición.

En cuanto a la recomendación sobre el tratamiento automático e invisible en Internet, el Grupo de trabajo anima a la industria del software y del hardware a trabajar en productos que protejan la privacidad, que contengan las herramientas necesarias para cumplir con las reglas europeas de protección de datos. A título anecdótico, les puedo informar de que en una de las sesiones nos reunimos con los responsables de la empresa Intel por cuanto el Pentium III, a través de un número identificativo, podía ser considerado como vulnerador de la intimidad. Al final se llegó a un acuerdo y algo que es útil en algunos casos --como en el supuesto de que exista una transacción comercial, en la que es bueno para la perfección del contrato que ambas partes se den a conocer--, en otros supuestos más generales de navegar por Internet sería contrario a la intimidad. De aquí que el acuerdo que se adoptó fue que este número identificativo pueda ser explicitado o no por el usuario según la función que esté realizando en la Red.

Los productos de software y de hardware para Internet deberán facilitar a los usuarios información acerca de los datos que pretenden recoger, almacenar o transmitir y la finalidad para la que son necesarios. La configuración del hardware y del software no debería permitir, por defecto, la recogida, el almacenamiento o el envío de información persistente del cliente.

El tercer documento --aún no se ha aprobado definitivamente, aunque está muy avanzado y posiblemente en la reunión del próximo 3 de mayo ya lo aprobemos--, se refiere al respeto a la privacidad durante las interceptaciones. El Grupo de trabajo manifiesta su inquietud sobre el contenido y las implicaciones de la resolución del Consejo de 17 de enero de 1995 relativo a la interceptación legal de las comunicaciones. Esta resolución detalla las condiciones técnicas necesarias para la interceptación de las telecomunicaciones sin abordar la cuestión de las condiciones en que una intercepta-ción puede tener lugar.

A este respecto, resulta de vital importancia que el Derecho nacional precise de forma rigurosa el respeto a las disposiciones mencionadas a continuación: Los servicios autorizados para recoger la interceptación legal de las telecomunicaciones deben especificar el fundamento legal de la intervención. Las circunstancias, las condiciones y las finalidades que pueden tener lugar deben manifestarse para que se pueda apreciar la proporcionalidad a la vista de los intereses nacionales en juego, las medidas de seguridad en lo relativo al tratamiento y almacenamiento de datos y el tipo de conservación de los mismos. Se debe informar al afectado de la interceptación siempre que ello sea posible. Estas modalidades de control deben estar sometidas a una autoridad de control independiente. A este respecto, España hizo la salvedad de que las interceptaciones, según nuestro Derecho Constitucional, no podrán hacerse, en ningún caso, si no es con una autorización judicial, al margen de que una autoridad de control pueda ejercer ese control sobre la independencia.

¿Qué ha hecho o qué está haciendo a este respecto la Agencia de Protección de Datos española? Además de participar en todas estas reuniones, también ha realizado algunas actuaciones internas que creemos pueden resultar de utilidad para los usuarios. En primer lugar, ya en el año 1997 la Agencia publicó un folleto de recomendaciones para los usuarios de Internet. La Agencia entiende que hay que concienciar a los usuarios de los problemas para que así su intimidad en Internet no pueda ser violada, puesto que si lo es, es porque voluntariamente ceden sus datos, pero nadie puede utilizarlos sin que al menos ellos lo sepan. Para ello es fundamental que conozcan y puedan adoptar medidas de seguridad a través de programas y servidores que permitan que los datos puedan ir cifrados y la firma encriptada en los supuestos en que así lo deseen, y en el caso de que no tengan ningún inconveniente a acceder a la Red, sabiendo que otros van a interceptar sus datos, también lo puedan hacer en el uso que cada uno debemos tener de nuestra propia libertad.

Por otro lado, la Agencia entiende que, dentro de las dificultades que supone reglar las transacciones o las comunicaciones en la Red --los problemas jurídicos, como a sus señorías no se les escapa, son múltiples--, un medio eficaz es promocionar códigos éticos para proteger los datos de los ciudadanos en Internet. Hemos sido el primer país de la Unión Europea en el que ha escrito un código ético de protección de datos elaborado por la Asociación Española de Comercio Electrónico. En este código, que también tengo a su disposición, las principales características son que no se establece una globalidad de cuestiones, sino que va referido fundamentalmente al marketing por «e-mail». La asociación que lo ha elaborado incluye empresas muy significativas, de diversos sectores como el bancario, los medios de comunicación audiovisual y escrita, Correos y Telégrafos, grandes establecimientos comerciales, edición y distribución de libros, informática, telecomunicaciones, marketing, consultoría y asesoría jurídica y empresarial.

En la promoción del código ético han participado las tres principales asociaciones de consumidores, así como la Asociación de Autocontrol de la Publicidad, organismo de carácter privado que actúa como autorregulador en el ámbito de la publicidad ilícita. De este modo, se ha pretendido que el contenido no se limite a tener en cuenta los criterios de la empresa, sino también la problemática y los intereses de los consumidores, lo cual creo que ha aportado una garantía más para considerar las bondades de este código.

Su presencia no se ha limitado a participar en la elaboración del código, sino que tiene un carácter estructural y permanente. Así vemos que, de los diez miembros que integran el Comité de Protección de Datos de la Asociación Española de Crédito de Comercio Electrónico, órgano que tiene atribuida la competencia de control del cumplimiento del código, cuatro son representantes de las asociaciones de consumidores y uno lo es de la Asociación de Autocontrol de la Publicidad.

El derecho de información a los afectados de que sus datos han sido recabados o capturados por los anunciantes, encuentra su primera manifestación en la obligación que se impone a éstos de informar en su página web, mediante un aviso, de que se está produciendo dicho tratamiento de datos. El consumidor podrá oponerse total o parcialmente al tratamiento de datos, exceptuando los casos en los que resulte necesario para el supuesto de perfeccionamiento de contratos. La utilización de datos para algunas de las finalidades sobre las que se ha informado puede también ser excepcionada. El consumidor podrá, de igual forma, seleccionar o excluir finalidades para las que consiente que sean destinados sus datos. En el caso de terceros, deberá informársele sobre la identidad de los cesionarios y sobre la finalidad perseguida con la cesión. Asimismo, el derecho de oposición puede ejercitarse mediante un sistema «on line».

En las relaciones con terceros contratantes, las empresas involucradas en la cesión de datos para realizar ofertas por «e-mail» deberán garantizar que cumplen los principios del código ético.

En relación con el tratamiento de datos sobre menores, ante la dificultad de conocer cuándo un menor facilita datos, se aplican garantías indirectas que tratan de evitar riesgos que afectan a tales usuarios.

Teniendo en cuenta la participación que ya da a los menores la Ley Orgánica de Protección del Menor, así como que, queramos o no, éstos van a estar funcionando en Internet, unas veces con el conocimiento de los titulares de la patria potestad y otras no, en la exposición de motivos se llama la atención sobre la obligación de los padres de ejercer estos derechos. Pero, a pesar de ello, se trata de que la publicidad que pueda ir dirigida a menores sea adecuada para ellos. Se concede a los padres la posibilidad de que, preventivamente, puedan ejercer los derechos de acceso, cancelación y rectificación, debiendo respetarse el aviso de los padres contrario a la solicitud de información de publicidad de los hijos. A tal efecto, los anunciantes deberán animar a los menores para que consulten con sus padres. Finalmente, no podrán ceder los datos ni utilizarlos para campañas inadecuadas para la edad de los menores.

El código ético crea un sello de garantía para las empresas adheridas, que tiene por objeto constituir una marca colectiva que pueda distinguir a aquellas empresas que se comprometen a garantizar la intimidad en el tratamiento de los datos personales.

El control del cumplimiento del código ético se atribuye al Comité de Protección de Datos de la Asociación, cuya composición ya les mencioné antes. El Comité tiene la obligación de velar por la evaluación del cumplimiento del código a través de un programa anual de auditorías sistemáticas y al azar.

Por último, se prevé la posibilidad de que la Asociación colabore con las empresas adheridas, a través del Servicio de Asesoría de Protección de Datos.

Como valoración del citado código ético, el juicio de la Agencia de Protección de Datos española es el que constituye una primera e interesante aproximación a los problemas que suscita el tratamiento de datos personales en Internet. Tales problemas se centran fundamentalmente en la posibilidad de captar datos personales sin consentimiento ni conocimiento del afectado, pudiendo tratarse automatizadamente para configurar perfiles personales vinculados a una dirección electrónica. De ahí que, aun pudiendo considerarse otras alternativas, entienda que debe seguirse un proceso gradual que estime un mejor cumplimiento de las normas de protección de datos. Ello no excluye, en modo alguno, que las infracciones que se produzcan sean perseguidas y sancionadas en este caso por la Agencia de Protección de Datos. En dicho proceso resulta necesario intensificar las acciones de evaluación interna y externa del código de conducta, quedando siempre abierta la posibilidad de proceder a su revocación si se acredita que no cumple con las previsiones que mantiene.

En definitiva, éstas son, expuestas brevemente, las principales actuaciones que la Agencia está llevando a cabo a este respecto.

Consciente también de la necesidad de tratar el comercio electrónico, tenemos prevista la celebración de unas jornadas para los días 1 y 2 de julio, en colaboración con la Universidad de Educación a Distancia, que se celebrarán en Mérida, sobre el tema monográfico del comercio electrónico, habiendo convocado a destacados especialistas para que toda la materia pueda ser tratada desde los diversos aspectos, jornadas a las que, por supuesto, quedan invitadas sus señorías.

Muchas gracias, señor Presidente.

El señor PRESIDENTE: Muchísimas gracias, don Juan Manuel.

Hoy llevamos una mañana llena de códigos éticos, lo cual es reconfortante, porque la comparecencia anterior ha sido la del Director de la Asociación de Autocontrol de la Publicidad, a la que usted se ha referido.

Pasamos al turno de portavoces.

En primer lugar, por el Grupo Parlamentario Socialista, tiene la palabra el Senador Lavilla.

El señor LAVILLA MARTINEZ: Muchas gracias, señor Presidente.

Doy la bienvenida a don Juan Manuel Fernández, Director de la Agencia de Protección de Datos.

Al hilo de su exposición sistemática y repasando toda la normativa, tanto europea como española que, de alguna forma, protege a los usuarios y a los ciudadanos, se plantean algunas reflexiones y, en algún caso, preguntas, deduciéndose una de ellas, incluso, de la exposición del interviniente anterior. (El señor Vicepresidente, Herranz Martínez, ocupa la Presidencia.) Cuando se accede a una página web y colocas las famosas cookies en el ordenador personal, no solamente te identifica ante las empresas, sino que incluso puede llegar a destruirte o a controlar la información que trabajas en ese momento. Evidentemente, este hecho puede afectar a muchos usuarios que acceden a páginas web. Precisamente una de las posibilidades de Internet es el acceso a la información y si éste conlleva la identificación del usuario, de sus gustos, preferencias e incluso del trabajo que se está realizando, lógicamente no se está respetando su privacidad. Sólo ha accedido a una información que ha querido incorporar a su ordenador personal, y ese acceso ha permitido a una determinada empresa controlar datos de tipo personal. Ante esto, que parece que está sucediendo, ¿qué hacer? ¿Qué medios tiene ese internauta corriente para proteger su privacidad o actuar frente a comportamientos no deseados en su ordenador personal? En relación a la Ley Orgánica 5/1992, de 25 de octubre, de Protección de Datos, el día 16 de marzo usted decía que era buena y que tan sólo había que recoger algunos matices con la nueva Directiva europea. Hablaba de la dualidad entre privacidad y seguridad e, incluso, se plantea que la nueva Directiva puede incorporar algunas recomendaciones en materia de terrorismo y de formas graves de delincuencia, que pueden rayar un poco en la privacidad, incluso en relación a la normativa vigente. Me gustaría que nos ampliara un poco su punto de vista.

Respecto a la publicidad, algunas publicaciones actuales están llegando a vender en Internet paraísos para el lavado de dinero. Se dice: La forma más simple y legal de ocultar sus bienes. Ante este tipo de publicidad, ¿con qué medios cuenta la Agencia y qué medios complementarios se pueden poner en marcha? En cuanto a la privacidad, se ha referido también a la de los menores.

Quisiera que nos diera su punto de vista al respecto en España, si considera que la privacidad de los menores está suficientemente protegida y, en cualquier caso, hacia dónde se deben dirigir las actuaciones, tanto legislativas como del Gobierno, para profundizar en este campo, compatibilizando, como ya se ha dicho, la privacidad con el uso libre de Internet.

Por otro lado, cuando se ha referido a la promoción de código éticos, ha citado que se incluyen cuatro miembros del sector de los consumidores y no del sector de la publicidad. Desearía preguntarle si también se ha contado con las asociaciones de internautas o si ya se incluyen en ese grupo de consumidores que usted ha citado.

Por mi parte, no tengo más preguntas que hacerle y reitero el agradecimiento a su exposición.

El señor VICEPRESIDENTE (Herranz Martínez): Muchas gracias, Senador.

Tiene la palabra la Senadora Vindel López para formular las preguntas al compareciente.

La señora VINDEL LOPEZ: Muchas gracias, señor Presidente.

En nombre de mi Grupo, quiero dar la bienvenida al Director de la Agencia de Protección de Datos, don Juan Manuel Fernández López y, asimismo, de forma personal, a mi amigo Juan Manuel Fernández López, porque, señorías, no les oculto que es la primera vez que en una sesión de trabajo del Senado contamos con la presencia del Director de la Agencia de Protección de Datos. El me ha recibido en distintas ocasiones, dándome la bienvenida, en la magnífica sede que dicha Agencia tiene en el Paseo de la

Castellana, porque, como sus señorías recordarán, yo represento al Senado, soy vocal del Consejo de la Agencia y, por tanto, tengo felizmente la oportunidad de trabajar con el Director y con su equipo.

Entre otras cosas, quiero felicitarle, aparte de por su magnífica y clara comparecencia, por el trabajo que ha venido realizando, que me consta que es mucho, cada vez mayor, lo cual significa que, aunque ustedes tendrán mucho más trabajo, los ciudadanos españoles, los usuarios de Internet, del correo electrónico y del comercio electrónico, se están empezando a preocupar de una forma efectiva por sus derechos y, desde luego, los reclaman, como me consta, al propio Director. Espero que no se vean sobrepasados por el trabajo y, si es así, señor Director, nos lo hace saber para que, a través de los Presupuestos Generales del Estado, quizá podamos aliviarle de la carga de trabajo.

Entrando ya en las comparecencia del señor Fernández López, yo quiero decir, señor Presidente, que, aprovechando esta oportunidad fantástica que tenemos desde esta Comisión, que hoy por primera vez se está retransmitiendo a través de Internet, a mí me gustaría hacer un recordatorio en este momento al Tribunal Constitucional para que, de una vez por todas, se pronuncie sobre el recurso que ha sido presentado hace más de seis años contra la Ley Orgánica reguladora del tratamiento automatizado de datos.

No me cabe ninguna duda de que, como muy bien dice el director de la Agencia de Protección de Datos, es una buena Ley para trabajar con ella, pero tiene un recurso pendiente, como ya he dicho, desde hace seis años y, dado el avance del ciberespacio, de Internet, y la velocidad con que se están produciendo los acontecimientos, pido sinceramente desde aquí que el Tribunal Constitucional se pronuncie.

Este recurso se presentó al mismo tiempo que otro a la famosa «Ley Corcuera». En aquella ocasión el Tribunal Constitucional tardó exactamente cinco meses en pronunciarse y, sin embargo, sobre este recurso lleva ya más de seis años. Yo comprendo que es muy gráfico ver saltar una puerta por los aires, pero no nos debemos olvidar de que el problema es que los ordenadores no hacen ruido, es decir, trabajan en silencio. Por tanto, como de lo que se trata es de proteger nuestra intimidad, yo hago desde aquí un llamamiento al Tribunal Constitucional para que cuanto antes y sin dilación, habida cuenta de que en el Congreso de los Diputados se está tratando la modificación de la LORTAD por aplicación de una directiva, nos haga saber qué criterios utiliza y cuál será el fallo que va a emitir relativo a los derechos fundamentales, ya que al cuerpo legislativo de este país le vendría muy bien.

En primer lugar, me gustaría preguntar al señor Fernández López si los conceptos de privacidad y de intimidad son los mismos, porque yo creo que uno es más que el otro o, quizá, uno se utiliza más en el mundo sajón y el otro en el europeo. Antes de empezar a hablar de la defensa necesaria del derecho a la intimidad frente a la publicidad, al comercio electrónico, a nuestra propia intimidad, tenemos que empezar a saber si son un mismo concepto o si son distintos y, si es así, cuál es mayor, cuál es menor, y si conviene ir creando un cuerpo doctrinal sobre la privacidad, que sustituya a la intimidad o viceversa, pero, dado que Internet es un mundo que no tiene fronteras y que no conoce límites, bueno será que el mundo entero empiece a estar dispuesto a hablar de los mismos conceptos, con el fin de saber cómo y de qué manera tenemos que defendernos.

En segundo lugar, el señor Fernández López se ha referido a las recomendaciones para los usuarios de Internet que publicó la Agencia hace año y medio, y me gustaría preguntarle si se han quedado antiguas, si es necesario ampliarlas o si son bastantes. Como miembro de la Agencia de Protección de Datos las tengo desde hace tiempo y son interesantísimas, pero constituyen una forma de autoprotección similar a los folletos que envía la policía a casa sobre lo que debe hacerse antes de realizar un viaje en verano: no dejar las persianas bajadas del todo; no dejar la correspondencia acumulada en el buzón, etcétera. Como le digo, esas recomendaciones están muy bien, pero me gustaría preguntarle: dado el avance que en año y medio se ha producido en Internet, ¿son bastantes? ¿Hay que ampliarlas? ¿Hay que modificarlas? Me gustaría también que el señor Fernández López nos diera su opinión sobre si nuestro sistema normativo, nuestras leyes son insuficientes a la hora de proteger la intimidad de los usuarios o, le hago la pregunta a la inversa, si nuestro sistema judicial nos protege suficientemente respecto a intromisiones no queridas en nuestra intimidad.

Como ésta es una comisión especial de estudio pero, a fin de cuentas, formamos parte de las Cortes Generales, y la actividad principal de éstas es la legislativa, le pregunto si usted cree que en el informe final que tendrá que elaborar esta Comisión sería necesaria una ley especial, al margen de las que ya hay, o si con sus recomendaciones podríamos ir adelantando el trabajo e incluirlas en la LORTAD, ¿o éste es un ámbito completamente diferente? Por último, me gustaría saber su opinión sobre esta noticia que se produjo a finales del verano pasado: el Vicepresidente de los Estados Unidos, señor Al Gore, en una comparecencia pública en la Universidad de Nueva York manifestaba que se necesitaba una carta magna electrónica sería la carta magna del siglo XXI-- es decir, una relación de derechos de los usuarios en Internet, en lo que se conoce en las redes de la información.

En el caso de que usted fuera favorable a la emisión de esa carta magna electrónica, también quisiera saber si se podría ir eliminando o desbrozando la cuantiosa normativa europea existente. Aunque me parecen estupendos y cuantos más códigos éticos de autorregulación se hagan desde el sector privado mejor, me gustaría saber, como le digo, si a través de grupos de trabajo se podría intentar hacer en Europa una carta magna al estilo de los Estados Unidos, como proponía el señor Al Gore, o si es preferible ir de forma más lenta y, por lo tanto, seguir con el sistema de las directivas que, dicho sea de paso, tanto nos distorsionan cuando llega su transposición a las Cortes Generales.

Nuevamente le doy las gracias, señor Fernández López.

Nada más, muchas gracias.

El señor VICEPRESIDENTE (Herranz Martínez): Gracias, Senadora Vindel.

Para contestar a las preguntas formuladas por los Senadores, tiene la palabra el señor Fernández López.

El señor DIRECTOR DE LA AGENCIA DE PROTECCION DE DATOS (Fernández López):

Muchas gracias, señor Presidente.

Trataré de contestar ordenadamente.

En primer lugar, sobre los problemas que en definitiva plantean los cookies, en cuanto a que pueden succionar datos de los programas y de los ordenadores, es una realidad que existe. Por eso la Agencia hizo esta publicación donde previamente se le informa al usuario --el problema empieza porque muchos usuarios de Internet no saben lo que está pasando, ni hasta dónde puede ser violada su intimidad--, se le dice: usted está en un medio maravilloso, tal vez en uno de los más importantes del siglo que viene o en donde posiblemente se llevarán a cabo las principales transacciones económicas en Internet, pero tiene que estar advertido de los peligros. De ahí que para evitar los problemas de las cookies, habrá que emplear programas y servidores a través de los mensajes cifrados y de las firmas encriptadas. A mí, por supuesto, no se me ocurriría dar los datos de mi tarjeta de crédito por Internet, a no ser que fueran cifrados, pero hay mucha gente que lo está haciendo a diario y las consecuencias, como sus señorías pueden imaginar, pueden ser desagradables para el que así actúa. De ahí que lo primero que hay que hacer es informar.

Pero no olviden sus señorías que, como decía antes, la Ley Orgánica de Protección de Datos, por lo que respecta a España, está vigente también en Internet, por lo tanto, hay que tener en cuenta no sólo cómo opinan los españoles, sino también el resto de nuestros socios europeos. Con lo cual, en el momento en que se produzca una denuncia, la Agencia actuará, investigará y sancionará. También tengo que decirles que la dificultad en poder demostrar una de estas prácticas es mucho mayor en el mundo de Internet que en otro supuesto. En definitiva, la Ley está vigente y la Agencia sancionará cualquier conducta contraria a los derechos de los ciudadanos en la preservación de esa intimidad.

En cuanto a mi criterio sobre la ley, he de decir que la Ley es muy buena, y hago una afirmación mayor, es la mejor de Europa; estamos protegiendo al mejor nivel los derechos de nuestros ciudadanos. El resto de los países europeos, que incluso tenían leyes muy anteriores a las nuestras, aún están desarrollando sistemas de inspección. Como anécdota les diré que en la Conferencia Internacional, celebrada este año en Santiago de Compostela, que España tuvo el honor de organizar para las autoridades de control no sólo ya de la Unión Europea, sino de otros países que tienen ley y tienen autoridad de control, con motivo de una ponencia de la Agencia Española sobre los estándares de inspección, varios países europeos han acudido a nosotros para que les explicitáramos las formas en que llevamos a cabo estas inspecciones, incluso han estado en Madrid para informarse de ellas in situ.

También este año, en la Conferencia de Primavera en Helsinki, con motivo de la exposición, España ha comparecido con tres ponencias --una de ellas, los Códigos éticos y, otra, las transferencias internacionales de datos--, y nuevamente los países europeos nos solicitan ayuda para conocer nuestros sistemas, porque, en definitiva, son los más avanzados.

Concretamente, nosotros hemos sido el primer país de Europa que ha autorizado una transmisión masiva de datos a Estados Unidos, donde no existe legislación, al menos a nivel federal; hay legislaciones sectoriales y en algunos otros supuestos hay legislaciones de protección de datos en algunos Estados.

Con esto, quiero decirle que efectivamente nuestro grado de protección es bueno, aunque, por supuesto, podría ser mejor, pero las cosas tampoco son sencillas y, sobre todo, hay que tener en cuenta que cuando se trata de Internet es como ponerle vallas al campo.

En cuanto a la publicidad de los menores, como saben sus señorías, la Ley Orgánica de Protección del Menor les otorga, sobre todo cuando alcanzan la edad de 12 años, una cierta autonomía y capacidad de decisión. Por otra parte, es una realidad que precisamente estos chicos son los que mejor manejan y más rápidamente acceden a Internet. Indudablemente, la primera obligación está en el deber de vigilancia por parte de sus padres, pero como esto en algunos casos no se va a producir, en el código ético también figura, como hemos visto, que las empresas que ofrezcan bienes a los menores tengan en cuenta su edad, es decir, que sean cosas que resulten adecuadas a su edad, a su desarrollo mental y a su desarrollo social.

En cuanto a la intervención de los internautas, efectivamente así ha sido, pero no directamente las asociaciones de internautas. Tengan en cuenta sus señorías que la Agencia no ha sido la promotora, del código, sino la Asociación de Marketing Electrónico, pero a través de las asociaciones de consumidores han estado presentes las personas conocedoras del tema. Una de mis satisfacciones ha sido precisamente que las tres asociaciones de consumidores dieran su placet, y no sólo eso, sino que incluso elogiaron este código, que al final fue aprobado por la Agencia de Protección de Datos. No sé si me he dejado alguna cosa en el tintero, si es así su señoría me lo dirá y, con mucho gusto, le responderé.

En cuanto a las preguntas de la señora Vindel, en primer lugar, le diré que estoy absolutamente de acuerdo; a ver si de una vez por todas el Tribunal Constitucional se pronuncia sobre los recursos planteados contra la vigente ley. Tengo pocas esperanzas porque antes de estar en la Agencia de Protección de Datos mi cometido estaba en el Tribunal de Defensa de la Competencia, y ahí nos encontramos con que la ley no era de 1992, sino de 1989, y que también estaba tachada de inconstitucionalidad y tampoco se ha pronunciado aún el Tribunal Constitucional. Por tanto, cualquier cosa que se haga para que se pronuncie será deseable, aunque soy escéptico respecto a la rapidez con que pueda producirse.

La Senadora Vindel también se ha referido a un tema interesante sobre si es mejor el empleo del barbarismo «privacidad» o del castellano «intimidad». Aunque soy un defensor acérrimo de nuestro idioma, creo que en este supuesto el término «privacidad» es más omnicomprensivo que el de «intimidad», por ello personalmente soy usuario de este término, teniendo en cuenta, por supuesto, que el de intimidad es el auténtico castellano.

La privacidad va a contemplar al individuo en un aspecto mucho más general, mientras que la intimidad va a referirse más a su relación personal y familiar.

En cuanto a si nuestras leyes protegen suficientemente, creo que sí y las recomendaciones sobre Internet tal vez habría que ponerlas al día, no porque las que figuran ahora sean inválidas, sino para ampliarlas y dar a los conocedores del sistema algunas herramientas al respecto. (El señor Presidente ocupa la Presidencia.) Lo que sucede es que estudiar Internet es complicado. Yo estaba pendiente de que a nivel europeo se llegara a mayores conclusiones para poner al día estas recomendaciones que, vuelvo a repetir, son válidas pero efectivamente podrían ampliarse.

También es cierto que el Vicepresidente americano, Al Gore, en el mes de octubre pasado estaba muy preocupado fundamentalmente porque los norteamericanos, que no tienen una normativa a nivel federal en cuanto a protección de datos, se consideraban para la Unión Europea terceros países a los que había que analizar caso por caso para la posibilidad de transferencias internacionales de datos y limitarlas con duras normas contractuales. Yo sé que el Vicepresidente, Al Gore, y el Presidente de la Comisión Europea están en continuo contacto, pero las cosas no avanzan mucho.

Sí es deseable que tengamos una carta magna de derechos europeos, pero aún vamos a tardar tiempo, porque no nos olvidemos de que los sistemas legislativos de los países de la Unión aún son muy dispares, y que en algunos países no existe ninguna tradición. Aunque hoy día todos tengan leyes protectoras de la intimidad, no existe una cultura en ese tipo de leyes. Piénsese que Grecia, incluso Italia, y Portugal tienen leyes, pero tan novedosas como del año 1996, con lo cual esa conciencia en la protección no existe suficientemente a nivel europeo. Poco a poco podremos ir marchando y algún día llegaremos a ese deseo de su señoría, que también es el mío, de poder establecer una carta de estos derechos a nivel europeo.

Muchas gracias, señor Presidente.

El señor PRESIDENTE: Muchas gracias, don Juan Manuel Fernández.

Podemos abrir un turno si algún Senador quiere hacer alguna pregunta o aclaración. (El señor Mòdol Pifarré pide la palabra.) Tiene la palabra.

El señor MODOL PIFARRE: Muchas gracias, señor Presidente.

No quiero hacer ninguna pregunta, sino, como no podía ser de otra manera, agradecer las explicaciones de don Juan Manuel Fernández y la claridad de su exposición.

Y antes de terminar la sesión de hoy, en nombre del Grupo Parlamentario Socialista, y supongo que lo puedo hacer también en nombre del Grupo Parlamentario Popular, quiero agradecer la eficacia de la nueva técnica demostrada hoy y, por tanto, agradecer a los servicios técnicos de la Casa su puesta en funcionamiento con la eficacia con la que lo ha hecho.

Muchas gracias, señor Presidente.

El señor PRESIDENTE: Muchas gracias.

Estoy convencido de que el Jefe del Departamento, que además está presente en la sala, sabrá transmitirlo a todos y a cada uno de los profesionales que colaboran con él. Yo ya lo he hecho a través de otros métodos, quizá más pertinentes, como el correo electrónico.

Sin más, y agradeciendo de nuevo la presencia de don Juan Manuel Fernández, Director de la Agencia de Protección de Datos, podemos levantar la sesión.

Eran las trece horas y veinte minutos.

MEMORIA DE 1999 - ANEXO VI - CÓDIGOS ÉTICOS

CODIGO ETICO SOBRE PUBLICIDAD EN INTERNET
ASOCIACIÓN DE AUTOCONTROL DE LA PUBLICIDAD

El presente Código Ético sobre Publicidad en Internet de la Asociación de Autocontrol de la Publicidad ha sido aprobado en su Asamblea General Ordinaria celebrada el 14 de abril de 1999.

EXPOSICIÓN DE MOTIVOS

Como es bien sabido, los orígenes de Internet se remontan a los años sesenta, y se encuentran en las actividades propias de un proyecto de investigación puesto en marcha por diversas agencias del gobierno de los Estados Unidos. Todo ello, sin olvidar la relevancia del papel desempeñado en el origen y evolución de Internet por los trabajos desarrollados en los años ochenta desde Europa, en concreto en el ámbito de la elaboración del protocolo de comunicaciones, por los laboratorios Europeos de Física de Partículas (CERN), en Suiza por los científicos R.Carillau y T. Berners-Lee, que bautizaron un sistema de información global para el intercambio de datos esenciales para la comunidad científica como "world wide web" (www). No obstante, desde aquella primera época hasta nuestros días, Internet ha experimentado una vertiginosa evolución. Hoy en día, Internet constituye un eficaz medio para intercambiar y acceder a gran cantidad de información. De este modo, Internet se ha convertido en un nuevo medio de comunicación y transacciones comerciales. Y, como tal medio de comunicación, puede ser utilizado también con finalidades publicitarias.

Es evidente, por lo demás, que la publicidad que se difunde a través de Internet queda sometida a las normas generales que regulan la actividad publicitaria. En la medida en que la publicidad tenga por objeto algún producto sometido a normativa específica, estas normas especiales serán también aplicables. No obstante, conviene aclarar que no resultan aplicables a Internet las normas especiales promulgadas para determinados medios como, por ejemplo, la televisión.

Así las cosas, el debate se centra, en gran medida, en determinar si Internet, como soporte o medio publicitario específico, precisa también de normas especiales que regulen la publicidad que en la Red se difunde. La respuesta, en principio, parece que debe ser afirmativa, toda vez que las características propias de este medio pueden hacer necesaria una cierta adaptación de las normas generales en la materia, así como la adopción de normas específicas que contemplen y regulen supuestos de hecho que no se plantean en los restantes medios de difusión.

Existe un relativo consenso, por lo demás, al afirmar que es preferible que las normas a las que se acaba de hacer referencia se adopten de forma voluntaria por los propios sectores interesados a través de los correspondientes códigos éticos o de autodisciplina. Consciente de esta necesidad, el presente Código pretende establecer unas mínimas normas sobre la publicidad en Internet.

Se parte, a estos efectos, del principio de control en origen. Las razones por las que se ha optado por este principio son, básicamente, dos. Así, en primer lugar, el principio de control en origen es el que actualmente propugnan las instituciones comunitarias europeas, como demuestra el Libro Verde sobre la Comunicación Comercial. Y, en segundo lugar, sólo la opción por el control en origen puede asegurar una cierta efectividad a la hora de establecer los mecanismos que aseguren el comportamiento del Código.

Tras establecer el principio de control en origen, el Código establece una serie de normas generales para la publicidad en Internet. Ahora bien, como queda expuesto, la publicidad en Internet da lugar también una serie de supuestos de hecho específicos que no se plantean en otros medios de difusión. De ahí que las normas generales a las que antes se hacía referencia se completen con un capítulo, el III, en el que se recogen normas especiales para la publicidad por correo electrónico, la publicidad en charlas (chats) y foros de discusión -a excepción de las charlas o foros de los que sea directamente titular un anunciante-, la publicidad en la world wide web, normas que son de aplicación a todos y cada uno de los supuestos conocidos actualmente de publicidad en Internet -y, por tanto, a las listas de correo, a las zonas de juego común y a los ICQ-, así como a cualquier otra forma de publicidad que pueda surgir en el futuro en el ámbito de Internet.

Considerando el dinamismo de este sector y las desconocidas posibilidades de evolución tecnológica, las normas contenidas en este Código deben ser revisadas, para garantizar su actualidad, en un plazo no muy lejano.

De igual forma, considerando la globalidad y extraterritorialidad implícita de la world wide web, este Código y los mecanismos de autocontrol establecidos para su aplicación tienen vocación de integración y/o coordinación en futuros sistemas internacionales de autorregulación publicitaria en Internet, cuando sean una realidad.

Asimismo, en el ámbito deontol6gico, este Código Ético de Publicidad en Internet tiene vocación de complementariedad con el establecido por la Asociación Española de Comercio Electrónico para la proteccion de datos personales en Internet.

CAPÍTULO I

Definiciones y Ámbito de aplicación

Artículo 1.- Definiciones.

A los efectos del presente Código, debe entenderse por:

a) Publicidad: toda forma de comunicación pública realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones. b) Internet: la red de acceso público de redes con un protocolo común que permite la transmisión de información entre usuarios, o entre usuarios y un lugar en la red, así como todos los medios interactivos y la red electrónica, como por ejemplo la WWW (world wide web) y los servicios en línea (on~line), c) Anunciante: la persona física o jurídica en cuyo interés se realiza la publicidad. d) Destinatarios: las personas a las que se dirija o alcance la publicidad.

Artículo 2.- Ámbito de aplicación,

1.- El presente Código será aplicable a la publicidad realizada en Internet, por personas físicas o jurídicas con establecimiento en España, y a la publicidad insertada en soportes cuyos titulares tengan nacionalidad o establecimiento en España y hayan aceptado este Código,

2.- Asimismo, entran en el ámbito de aplicación del presente Código las páginas hospedadas en servidores ubicados en territorio español, que hayan aceptado este Código.

3.- El presente Código no será de aplicación a la comunicación bilateral originada por solicitud del usuario, ni a los contenidos editoriales de las páginas web, entendiendo por tales todos aquéllos que no estén orientados a la promoción, directa o indirecta, de la contratación de bienes, servicios, derechos y obligaciones.

CAPÍTULO II

NORMAS GENERALES

Artículo 3.- Principios generales.

1.- La publicidad en Internet deberá ser conforme a la ley aplicable, decente, honesta y veraz, en los términos en que estos principios han sido desarrollados por el Código de Conducta Publicitaria de la AAP y por el Código de Práctica Publicitaria de la Cámara Internacional de Comercio.

2.- La publicidad en Internet deberá respetar las normas recogidas en los Códigos mencionados en el párrafo anterior, así como aquellas otras que se recojan en los Códigos sectoriales contemplados en el artículo 8 del Código de Conducta Publicitaria de la AAP.

3.- La publicidad en Internet deberá ser elaborada con sentido de la responsabilidad social, y no deberá constituir nunca un medio para abusar de la buena fe de sus destinatarios, evitando así que pueda deteriorarse la confianza del público en Internet.

4.- La publicidad en Internet no tendrá contenidos que atenten contra la dignidad de la persona, o sean discriminatorios (por razón de nacionalidad, raza, sexo, orientación sexual, convicciones religiosas o políticas), o incitadores de la comisión de actos ilícitos.

Artículo 4.- Identificación M anunciante.

En la publicidad en Internet el anunciante deberá ser siempre identificable, de forma tal que el usuario pueda reconocerlo y ponerse en contacto con él sin dificultades.

Artículo 5.- Identificación de la publicidad.

La publicidad en Internet será fácilmente identificable como tal. No se admitirá la publicidad encubierta.

Artículo 6.- Protección de datos personales.

1.- Los anunciantes que difundan publicidad en Internet deberán respetar la legislación vigente en materia de protección de datos personales.

2.- Cuando a través de la red los anunciantes recaben o traten datos personales, deberán avisar a los destinatarios, de forma claramente perceptible, de dicha recogida y tratamiento, y deberán informarles de la finalidad a que se destinan dichos datos, así como, en su caso, de la posible cesión de los mismos a terceros. La información recabada no podrá ser utilizada para fines distintos de los manifestados.

3.- Los anunciantes deberán garantizar a los destinatarios el ejercicio de los derechos de acceso, rectificación y cancelación de sus datos personales, así como del derecho a oponerse al tratamiento y/o transferencia de los mismos,

poniendo para ello a su disposición mecanismos de utilización sencilla (dirección de correo electrónico y postal).

4.- Los anunciantes deberán respetar la privacidad de quienes entren en su web, garantizando así los derechos de los ciudadanos.

5.- Los anunciantes también deberán apoyar iniciativas para ayudar a educar al consumidor sobre cómo proteger su intimidad en la Red.

6.- La información que se almacene en las denominadas "listas de no abonados" será la mínima e imprescindible para evitar el envío de publicidad por correo electrónico no deseada. En consecuencia, no podrá almacenarse más información que la dirección de correo electrónico, salvo acuerdo en contrario.

Artículo 7.- Información al destinatario.

1.- Los anunciantes deberán informar del coste o precio de acceder a un mensaje o servicio cuando aquél sea mayor que el de las tarifas básicas de telecomunicación. Los destinatarios serán informados de tales costes antes de acceder al mensaje o servicio, de forma clara, y deberán disponer de un plazo de tiempo razonable y suficiente para poder desconectarse del servicio sin incurrir en gastos.

2.- Las ofertas deberán identificarse de modo que el que las recibe pueda reconocerlas como ofertas. Si en la publicidad se presenta o realiza una oferta directa de contratación, se deberá proporcionar al destinatario una información clara, completa y precisa sobre el contenido y el alcance de aquélla.

3.- La información a la que se refiere el párrafo anterior deberá incluir de forma visible, como mínimo, los siguientes extremos:

a) Precio de compra completo, incluyendo en su caso la moneda, la modalidad de pago, el franqueo y los portes. b) Duración de la oferta y limitaciones de la misma. c) Términos, condiciones y formas de pago, incluyendo opciones de crédito. d) Características de los bienes o servicios y, en su caso, condiciones necesarias para su utilización. e) Existencia o inexistencia de costes adicionales. f) Condiciones relacionadas con devoluciones, cancelaciones o cambios M correspondiente producto o servicio. g) Garantías aplicables a la adquisición del producto o servicio. h) Lugar y forma de presentación de posibles reclamaciones. i) Domicilio del proveedor a efectos legales.

Artículo 8.- Competencia desleal y respeto a los derechos de propiedad intelectual e industrial.

1.- La publicidad en Internet deberá respetar los derechos de propiedad intelectual e industrial de terceras personas distintas del anunciante.

2.- La publicidad en Internet no deberá constituir nunca un medio de competencia desleal.

3.- No se admite la introducción en el código fuente de nombres ocultos (metanames) que coincidan con marcas, nombres, rótulos o denominaciones de empresas o productos sobre los que no se ostente la titularidad o una autorización de uso.

Artículo 9.- Protección de los menores.

La publicidad difundida en Internet no deberá perjudicar moral o físicamente a los menores y deberá, por consiguiente, respetar los siguientes principios:

a) Deberá identificar los contenidos dirigidos únicamente a adultos.

b) No deberá incitar directamente a los menores a la compra de un producto o servicio, explotando su inexperiencia o su credulidad, ni a que persuadan a sus padres o tutores, o a los padres o tutores de terceros, para que compren los productos o servicios de que se trate.

c) En ningún caso deberá explotar la especial confianza de los niños en sus padres o tutores, profesores u otras personas.

d) No deberá, sin motivo justificado, presentar a los niños en situaciones peligrosas.

e) Deberá alentar a los menores a obtener autorización de sus padres o tutores antes de facilitar información en línea (on-line), y establecer mecanismos que aseguren que los niños han obtenido el consentimiento de aquéllos.

f) Deberá ofrecer a los padres o tutores información acerca de cómo proteger en línea (on-line) la privacidad de sus hijos o pupilos, así como facilitarles mecanismos para ejercer los derechos de acceso, cancelación y determinación de la finalidad sobre los datos de aquéllos.

CAPíTULO III

NORMAS ESPECIALES

Artículo 10.- Publicidad por correo electrónico.

1.- No se admitirá el envío de publicidad por correo electrónico por parte del anunciante cuando ésta no haya sido previamente solicitada o autorizada por el destinatario.

2.- Se entiende concedida la autorización prevista en el párrafo anterior cuando, al tiempo de recabar los datos, se haya informado debidamente al destinatario sobre la posibilidad de envío publicitario y éste no se haya opuesto.

3.- Asimismo, se entiende concedida la autorización prevista en el primer párrafo de este precepto cuando la publicidad se dirija a un cliente de la empresa con el que ya existían previamente relaciones contractuales o precontractuales.

4.- Aquellos anunciantes que utilizan el correo electrónico deberán informar sobre la posibilidad de notificar al anunciante su deseo de no recibir ofertas posteriores y proporcionar un mecanismo a través del cual el usuario pueda ejercitar este derecho.

5.- En todo caso, los mensajes publicitarios enviados por correo electrónico deberán identificarse claramente como tales, revelando asimismo la identidad del anunciante.

Artículo 11.- Publicidad en grupos de noticias, foros, charlas (chats) y similares.

1.- No podrán utilizarse los grupos de noticias, tablón de anuncios o foros o charlas para captar datos con finalidad publicitaria o para enviar publicidad en línea (on-line), salvo que, en este último caso, previamente se haya obtenido el consentimiento del moderador del punto de encuentro o, en su defecto, del proveedor del servicio, o se ajuste a las reglas de admisión de publicidad establecidas para ese grupo, foro, charla o similar.

2.- Se excluyen, de lo previsto en este artículo, los foros o charlas de naturaleza publicitaria.

Artículo 12.- Publicidad en la world wide web.

1.- La publicidad en la world wide web no puede, sin el conocimiento previo del usuario, impedir su libre navegación en Internet.

2.- Cuando las interrupciones publicitarias o la recepción de mensajes publicitarios sean condición inevitable para el acceso al contenido editorial de una página web o para la navegación en la red, esta circunstancia deberá ser previamente advertida al usuario. Para ello, bastará con la inserción, en la "portada", de un mensaje fácilmente visible que informe de la existencia de contenidos publicitarios en la página web a la que el usuario se dispone a acceder.

Artículo 13.- Patrocinio.

1.- Se entenderá por patrocinio cualquier contribución realizada por una empresa pública o privada a la financiación de páginas web con la finalidad de promover su nombre, marca, imagen, actividades o productos.

2.- Las web patrocinadas deberán cumplir los siguientes requisitos:

a) El contenido editorial de una web patrocinada no podrá, en ningún caso, ser influido por el patrocinador de tal forma que se atente contra la responsabilidad y la independencia editorial del titular de la página web.

b) Deberán estar claramente identificadas como tales, e incluirán el nombre, logotipo, marca, servicios u otros signos del patrocinador al principio o al final de la página web, o en los dos momentos.

También podrá identificarse al patrocinador por los medios antes mencionados en el desarrollo de la página patrocinada, siempre que ello se haga de forma esporádica y sin perturbar su lectura.

CAPíTULO IV

NORMAS DE APLICACIÓN DEL CÓDIGO

Artículo 14.- Empresas adheridas.

1.- Las empresas que manifiesten su adhesión al presente Código Ético se comprometen a respetar en su actividad publicitaria las normas en él recogidas. Los socios de la Asociación de Autocontrol de la Publicidad (AAP) y las empresas adheridas a este Código se comprometen a cumplir escrupulosamente las resoluciones que el Jurado de la AAP dicte como consecuencia de la tramitación de reclamaciones contra acciones publicitarias concretas en Internet.

2.- la AAP hará pública la relación de empresas adheridas.

3.- Las empresas adheridas y los socios de la AAP podrán, si lo desean, insertar en sus web un enlace de conexión con la web de la AAP con el fin de ofrecer a los usuarios la posibilidad de consultar los contenidos del presente Código Ético, formular una queja o presentar una reclamación.

4.- Dicho enlace dirá: "La empresa X está adherida al Código Ético de Publicidad en Internet de la ASOCIACIÓN DE AUTOCONTROL DE LA PUBLICIDAD de España. Si quiere ver el texto de dicho Código, conocer la relación de empresas adheridas o presentar una reclamación por publicidad incorrecta puede acudir a la AAP (logotipo, de la AAP)".

Artículo 15.- Control de cumplimiento.

1.- El control del cumplimiento de las normas del presente Código corresponde al Jurado de la AAP.

2.- La AAP establecerá los mecanismos necesarios que permitan on-line la presentación de reclamaciones y la comunicación de las resoluciones del Jurado.

3.- Para la efectiva aplicación de las normas de este Código y la tramitación y resolución de las eventuales reclamaciones que se presenten contra acciones publicitarias concretas en Internet, el Jurado de la AAP se atendrá a lo previsto en su Reglamento.

CAPITULO V

COLABORACIÓN CON LAS AUTORIDADES

Artículo 16.- Los anunciantes, medios y soportes en Internet tienen la obligación de colaborar con las autoridades competentes, y de poner en su conocimiento cualquier información relevante a la que haya tenido acceso, acerca de actividades delictivas en la red (contenidos pornográficos referidos a menores, promoción o comercialización ilícita de medicamentos o drogas, proxenetismo, u otras que se encuentren tipificadas como delito en el Código Penal español).

CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS PERSONALES DE LAS EMPRESAS DEL SECTOR DE INFORMACIÓN COMERCIAL

EXPOSICIÓN DE MOTIVOS

En la actualidad, la conciencia social es favorable al uso de los medios automáticos para el tratamiento de la información, no concibiéndose ninguna actividad profesional y comercial que pueda esta ajena a la informática.

Es manifiesta la importancia de las empresas dedicadas a acercar, mediante su actividad informadora, a los sujetos de las relaciones negociales y crediticias que surgen en la sociedad.

Muchas de estas relaciones se fundamentan y necesitan para su desarrollo en el mutuo conocimiento de las partes, conocimiento que en ocasiones sólo es posible alcanzar acudiendo a empresas especializadas cuya actividad consiste en agilizar y facilitar el acceso de personas, tanto físicas como jurídicas a las múltiples posibilidades de participación activa existentes en el entorno.

El sector de Información Comercial encuadrado dentro de ASEDIE Asociación Multisectorial de la Información, consciente de la importancia de la labor de sus miembros, reconoce la necesidad para el sector de elaborar este CÓDIGO ÉTICO, con el fin de prevenir las violaciones de la privacidad de las personas, que pudieran resultar del tratamiento de sus datos personales.

TITULO I: DISPOSICIONES GENERALES

ARTICULO 1. OBJETO.

El presente Código, en desarrollo de lo previsto en el artículo 31 de la Ley Orgánica 5/1.992 de 29 de Octubre de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), tiene por objeto establecer las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la LORTAD y sus normas de desarrollo.

ARTICULO 2. ÁMBITO DE APLICACIÓN DEL CÓDIGO

El presente Código se aplicará a las relaciones que mantengan las empresas asociadas a ASEDIE (Sector de Información Comercial) con las personas objeto de informes comerciales, con los usuarios de los mismos, así como a las relaciones que dichos asociados mantengan entre sí y con terceras personas, empresas, entidades u organismos relacionados de forma directa o indirecta con el ejercicio de la actividad de Información Comercial.

Asimismo, este Código Ético se aplicará a los ficheros automatizados que contengan datos de carácter personal y de los que sean responsables las empresas asociadas a ASEDIE (Sector de Información Comercial), cuya finalidad sea la

prestación de servicios de información sobre la solvencia patrimonial y crédito.

Las empresas asociadas a ASEDIE (Sector de Información Comercial) figuran relacionadas en el Anexo a este Código Ético. Cada seis meses ASEDIE presentará ante la Agencia de Protección de Datos, una relación actualizada que contenga todas las empresas asociadas al Sector de Información Comercial de la Asociación.

No obstante la Asociación comunicará a la Agencia de Protección de Datos, en el plazo de 15 días naturales, cualquier alta o baja de empresas asociadas encuadradas en dicho sector, que se produzca.

ARTICULO 3. DEFINICIONES

A los efectos del presente Código se entenderá por:

a) ASEDIE: La Asociación Multisectorial de la Información (Sector de Información Comercial).

b) Empresa asociada o miembro: todas y cada una de las empresas de servicios de Información Comercial legitimadas para el ejercicio de la actividad, admitidas en la Asociación y encuadradas dentro del Sector de Información Comercial.

c) Usuario/Cliente: cualquier empresa, organismo y entidad con personalidad jurídica, de naturaleza pública o privada, así como comerciantes o profesionales solicitantes de informes comerciales

d) Titular: persona objeto del informe. Persona física con o sin negocio, así como socios de negocios o empresas, o personas que ocupan cargos de responsabilidad en las mismas, sobre el que se elabora el informe comercial.

e) Informe comercial, de crédito, de solvencia patrimonial o de capacidad financiera: recopilación/sistematización de datos sobre personas físicas dedicadas o no a actividades mercantiles, recabados para actuaciones con trascendencia económica o financiera, créditos, promoción de mercados y elaboración de listas comerciales para tal fin, relaciones administrativas, comerciales o de negocios de diversa índole, etc.

TITULO II: DERECHOS DE LOS TITULARES DE LOS DATOS

ARTICULO 4. INFORMACIÓN EN LA RECOGIDA DE LOS DATOS.

1- Las empresas asociadas, en las visitas personales, conversaciones telefónicas o cualquier otro tipo de comunicaciones que realicen con el titular, en tomo a la recopilación/sistematización de datos, informarán claramente al titular de los fines de la información comercial que pretende, así como de la identidad y dirección de la empresa asociada, responsable del fichero.

2- Cuando se recopilen datos de carácter personal mediante cuestionarios, se ha de poner claramente de manifiesto que los datos recopilados serán utilizados para fines de información comercial, evitando de este modo cualquier inducción a engaño o error a sus titulares en cuanto al fin de la recopilación.

3- Los datos recogidos en cualquiera de las formas indicadas en los dos puntos anteriores, supondrá la existencia del consentimiento del titular de los mismos.

4- No obstante la empresa asociada, estará obligada a facilitar al titular, información ampliatoria al respecto, en el caso de que éste la solicite.

5- Las empresas asociadas podrán hacer uso de datos derivados de relaciones con pasados, actuales y potenciales clientes, debiendo para ello contar con su consentimiento, cuando estos sean personas físicas.

6- No será necesaria la información a que se refiere el apartado 1 del artículo 5 de la LORTAD, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se soliciten o de las circunstancias en que se recaban.

ARTICULO 5. DERECHO DE ACCESO

1- El Titular tendrá derecho a solicitar y obtener información de sus datos de carácter personal, incluidos en los ficheros. Este derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio, que garantice la identificación del afectado.

2- La información podrá consistir en la mera consulta de los ficheros por medio de su visualización o en la comunicación de los datos pertinentes por escrito, mediante carta, certificada o no, copia, telefax o fotocopia, en forma legible e inteligible.

3- El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado en intervalos no inferiores a 12 meses, salvo que el titular acredite un interés legítimo al efecto en cuyo caso podrá ejercitarlo antes.

4- El responsable del fichero deberá resolver sobre la petición de acceso en el plazo máximo de un mes, a contar

desde la recepción de la solicitud. Si transcurrido este plazo no se hubiera respondido a la petición de acceso, ésta se puede entender desestimada a los efectos de interponer la oportuna reclamación ante la Agencia de Protección de Datos.

5- En cualquier caso, el Titular podrá dirigirse al Registro General de Protección de Datos, para obtener información sobre la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

ARTICULO 6. DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

1- Los titulares tendrán derecho a que sean rectificados y completados, o en su caso cancelados los datos personales contenidos en los ficheros siempre que tales datos resulten incorrectos o incompletos.

2- Todo dato rectificado, completado o cancelado deberá notificarse a todas aquellas personas o entidades a las que se les hubiere comunicado.

ARTICULO 7. GRATUIDAD DE LOS DERECHOS

Los derechos anteriormente señalados de Acceso, Rectificación y Cancelación, tendrán siempre el carácter de gratuitos, y por lo tanto, no podrá imponerse condición económica alguna.

TITULO III- ELABORACIÓN DE INFORMES COMERCIALES

ARTICULO 8. LEGISLACIÓN APLICABLE

Los datos conocidos susceptibles de utilización deberán recopilarse y/o sistematizarse para elaborar informes comerciales, de acuerdo con la legislación vigente y con este Código Ético.

ARTICULO 9. UTILIZACIÓN DE LOS DATOS

1- Las empresas asociadas a ASEDIE, en su actividad de recopilación y/o sistematización de datos, utilizarán los que sean adecuados y necesarios a fin de elaborar informes comerciales, relativos a los Titulares.

2- A tales efectos, los datos que habitualmente se utilizarán serán los siguientes:

a) Datos relativos a nombres, direcciones y D.N.I. para identificar a los Titulares y evitar de este modo la confusión con otras personas.

b) Datos tales como edad, formación, experiencia y antigüedad profesional a efectos de determinar tanto la capacidad legal como la capacidad de actuación en la actividad que desarrolla.

c) Datos comerciales que facilitarán el conocimiento de la actividad que desarrolla el Titular.

d) Datos descriptivos económicos y evolutivos del negocio o actividad para determinar la importancia del mismo, la solvencia y seriedad en sus actividades mercantiles y/o crediticias.

e) Datos económicos relativos a los negocios o actividades familiares o de terceras personas que pudiesen respaldar las distintas obligaciones negociales o crediticias del titular del informe.

f) Cualquier otro dato que el propio titular facilite u obtenido con su expreso consentimiento, que se considere conveniente incluir para un mejor conocimiento de la solvencia del titular.

3- Las empresas miembros de ASEDIE utilizarán la información obtenida para la perfecta identificación y descripción de los titulares, y para la correcta descripción de su situación, evolución y valoración.

ARTICULO 10. DATOS DISCRIMINATORIOS

Queda prohibido de forma total y expresa a todas las Empresas miembros de ASEDIE, el obtener, almacenar y difundir, bajo ningún tipo de procedimiento, datos que puedan discriminar a las personas por causa de su origen racial, religión, ideología, creencias, salud, y vida sexual o por cualesquiera otras circunstancias o comportamientos que pertenezcan a la esfera de su vida privada.

ARTICULO 11. RELACIÓN NEGOCIAL

1- Siempre que las empresas asociadas elaboren un informe comercial sobre una persona física, que sea o no titular de un negocio o que desarrolle una actividad mercantil, tendrán del peticionario del mismo una comunicación que indique la existencia efectiva de una relación negocial, contractual, laboral o de crédito entre el usuario del informe y el titular del mismo.

2- El usuario, en todo caso, deberá hacer constar de manera expresa a la empresa asociada a ASEDIE la existencia previa de una relación negocial o contractual entre aquel y el titular.

3- En los supuestos a que se refieren los apartados 1 y 2 de este artículo, no se precisará del consentimiento del Titular para el tratamiento automatizado de los datos de carácter personal ó elaboración del informe comercial, salvo que la ley disponga otra cosa.

TITULO IV: CONSERVACIÓN DE LOS DATOS

ARTICULO 12. DATOS UTILIZADOS

1- Los datos personales utilizados en la elaboración de informes comerciales, han de recopilarse y/o sistematizarse conforme a lo establecido en la LORTAD.

2- En todo caso, el régimen de mantenimiento de los datos será el siguiente:

a) Serán procesados leal y lícitamente poniendo el mayor interés para no incluir ningún elemento que induzca a error o falsedad de los mismos.

b) Serán guardados en relación a los fines legítimos para los que se hayan obtenido, no pudiendo ser utilizados de ningún otro modo incompatible a éstos.

c) Los datos habrán de ser adecuados, pertinentes y no excesivos a la finalidad para la cual se recabaron.

d) Exactos y puestos al día de oficio, cuando las fuentes de obtención de la información así lo permitan, o a instancia de los titulares, de modo que reflejen la situación real del titular.

ARTICULO 13. CANCELACIÓN

1**-** Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin para el cual fueron recabados y registrados.

2- Se conservarán sólo durante el tiempo necesario para servir a los fines en base a los cuales fueron recabados y registrados.

3- Los datos inexactos y caducados serán cancelados y en todo caso sustituidos por los correspondientes datos rectificados. Los datos incompletos deberán ser completados.

4- Cuando los datos sean adversos, se respetará el plazo señalado en el art. 28.3 de la LORTAD.

TITULO V: GARANTÍAS

ARTICULO 14. INTEGRIDAD Y SEGURIDAD

1**-** Cada empresa asociada, responsable de ficheros automatizados, adoptará las medidas exigidas para los ficheros calificados como de nivel medio, según se establece en el apartado 2 del artículo 4 del Reglamento de Medidas de Seguridad aprobado por el Real Decreto 994/1999 del 11 de junio, procurando que los datos reúnan las condiciones necesarias que garanticen su integridad y seguridad, así como respecto de los centros de tratamiento, sistemas, programas, equipos y locales

2- La empresa miembro responsable del fichero adoptará las medidas de índole técnico y organizativo necesarias para garantizar razonablemente la seguridad y confidencialidad de los datos y evitar su alteración, pérdida, tratamiento, acceso no autorizado por terceros, o la transmisión a éstos de igual modo.

3- Las obligaciones a que se refiere el apartado anterior serán exigibles de igual modo a la persona encargada de la gestión, mantenimiento y explotación del fichero respecto de la parte o el total del equipo bajo su responsabilidad.

ARTICULO 15. DEBER DE SECRETO

1- La empresa miembro responsable del fichero y las personas que con la debida autorización por parte de aquella intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos.

2- Esta obligación subsistirá para dichas personas, aún después de finalizar sus relaciones con la empresa asociada responsable del fichero automatizado.

TITULO VI: COMITÉ DE PROTECCIÓN DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL

ARTICULO 16. ORGANIZACIÓN Y FUNCIONAMIENTO

1- Se crea el Comité de protección de tratamiento automatizado de datos personales de ASEDIE

2- Actuará con plena independencia de las empresas miembros de ASEDIE en el ejercicio de sus funciones.

3- El Comité se compondrá de un número de 3 a 5 personas, elegidas por la Junta Directiva de la Asociación a propuesta de la Comisión de Trabajo del sector de Información Comercial. Este Comité podrá asesorarse por consejeros técnicos y jurídicos.

4- Funciones del Comité:

a) Ejercer la potestad sancionadora de acuerdo a lo dispuesto en el título VII de este Código.

b) Podrá autoconvocarse en el caso de que le conste fehacientemente la existencia de una violación flagrante de las normas de este Código.

c) Podrá llegar a acuerdos con asociaciones de consumidores al objeto de que éstas sean consultadas antes de tomar una decisión final.

d) Tomará decisiones en materia de conflictos por la mayoría absoluta de los votos de sus miembros presentes.

e) Oirá a la empresa que se encuentre afectada por un procedimiento, pudiendo asistirse el Comité de los expertos que considere necesarios para resolver.

5- Las deliberaciones del Comité son secretas, quedando sus miembros obligados al mismo

ARTICULO 17. PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

1- Toda persona tendrá derecho de queja cuando tenga constancia de la actuación de una empresa miembro contraviniendo lo dispuesto en la LORTAD o en el presente Código Ético.

2- Este derecho se ejercitará mediante la remisión del escrito de queja al responsable del fichero en los quince días naturales siguientes a ser conocida la actuación que se pretende rectificar, de tal forma que permita tener constancia de su fecha y de su recepción.

3- La queja deberá limitarse a los hechos que contravengan la LORTAD o el presente Código Ético, y su extensión no excederá substancialmente de la de éstos.

4- Siempre que el derecho se ejercite conforme a lo establecido en los párrafos anteriores, el responsable del fichero dispondrá del plazo de un mes, a partir de la notificación de la queja para modificar oportunamente su actuación.

5- Si en el plazo señalado el responsable del fichero no hubiese rectificado su actuación, el titular podrá presentar la queja ante el comité en un plazo de quince días naturales.

6- La solicitud de intervención del citado comité deberá hacerse también por escrito, acompañando la justificación de que se intentó la queja ante el responsable del fichero y aportándose al mismo tiempo todas las pruebas útiles de que se disponga.

7- Todo lo anteriormente señalado, se establece sin perjuicio de la potestad sancionadora que la LORTAD y las disposiciones concordantes, atribuyen a la Agencia de Protección de Datos.

TITULO VII: INFRACCIONES Y SANCIONES

ARTICULO 18. RESPONSABLES

Las empresas responsables de los ficheros quedarán sujetas al régimen sancionador que establece este código, independientemente de lo dispuesto en la LORTAD y sus normas de desarrollo.

ARTICULO 19. TIPOS DE SANCIONES

1- El Comité apreciará, en función de la gravedad del caso y de los daños ocasionados, las sanciones a aplicar.

2- Estas podrán consistir en:

a) Advertencia verbal.

b) Amonestación por escrito.

c) Baja obligatoria en ASEDIE de la empresa sancionada por un período mínimo de tres meses al máximo de 2 años, si es primera falta, y por un período mínimo doble del anterior a un máximo de 5 años, si es una empresa reincidente en esta infracción.

3- El Comité, de forma independiente a las sanciones expuestas en el apartado anterior, podrá exigir a las empresas sancionadas la obligación complementaria de insertar los datos de carácter personal del titular, en la forma que en justicia acuerde el Comité, en todos los informes que del titular se elaboren.

4- Podrá exigir a la empresa sancionada la comunicación efectiva, a todos los usuarios de informes comerciales de que haya sido objeto el titular durante los últimos 12 meses de los datos debidamente expresados y de aquellos que el Comité haya considerado oportuno cancelar y/o modificar.

5- Todo lo anteriormente señalado, se establece sin perjuicio de la potestad sancionadora que la LORTAD y las disposiciones concordantes, atribuyen a la Agencia de Protección de Datos.

ARTICULO 20. NOTIFICACIÓN Y PUBLICIDAD

1- Finalizado el procedimiento, y una vez resuelto, el Secretario del Comité notificará a la empresa asociada y al titular interesado el aviso o sanción impuesta.

2- En todo caso, será competencia del Comité dar publicidad externa a la sanción impuesta, reservándose tal derecho según las circunstancias de cada caso concreto.

TITULO VIII: JURISDICCIÓN

ARTICULO 21. EMPRESAS NO MIEMBROS DE ASEDIE

El Comité contará entre sus atribuciones la iniciación de acciones legales, gozando de capacidad legal suficiente para emprender tales acciones contra empresas que no formen parte de ASEDIE en los supuestos pertinentes y, en todo caso, cuando se vea afectada la credibilidad de la profesión.

MEMORIA DE 1999 - ANEXO VII - RECOMENDACIÓN SOBRE INTERNET DEL CONSEJO DE EUROPA

CONSEJO DE EUROPA
PROTECCIÓN DE DATOS PERSONALES
Recomendación nº R(99)5
DEL COMITÉ DE MINISTROS DE LOS ESTADOS MIEMBROS SOBRE LA PROTECCIÓN DE LA INTIMIDAD EN INTERNET

DIRECTRICES
para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información".
(adoptada por el Comité de Ministros el 23 de febrero de 1999, durante la 660ª reunión de Delegados de Ministros)

Preámbulo

El Comité de Ministros, al amparo del artículo 15.b del Estatuto del Consejo de Europa;

Considerando que la finalidad del Consejo de Europa es realizar una unión más estrecha entre sus miembros;

Observando el desarrollo de las nuevas tecnologías y de los nuevos servicios de comunicación y de información en línea;

Teniendo en cuenta que dicho desarrollo influirá notablemente en el funcionamiento de la sociedad, en general, y de las relaciones entre personas naturales, en concreto ofreciendo mayores posibilidades de comunicación y de intercambio de información tanto a nivel nacional como internacional;

Considerando las ventajas que los usuarios de las nuevas tecnologías pueden obtener de dicho desarrollo;

Considerando, sin embargo, que el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las "autopistas de la información" suponen riesgos para la intimidad de las personas naturales;

Teniendo en cuenta que el desarrollo de las tecnologías también contribuye al respeto de los derechos y las libertades fundamentales, en concreto del derecho a la intimidad, durante el tratamiento de datos de carácter personal referentes a personas físicas;

Considerando la necesidad de desarrollar técnicas que garanticen el anonimato de las personas afectadas y la confidencialidad de la información intercambiada a través de las "autopistas de la información", en el respeto de los derechos y libertades de los demás y de los valores de una sociedad democrática;

Considerando que las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto de la intimidad y del secreto de la correspondencia, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos.

Reconociendo que la recogida, el tratamiento, y, sobre todo, la comunicación de datos de carácter personal a través de las nuevas tecnologías de la información, en concreto de las "autopistas de la información", están regidas por las disposiciones del Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo, 1981, Serie de Tratados Europeos número 108) y por las recomendaciones sectoriales relativas a la protección de datos, en concreto por la Recomendación nº R (90) 19 sobre la protección de datos personales utilizados con fines de cobro y otras operaciones relacionadas, la Recomendación nº R (91) 10 sobre la comunicación a terceros de datos personales poseídos por organismos públicos y la Recomendación nº R (95) 4 sobre la protección de datos personales en el sector de los servicios de telecomunicaciones, referidos sobretodo a los servicios telefónicos;

Pensando que es conveniente sensibilizar a los usuarios y a los proveedores de servicios de Internet sobre la aplicación de las disposiciones generales del Convenio arriba indicado, respecto a la recogida y al tratamiento de datos de carácter personal en las "autopistas de la información",

Recomienda a los Gobiernos de los Estados miembros que difundan ampliamente las directrices contenidas en el anexo de esta Recomendación, sobre todo entre los usuarios y los proveedores de servicios de Internet, así como entre cualquier autoridad nacional encargada de velar por el respeto de la normativa de protección de datos.

Anexo a la Recomendación nº R (99) 5 del Comité de Ministros de los Estados miembros sobre la protección de la intimidad en Internet Directrices para la protección de personas respecto a la recogida y al tratamiento de datos personales en las "autopistas de la información", que pueden integrase o anexionarse a los códigos deontológicos

I. Introducción

Estas directrices enuncian los principios de una conducta honesta que los usuarios y los proveedores de servicios de Interneti deben respetar en materia de protección de la intimidad. Estos principios pueden integrarse en códigos deontológicos.

Los usuarios deberían ser conscientes de la responsabilidad de los proveedores de servicios de Internet y viceversa. Por lo tanto, se aconseja a usuarios y proveedores de servicios de Internet que lean este texto íntegramente, aunque esté dividido en varias partes para que su uso sea más fácil. Usted puede estar afectado por una o por varias partes de este texto simultáneamente.

El uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad. Es importante comportarse de tal forma que uno se proteja y que se promuevan las buenas relaciones con los demás. Estas directrices enuncian algunas soluciones prácticas para la protección de la intimidad, pero no le dispensan de conocer sus derechos y obligaciones.

Recuerde que el respeto de la intimidad es un derecho fundamental de todo individuo que puede ser protegido por leyes sobre la protección de datos. Así pues, le conviene comprobar su situación jurídica.

II. Para los usuarios

1. Recuerde que Internet no es seguro. Sin embargo, existen y se desarrollan diferentes medios que le permiten mejorar la protección de sus datosii. Así pues, utilice cualquier medio que esté a su alcance para proteger sus datos y sus comunicaciones, como la codificación legalmente disponible para el correo electrónico confidencial y los códigos de acceso a su propio PCiii.

2. Recuerde que cada transacción efectuada, cada visita a un sitio en Internet dejan rastros. Estos "rastros electrónicos" pueden utilizarse sin que usted lo sepa para establecer un perfil de su persona y sus intereses. Si usted no quiere que se le haga un perfil, le animamos a que utilice los dispositivos técnicos más avanzados que incluyen la posibilidad de ser informado cada vez que deja usted rastro y a rechazar dicho rastro. También puede usted solicitar que se le informe de las normas de conducta que tienen los diferentes programas y sitios en materia de protección de la intimidad y preferir aquéllos que registran pocos datos o cuyo acceso es anónimo.

3. El acceso y el uso anónimos de los servicios y de los pagos constituyen la mejor protección de la intimidad. Infórmese de los medios técnicos que existen para recurrir al anonimato, si es posibleiv.

4. El anonimato absoluto puede no ser posible debido a limitaciones legales. En tal caso, si la ley lo permite, puede usted utilizar un pseudónimo, de tal forma que su identidad verdadera no sea conocida por su proveedor de servicios de Internet.

5. Comunique únicamente a su proveedor de servicios de Internet o a cualquier otra persona los datos necesarios para un fin concreto del que haya sido usted informado. Tenga mucho cuidado con las tarjetas de crédito y los números de cuenta, que pueden utilizarse con mucha facilidad (de forma abusiva) en Internet.

6. Recuerde que su dirección electrónica constituye un dato de carácter personal y que otras personas pueden querer utilizarla para diferentes fines, como incluirla en guías o en listas de usuarios. No dude en preguntar cuál es la finalidad de dichas guías o de los demás usos. Puede solicitar que su dirección se borre si no desea aparecer en dichas guías o listas.

7. Sea prudente respecto a sitios que solicitan más datos de los necesarios para acceder a ellos o para efectuar una transacción, o con los que no especifican para qué necesitan todos los datos que le conciernen.

8. Recuerde que es usted responsable jurídicamente del tratamiento de datos, por ejemplo, si usted carga o descarga ilícitamente y que, aunque haya usted utilizado un pseudónimo, se le puede identificar.

9. No envíe correo de mala fe, puede volverse contra usted y tener consecuencias jurídicas.

10. Su proveedor de servicios de Internet es responsable del buen uso de los datos. Pregúntele qué datos recoge, trata y conserva, de qué forma y con qué fines. Repítale esta pregunta de vez en cuando. Exíjale que los modifique si no son exactos o que los borre si son excesivos, si no están actualizados o si no son necesarios. Pida a su proveedor de servicios de Internet que notifique dicha modificación a las demás partes a las que haya comunicado sus datosv.

11. Si no está usted satisfecho con la forma que tiene su proveedor de servicios de Internet actual de recoger, tratar, conservar o comunicar sus datos y si éste se niega a modificar su actitud, considere entonces cambiar de proveedor. Si cree usted que su proveedor de servicios de Internet no respeta las normas relativas a la protección de datos, puede usted informar de ello a las autoridades competentes o entablar una acción judicial.

12. Infórmese de los riesgos para al intimidad y la seguridad en Internet, así como de los medios disponibles para reducir dichos riesgos.

13. Si tiene la intención de enviar datos a otro país, debe ser consciente del hecho de que dichos datos pueden estar peor protegidos. Si se trata de sus propios datos, evidentemente es usted libre de enviarlos a pesar de todo. Sin embargo, antes de enviar a otro país datos referentes a otras personas, infórmese, por ejemplo ante sus autoridades, de la posibilidad de efectuar dicha transmisiónvi. Si procede, debe pedir a la persona que recibe los datos que tome las medidasvii necesarias para garantizar la protección de los datos.

III: Para los proveedores de servicios de Internet.

1. Utilice los procedimientos adecuados y las tecnologías disponibles, preferentemente aquéllas que tienen un certificado que garantiza la intimidad de las personas afectadas (incluso si no son usuarios de Internet) y, en concreto, la integridad y la confidencialidad de los datos, así como la seguridad física y lógica de la red y de los servicios suministrados por ella.

2. Informe a los usuarios de los riesgos que el uso de Internet supone para la intimidad, antes de que se inscriban o de que empiecen a utilizar dichos servicios. Puede tratarse de riesgos referidos a la integridad de los datos, a su confidencialidad, a la seguridad de la red u otros riesgos relacionados con la intimidad, como la recogida o el registro de datos llevados a cabo sin que ellos lo sepan.

3. Informe a los usuarios de los medios técnicos que pueden utilizar legalmente para disminuir los riesgos referidos a la seguridad de los datos y las comunicaciones, como la codificación y las firmas electrónicas disponibles legalmente. Ofrezca dichos medios técnicos a un precio basado en los costes que no sea disuasivo.

4. Antes de aceptar abonados y de conectar usuarios a Internet, informe a estos últimos de los medios para acceder a ello, de utilizar los servicios y de pagarlos anónimamente (por ejemplo mediante tarjetas prepagadas). El anonimato absoluto puede no ser posible debido a limitaciones legales. En tal caso, si la ley lo permite, ofrezca la posibilidad de utilizar pseudónimos. Informe a los usuarios de la existencia de programas que permiten buscar y navegar anónimamente por Internet. Diseñe su sistema de tal forma que evite o reduzca al mínimo el uso de datos.

5. No lea, modifique o suprima mensajes enviados a otras personas.

6. No permita ninguna intrusión en el contenido de las comunicaciones, salvo si tal intrusión está prevista por la ley y efectuada por una autoridad pública.

7. Recoja, trate o conserve datos sobre usuarios únicamente si fuere necesario para fines explícitos, concretos y legales.

8. No comunique datos a terceros, salvo si dicha comunicación estuviere prevista por la leyviii.

9. No conserve datos durante un periodo mayor del necesario para alcanzar el objetivo del tratamientoix.

10. Utilice datos para promocionar o comercializar sus propios servicios únicamente si la persona, después de haber sido informada de ello, no ha puesto objeciones o si, en el caso de tratamiento de datos de tráfico o de datos personales, lo ha permitido explícitamente.

11. Es usted responsable del buen uso de los datos. En su página de bienvenida indique mediante una advertencia clara y visible su política respecto a la intimidad. Dicha indicación debería realizar, mediante un hipervínculo, la conexión con una explicación detallada sobre sus prácticas respecto a la intimidad. Antes de que el usuario empiece a utilizar sus servicios, cuando visitare su sitio y cada vez que lo pregunte, infórmele de su identidad, de los datos que recoge, trata y conserva, de qué forma lo hace, para qué fines y durante cuánto tiempo los conserva. Si fuere necesario, pídale su autorización. A petición de la persona afectada, rectifique sin demora los datos erróneos, bórrelos si fueren excesivos, si no estuvieren actualizados o si ya no fueren necesarios y detenga el tratamiento de datos si el usuario se opusiere. Notifique a los terceros a quienes hubiere comunicado los datos cualquier modificación. Evite cualquier recogida de datos efectuada sin que lo sepa el interesado.

12. La información suministrada al usuario debe ser exacta y estar actualizada.

13. íPíenselo dos veces antes de publicar datos en su sitio! Dicha publicación podría atentar contra la intimidad de otras personas y, por ello, estar prohibida por la ley.

14. Antes de enviar datos con destino a otro país, infórmese, por ejemplo ante sus autoridades, de la posibilidad de efectuar dicha transmisiónx. Si procede, debe usted pedir a la persona que recibe los datos que tome las medidas necesarias para garantizar la protección de los datos.

IV Aclaraciones y recursos

1. Cuando en el texto se utilizan los términos "proveedor" o "prestatario del servicio" se aplican también, si procede, a los demás participantes en Internet, tales como los proveedores de acceso, de contenido, de red, los diseñadores de programas de navegación, los coordinadores de foros o de "kioscos de información", etc.

2. Es importante que se asegure que se respetan sus derechos. Los mecanismos de "feedback" ofrecidos por los foros

de Internet, las asociaciones de proveedores de servicios, las autoridades de protección de datos u otras instancias, son medios fundamentales para garantizar el respeto de estas directrices. Póngase en contacto con ellos si necesitare aclaraciones o presentar una reclamación.

3. Las presentes directrices se aplican a cualquier tipo de "autopista de la información".

i Véase parte IV, párrafo I.

ii El término "dato" se refiere a los datos de carácter personal y significa cualquier información que se refiera a usted o a otras personas.

iii Por ejemplo, utilice claves de acceso y modifíquelas con regularidad.

iv Por ejemplo utilizando quioscos de Internet públicos o tarjetas de acceso prepagadas y tarjetas de pago.

v Las leyes de protección de datos, en virtud del artículo 5 del Convenio sobre la protección de personas respecto al tratamiento automatizado de datos de carácter personal, del Consejo de Europa, hace responsable de la exactitud y de la actualización de los datos a quien los tratare.

vi La legislación de muchos países europeos prohibe enviarlos a países que no tuvieren un nivel de protección de datos adecuado o equivalente al de su país. De todas formas hay excepciones, en concreto si la persona afectada ha autorizado que sus datos sean enviados a ese país.

vii Dichas medidas pueden desarrollarse o presentarse, en concreto en el contrato que rija el flujo transfronterizo de datos.

viii Generalmente, las leyes relativas a la protección de datos permiten, en determinadas condiciones, la comunicación a terceros, en concreto:

- de datos personales y de datos de tráfico, con la condición de que la persona afectada lo haya consentido explícita-mente;

- de otros datos cuando la comunicación fuere necesaria para alcanzar la finalidad legítima perseguida o cuando la persona afectada, después de haber sido informada, no se hubiere opuesto.

ix Por ejemplo, no conserve datos de facturación a menos que estuviere previsto por la ley.

x Véase nota 6.

MEMORIA DE 1999 - ANEXO VIII - DOCUMENTOS DEFINITIVOS APROBADOS POR EL GRUPO DE TRABAJO DEL ARTICULO 29 DE LA DIRECTIVA 95/46/CE

DOCUMENTO DE TRABAJO SOBRE EL TRATAMIENTO DE DATOS PERSONALES EN INTERNET
5013/99/ES/final
WP 16
Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales Documento de trabajo:
Tratamiento de datos personales en Internet
Aprobada por el Grupo de Trabajo el 23 de febrero de 1999.2
Documento de Trabajo: Tratamiento de datos personales en Internet

1. Introducción

Cada nueva fase de desarrollo tecnológico plantea un desafío para la protección de los datos personales y el derecho a la vida privada. Las experiencias anteriores que se vivieron con ocasión de la difusión de los ordenadores personales, el comienzo de las aplicaciones telemáticas, etc. lo demuestran. Internet forma parte de estos desafíos al menos por las siguientes razones:

- La utilización de la infraestructura suele estar directamente basada en el tratamiento de datos personales, como ocurre con determinadas direcciones de protocolo Internet.

- Los servicios proporcionados a través de esa infraestructura ofrecen nuevas posibilidades especialmente las relativas a la distribución de información que incluya datos personales (por ej. Listas de direcciones, grupos de discusión, acceso a bases de datos, etc.).

- Los instrumentos técnicos son nuevos, por ejemplo el software de navegación, y evolucionan a un ritmo muy rápido.

- Muchos actores son también nuevos para las nuevas actividades comerciales en línea que implican el tratamiento de datos personales y los límites tradicionales entre las diferentes profesiones se encuentran en un proceso de redefinición igualmente rápido.

- Uno de los usos de Internet que plantea mayores desafíos es hacer negocios en línea: el comercio electrónico consiste en vender directamente y de forma privada de las empresas a los consumidores sin ningún tipo de intermediario, utilizando nuevos métodos de selección y nuevos medios de pago.

- La dimensión global está inmediatamente presente.

En este contexto complejo y, desde el punto de vista de la protección de datos, controvertido las autoridades nacionales de protección de datos han trabajado de manera pragmática durante unos tres años y su experiencia se va consolidando gradualmente (véanse, por ejemplo, sus informes anuales).

De forma similar, el Grupo de Trabajo 1 ha comenzado a estudiar las cuestiones relativas a la aplicación de los principios de la protección de datos al tratamiento de datos personales en Internet de manera pragmática y de acuerdo con la urgencia que el asunto empieza a adquirir a nivel europeo o internacional.

1 Creado en virtud del artículo 29 de 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, DO L 281, 23 de noviembre de 1995, p. 31. Se puede consultar en http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm.3

Podemos poner los siguientes ejemplos:

- Anonimato en Internet 2

- Apoyo al "Memorando de Berlín - Budapest" del Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones 3

- Un primer dictamen sobre el proyecto P3P del Consorcio World Wide Web 4

- Recomendación 1/99 sobre "el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware", aprobada el 23 de febrero de 1999 5 .

El tema de la protección de datos y de la vida privada en Internet se está debatiendo asimismo en foros internacionales como el Consejo de Europa 6 y la OCDE 7 . En relación con la propuesta de la Unión Europea en el sentido de adoptar soluciones globales en el marco de la OMC, esta última ha aceptado incluir la protección de datos en su programa de trabajo sobre los aspectos comerciales del comercio electrónico. Este asunto lo debatirá el Consejo del Comercio de Servicios, que se reúne periódicamente con objeto de presentar un informe antes de junio de 1999. El objetivo es alcanzar un acuerdo sobre los principios obligatorios básicos que permitan un libre flujo de datos personales en el

comercio electrónico mundial a la vez que se respeta el derecho de las personas a la intimidad y, por consiguiente, se garantiza la confianza en el comercio electrónico.
La Conferencia Europea de Comisarios sobre Protección de Datos, celebrada en Dublín los días 23 y 24 de abril de 1998, expresó el deseo de que el Grupo de Trabajo pueda abordar el asunto de una forma más sistemática para clarificar las cuestiones en juego y buscar soluciones encaminadas a contribuir a un desarrollo de Internet y sus servicios conexos que respete el derecho del usuario a la intimidad y, por ello, dé confianza tanto a las aplicaciones comerciales como a las privadas. Los Comisarios recordaron que las reglas derivadas de la legislación comunitaria de protección de datos se aplican en su integridad, de acuerdo con sus correspondientes modalidades, al tratamiento de datos personales en Internet, con independencia de los instrumentos técnicos utilizados.

2 Véase la Recomendación 3/97 del Grupo de Trabajo "Anonimato en Internet", adoptada el 3.12.1997, se puede consultar en: véase la nota 1.

3 Véase la Recomendación 2/97 del Grupo de Trabajo "Informe y orientaciones elaborados por el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones ("Memorando de Budapest - Berlín sobre protección de datos e intimidad en Internet"), aprobada el 3.12.1997, que se puede consultar en: véase la nota 1. 4 Véase el Dictamen 1/98 del Grupo de Trabajo "Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS)", adoptado el 16 de junio de 1998, que se puede consultar en: véase la nota 1.

5 Se puede consultar en: véase la nota 1.

6 El Consejo de Europa está a punto de adoptar unas orientaciones sobre protección de la vida privada en las autopistas de la información.

7 Véanse los resultados de la Conferencia de Ottawa en octubre de 1998: se pueden consultar en http://www.oecd.org

2. La importancia de las directivas sobre protección de datos

El Grupo de Trabajo comparte la opinión de la Conferencia Europea de Comisarios sobre Protección de Datos. Internet no es un vacío jurídico. El tratamiento de los datos personales en Internet debe respetar los principios de protección de datos al igual que en el mundo normal (off-line)8 . Esto no constituye una limitación de la utilización de Internet, sino que, por el contrario, forma parte de los requisitos fundamentales destinados a garantizar la confianza de los usuarios en el funcionamiento de Internet y los servicios que se facilitan mediante esa red. La protección de datos en Internet es, por tanto, una condición indispensable par el desarrollo del comercio electrónico.

La Directiva 95/46/CE, de carácter general sobre la protección de datos hace referencia a cualquier tipo de tratamiento de datos personales dentro de su campo de acción, con independencia de los medios técnicos utilizados. Por consiguiente, el tratamiento de datos personales en Internet debe considerarse a la luz de la directiva.

La Directiva específica 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones 9 complementa la directiva general 95/46/CE mediante la fijación de disposiciones jurídicas y técnicas específicas.10

Internet es una red de ordenadores abierta a todo el mundo y, por ello, forma parte del sector público de telecomunicaciones. Las disposiciones de la Directiva 97/66/CE, por tanto, afectan al tratamiento de los datos personales en relación con la prestación de servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad 11 .

3. El Grupo Operativo Internet

El Grupo de Trabajo es consciente de que la aplicación homogénea de las directivas sobre protección de datos al tratamiento de datos personales en Internet requiere un análisis que tenga en cuenta en particular tanto los aspectos técnicos como los jurídicos. El Grupo de Trabajo tiene la intención de contribuir además a dar respuesta a las numerosas y detalladas cuestiones que pueden plantearse en este contexto.

Con objeto de garantizar un planteamiento coherente y homogéneo sobre el tratamiento de datos en Internet, el Grupo de Trabajo ha creado el Grupo Operativo (Task Force) interdisciplinario Internet, cuya tarea consiste en identificar las cuestiones relacionadas con Internet que necesitan tratarse y preparar los puntos de vista del Grupo de Trabajo sobre el particular.

8 Véase también la Declaración Ministerial de la Conferencia de Bonn sobre redes mundiales, junio de 1997, que se puede consultar en: http://www2.echo.lu/bonn/conference.html.

9 El apartado 3 del artículo 14 de la Directiva 97/66/CE encarga al Grupo de Trabajo establecido con arreglo a la Directiva 95/46/CE a ejercer sus funciones también por lo que se refiere a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las telecomunicaciones, que son objeto de la Directiva 97/66/CE.

10 Para todas las cuestiones que no están cubiertas de forma específica por la Directiva 97/66/CE, incluidas las obligaciones del controlador y los derechos de las personas o los servicios de telecomunicaciones que no están disponibles para el público, se aplica la Directiva 95/46/CE (véase el considerando 11 de la Directiva 97/66/CE).

11 Véase el apartado 1 del artículo 3 de la Directiva 97/66/CE..5

El Grupo Operativo Internet ya ha preparado la Recomendación 1/99 del Grupo de Trabajo sobre el tratamiento invisible y automático de datos personales en Internet efectuados por software y hardware 12 .

El Grupo Operativo Internet va a seguir trabajando de manera más general sobre la aplicación de las dos directivas al tratamiento de datos personales en Internet y presentará propuestas sobre la forma de llevar a la práctica sus disposiciones de manera homogénea, por ejemplo en relación con los servicios de correo electrónico (e-mail) y los datos sobre el tráfico en Internet.

Bruselas, 23 de febrero de 1999

Por el Grupo de Trabajo

El Presidente

Peter HUSTINX

12 Aprobada el 23 de febrero de 1999. Se puede consultar en: véase la nota 1.

RECOMENDACION 1/99 SOBRE EL TRATAMIENTO INVISIBLE Y AUTOMATICO DE DATOS PERSONALES EN INTERNET EFECTUADO POR SOFTWARE Y HARDWARE
5093/98/ES/final
WP 17
Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware
Aprobada por el Grupo de Trabajo el 23 de febrero de 1999.2
Recomendación 1/99 sobre el Tratamiento Invisible y Automático de Datos Personales en Internet Efectuado por Software y Hardware

Aprobada por el Grupo de Trabajo el 23 de febrero de 1999

EL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, Vistos el artículo 29 y el apartado 3 del artículo 30 de la citada Directiva, Visto su Reglamento Interno y, en particular, sus artículos 12 y 14, HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

1. El Grupo de Trabajo anima a la industria informática (software y hardware) a trabajar en productos Internet que respeten la vida privada y que faciliten los instrumentos necesarios para ajustarse a la normativa europea sobre protección de datos.

Una condición para el tratamiento legítimo de los datos personales es que se informe al interesado y se le tenga al corriente del tratamiento en cuestión. Por lo tanto, el Grupo de Trabajo se muestra especialmente preocupado por todos los tipos de operaciones de tratamiento informático que se llevan a cabo actualmente en Internet a través del software y del hardware sin el conocimiento del interesado y que, por consiguiente, son "invisibles" para el mismo. Ejemplos típicos de este tipo de tratamiento invisible son el chattering en el nivel HTTP 1 , los hipervínculos automáticos a terceros, el contenido activo (como Java, ActiveX u otras tecnologías que ejecutan scripts en el cliente) y el mecanismo cookies en su aplicación actual en los navegadores usuales.

2. Los productos (software y hardware) de Internet deberían proporcionar a los usuarios de Internet información sobre los datos que pretenden recopilar, almacenar o transmitir y el fin para el que son necesarios.

Los productos (software y hardware) de Internet deberían asimismo permitir al usuario de los datos un fácil acceso a cualquier dato recopilado que le concierna posteriormente.

1 Esto significa que con la solicitud http se envía más información de la necesaria para contactar con el servidor..3

Esto significa, por ejemplo, que:

- En el caso de un navegador, al establecer una conexión con un servidor web (al enviar una solicitud o al recibir una página Web) se informa al usuario de qué información se pretende transferir y con qué objetivo.

- En el caso de hipervínculos que envía un sitio web a un usuario por el medio que sea, el navegador del usuario debería indicárselos en su totalidad al usuario.

- En el caso de cookies, debería informarse al usuario cuando está previsto que el software de Internet reciba, almacene o envíe un cookie. El mensaje debería especificar, en un lenguaje normalmente comprensible, qué información se pretende almacenar en el cookie y con qué objetivo así como el periodo de validez del cookie.

3. La configuración de los productos informáticos (hardware y software) no debería, por defecto, permitir la recopilación, almacenado o envío de información persistente del cliente 2 . Por ejemplo:

- El software navegador debería, por defecto, estar configurado de tal forma que sólo pudiera tratarse la mínima cantidad de información necesaria para establecer una conexión Internet. Los cookies deberían, por defecto, no ser enviados ni almacenados.

- Durante su instalación, una función del navegador concebida para almacenar y enviar datos sobre la identidad o el comportamiento comunicativo del usuario (perfil) no debería rellenarse automáticamente con datos previamente almacenados en el equipo informático del usuario.

4. Los productos Internet (hardware y software) deberían permitir al interesado decidir libremente en cuanto al tratamiento de sus datos personales ofreciéndole instrumentos de fácil manejo para filtrar (es decir rechazar o modificar) la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados (incluidos los perfiles, el dominio o la identidad del servidor Internet, el tipo y duración de la información recopilada, almacenada o enviada y así sucesivamente). El usuario debería disponer de instrucciones claras sobre el uso tanto del software como del hardware para la aplicación de esas opciones e instrumentos. Por ejemplo:

2 Información persistente del cliente es un término técnico (no jurídico) que hace referencia a la información relacionada con el cliente (el PC del usuario) y que permanece más de una sesión en el equipo informático. Una sesión comienza cuando el cliente solicita una página en un sitio Web determinado y termina cuando decide apagar el programa de navegación o el ordenador, o cuando solicita una página de otro sitio Web. Los cookies son un ejemplo típico de información persistente del cliente, y lo mismo ocurre con las preferencias relativas a la vida privada..4

- Eso significa que el software navegador debería proporcionar opciones para que el usuario pueda configurar el navegador, especificando el tipo de información que debería o no debería recopilar y transmitir.

- Eso significa en el caso de los cookies que el usuario debería contar siempre con la opción de aceptar o rechazar el envío o almacenamiento de un cookie en su totalidad. Asimismo el usuario debería disponer de opciones para determinar los elementos de información que se van a conservar o eliminar de un cookie, en función por ejemplo del periodo de validez del cookie o los sitios Web de envío y recepción.

5. Los productos (software y hardware) Internet debería permitir que los usuarios eliminen la información persistente del cliente de una manera simple y sin que el remitente se vea afectado. El usuario debería contar con instrucciones claras para poder realizar todas estas operaciones. Si no se puede eliminar la información, deberá existir una forma fiable de evitar su transferencia y lectura.

- Los cookies y demás información persistente del cliente deberían almacenarse de una forma normalizada y permitir un borrado selectivo en el ordenador del cliente.

ANTECEDENTES

Actualmente, es casi imposible utilizar Internet sin verse confrontado con una serie de hechos que invaden nuestra vida privada y que llevan a cabo todo tipo de operaciones de tratamiento de datos personales de manera invisible para el interesado. En otras palabras, el usuario de Internet no es consciente de que sus datos personales se han recopilado y, posteriormente, tratado y podrían usarse con intenciones que le son desconocidas. El interesado no conoce el tratamiento y no es libre para decidir sobre el particular.

En ejemplo de este tipo de técnica es el denominado cookie, que se puede definir como una ficha de información informatizada que se envía desde un servidor web al ordenador de un usuario con objeto de identificar en el futuro ese ordenador en sucesivas visitas al mismo sitio web.

Los navegadores son programas de software destinados, entre otras cosas, a visualizar gráficamente material disponible en Internet. Los navegadores comunican entre el ordenador del usuario (cliente) y el ordenador remoto donde está almacenada la información (servidor Web). Los navegadores suelen enviar al servidor Web más información de la estrictamente necesaria para establecer la comunicación. Los navegadores tradicionales envían automáticamente al servidor Web visitado el tipo y la lengua del navegador, el nombre de otros programas instalados en el PC y el sistema operativo del usuario, la página de referencia, cookies, etc. Dichos datos.5 también se pueden transmitir sistemáticamente a terceros mediante el software del navegador, de manera invisible.

Estas técnicas permiten la creación de rastros de cliqueo sobre el usuario de Internet.

Los rastros de cliqueo consisten en información sobre el comportamiento, la identidad, el recorrido efectuado o las elecciones expresadas por la persona al visitar el sitio web y contienen los vínculos por los que ha pasado un usuario y que están registrados en el servidor web.

Las Directivas europeas 95/46/CE y 97/66/CE sobre protección de datos contienen disposiciones detalladas para la

protección de las personas en lo que respecta al tratamiento de datos personales. Las dos directivas son pertinentes para las situaciones tratadas en esta recomendación ya que los datos personales que afectan a los usuarios de Internet se tratan en este contexto. Los cookies o los navegadores pueden contener o volver a tratar datos que permitan una identificación directa o indirecta del usuario individual de Internet.

La aplicación de las disposiciones sobre el tratamiento adecuado, las causas legítimas de tratamiento y el derecho del interesado a decidir sobre el tratamiento de sus propios datos han dado lugar a esta recomendación.

El Grupo de Trabajo está especialmente preocupado por los riesgos inherentes al tratamiento de los datos personales sobre personas que desconocen por completo tal tratamiento. Se insta a los conceptores de software y hardware, por tanto, a tomar en consideración y respetar los principios de estas directivas con objeto de incrementar la intimidad de los usuarios de Internet.

Bruselas, 23 de febrero de 1999

Por el Grupo de Trabajo

El Presidente

Peter HUSTINX

RECOMENDACION 2/99 SPBRE LA PROTECCION DE LA INTIMIDAD EN EL CONTEXTO DE LA INTERCEPTACION DE LAS TELECOMUNICACIONES
5005/99/def.
WP 1
Grupo de trabajo sobre la protección de la persona por lo que respecta al tratamiento de datos personales.
Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones.
Adoptada el 3 de Mayo de 1999.2
Recomendación sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones
EL GRUPO DE PROTECCIÓN DE LAS PERSONAS POR LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES,
Creado por la Directiva 95/46/C del Parlamento Europeo y del Consejo, de 24 de octubre de 1995

1, Considerando del artículo 29 y los apartados 1 y 3 del artículo 30 de la Directiva

2, Considerando su reglamento interno, y en particular los artículos 12 y 14 de este último,

Ha adoptado la presente recomendación:

El objetivo de la recomendación consiste en recordar la aplicación de las medidas adoptadas a nivel europeo en cuanto a interceptación de las telecomunicaciones, de los principios de protección de los derechos y libertades fundamentales de las personas físicas, y, en particular, de su intimidad y del secreto de la correspondencia.

El ámbito de aplicación de la presente recomendación contempla las interceptaciones en sentido amplio, es decir, la interceptación del contenido de las telecomunicaciones, pero también los datos correspondientes a las telecomunicaciones, y, en particular, posibles medidas preparatorias (tales como el "monitoring" y el "datamining" de los datos de tráfico) que se pudieran prever con el fin de decidir la oportunidad de la interceptación del contenido de la telecomunicación

3."A. Alcance de las disposiciones adoptadas a nivel europeo en cuanto a interceptación de las comunicaciones

1 Directiva 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 DO L 281 de 2.11.1995, p 1.

2 Los tres miembros que representan respectivamente el Registertilsynet (Dinamarca), la Commission Nationale de l'Informatique et des Libertés (CNIL, Francia) y el Data Protection Register (Reino Unido), no participaron en el voto de esta recomendación, considerando que el asunto tratado no era competencia del grupo. Con todo dan su apoyo , de un modo general, en cuanto al fondo de la recomendación.

3 Este carácter amplio del concepto de interceptación de las telecomunicaciones corresponde al ámbito de aplicación de la Resolución del Consejo del 17 de enero de 1995 relativa a la interceptación legal de las telecomunicaciones, ya citada (Capítulo A.1.), y al marco general de las disposiciones jurídicas aplicables sobre este tema (véase más adelante, Capítulo B.).

La recomendación se aplica así a la interceptación de las telecomunicaciones no públicas en Internet. Se presta especial atención a la problemática general del tratamiento de datos personales vinculada al desarrollo de la red Internet por el grupo de protección de las personas respecto al tratamiento de los datos personales, en el marco de trabajos realizados en paralelo por el "grupo de trabajo Internet" del grupo .3

1. La Resolución del Consejo de 17 de enero de 1995 relativa a la interceptación legal de las telecomunicaciones 4 enumera las condiciones técnicas necesarias para la interceptación de las telecomunicaciones, sin abordar la cuestión de las condiciones en las que deberían tener lugar tales interceptaciones. El texto de la Resolución prevé una obligación por parte los operadores de redes o proveedores de servicios de proporcionar ya descifrados a los «servicios autorizados» los datos interceptados. Estos datos abarcan las llamadas telefónicas, móviles o no, los correos electrónicos, los mensajes fax y télex, los flujos de datos Internet, tanto por lo que se refiere al conocimiento del contenido de las telecomunicaciones como de los datos sobre las telecomunicaciones (en particular, los datos de tráfico, pero también todas las señales emitidas por la persona supervisada - apartado 1.4.4. de la Resolución).

Los datos se refieren a la persona supervisada, a las personas que la llaman y a las personas a quienes ésta llama 5. La Resolución prevé también que la localización geográfica de los abonados de servicios móviles constituya un dato al cual deben tener acceso los servicios autorizados 6. Esta Resolución de 1 de enero de 1995 está actualmente siendo objeto de una revisión, uno de cuyos principales objetivos es adaptarla a las nuevas tecnologías de la comunicación. El texto en proyecto precisa en particular la aplicación de las medidas de interceptación a las telecomunicaciones por satélite 7.

2. Las reflexiones del grupo de trabajo se refieren al ámbito de aplicación de las medidas previstas por la Resolución del Consejo de 17 de enero de 1995. Una versión no publicada del documento antes citado y posterior a éste («declaración de intenciones» con fecha de 25 de octubre de 1995) prevé que los signatarios del texto puedan ponerse en contacto, por lo que se refiere a las especificaciones en cuanto a interceptación de las telecomunicaciones, con el director del «Federal Bureau of Investigation» de los Estados Unidos. El texto prevé por otro lado que, con el consentimiento de los «participantes», otros Estados puedan participar en el intercambio de información, en la revisión y en la actualización de las especificaciones. El grupo observa, por una parte, que el estatuto jurídico de este texto - en particular su firma efectiva por los países implicados - no queda claro y que no constituye, en el sentido de la jurisprudencia citada del Tribunal Europeo de Derechos Humanos, una medida accesible al ciudadano al no ser objeto de publicación alguna. Por otra parte, este texto confirma la voluntad de desarrollar medidas técnicas de interceptación de las telecomunicaciones en concertación con Estados no sujetos a las exigencias del Convenio Europeo de Derechos Humanos y de las Directivas 95/46/C y 97/66/C.

4 DO C 29 de 14.11.1996.

5 Artículo 1.4 del Anexo de la Resolución del Consejo de 17 de enero de 1995.

6 Artículo 1.5, ibid.

7 Documento 10951/1/98, Enf p l 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enf /6 2/1.htm). Parece que una versión aún más reciente ha recibido el acuerdo del grupo de trabajo sobre cooperación policial del Consejo y que se ha transmitido al Parlamento Europeo para que éste pueda adoptarlo o modificarlo . Se prevé al parecer que el Consejo adopte la nueva Resolución los días 27-28 de mayo de 1999 (véase "Datenschutz-Berater", 15.02.99, p 5, que hace referencia a una versión no pública de 20.01.99). La comisión jurídica del Parlamento europeo recomendó a la comisión sobre libertades públicas (coordinador) rechazar el proyecto de revisión de la recomendación del Consejo tal como se propone en ENFOPOL 98, entre otras cosas por razones de protección de la intimidad y por la entrada en vigor inminente del Tratado de Amsterdam (véase informe Fl ri). La comisión de libertades públicas no siguió este dictamen y propondrá al Pleno que apruebe ENFOPOL 98 sobre la base del informe Schmid. El Parlamento Europeo debería tomar una decisión a principios de mayo.4

3. El grupo constata que el texto de la Resolución del Consejo pretende resolver cuestiones técnicas relativas a las modalidades de interceptación de las comunicaciones, sin poner en causa las disposiciones nacionales que regulan las escuchas desde el punto de vista jurídico. Resulta, sin embargo, que algunas medidas previstas por la Resolución y destinadas a ampliar las posibilidades de interceptación de las comunicaciones están en contradicción con las disposiciones nacionales, más protectoras, de ciertos países de la Unión Europea (en particular: apartado 1.4, comunicación de los datos correspondientes a las llamadas, incluidas las llamadas de los usuarios móviles, sin tomar en consideración los servicios anónimos y pagados por adelantado actualmente disponibles; apartado 1.5, localización geográfica de los usuarios móviles; apartado 5.1, prohibición a los operadores de revelar a posteriori las interceptaciones realizadas).

4. Si bien la Resolución del Consejo se inscribe en un objetivo «de protección de los intereses nacionales, de seguridad nacional e investigación de crímenes graves», el grupo desea llamar la atención sobre los riesgos de deriva por lo que respecta a los objetivos de las escuchas, riesgos que se verían aumentados por una extensión a un número creciente de países - exteriores algunos a la Unión Europea - de las técnicas de interceptación y descifrado de las telecomunicaciones.

Una resolución oficial del Parlamento Europeo de 16 de septiembre de 199 sobre las relaciones transatlánticas 8, «considera que la importancia creciente de la red Internet, de las telecomunicaciones a escala mundial, en general, pero sobre todo del sistema ECHELON, así como los riesgos de su utilización abusiva, exigen la adopción de medidas de protección de las informaciones económicas y de un cifrado eficaz.»

Estas consideraciones ponen de relieve los riesgos vinculados a una interceptación de las telecomunicaciones que sobrepase el marco estricto de las cuestiones de seguridad nacional - e incluso el marco del "tercer pilar" de la Unión Europea. Plantean asimismo la cuestión de su legitimidad, en particular, a la luz de las obligaciones que se derivan de

los textos de derecho comunitario en cuanto a protección de los derechos y libertades fundamentales de las personas físicas, y, en particular, de su intimidad.

8 Sesión plenaria, parte II, B4-080 , 0805, 0806 y 0809/98..5

5. El grupo destaca finalmente que la entrada en vigor del Tratado de Amsterdam implicará un cambio de base jurídica a nivel europeo por lo que se refiere a las medidas de interceptación de las telecomunicaciones. La competencia actual del Consejo para elaborar el texto de la Resolución, basada en el apartado 9 del artículo K.1 y en el apartado 2 del artículo K.3 del Tratado relativos a la cooperación policial y judicial, se convertirá en una competencia de iniciativa de la Comisión Europea sobre la base del apartado 2 del nuevo artículo K.6.

B. Cuadro jurídico general

6. El grupo recuerda que cada interceptación de telecomunicación, entendida como el conocimiento de una tercera parte del contenido y/o de los datos asociados a las telecomunicaciones privadas entre dos o varios corresponsales, en particular los datos de tráfico vinculados a la utilización de los servicios de telecomunicación, constituye una violación del derecho a la intimidad de los individuos y del secreto de la correspondencia.

Sólo puede por lo tanto admitirse una interceptación si responde a tres requisitos fundamentales, de acuerdo con el apartado 2 del artículo del Convenio Europeo de Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950 9, y de la interpretación reservada a esta disposición por el Tribunal Europeo de Derechos Humanos: un fundamento jurídico, la necesidad de tal medida en una sociedad democrática y la conformidad con uno de los objetivos legítimos enumerados en el Convenio 10. El fundamento jurídico deberá definir precisamente los límites y modalidades de su ejercicio, por medio de normas claras y detalladas, necesarias sobre todo debido al perfeccionamiento continuo de los medios técnicos utilizables 11. Este texto legal debe ser accesible al público para que el ciudadano pueda prever las consecuencias de su comportamiento 12. En este contexto jurídico debe prohibirse la vigilancia exploratoria o general de las telecomunicaciones a gran escala 13.

7. En la Unión Europea, la Directiva 95/46/C 14 consagra el principio de la protección del derecho a la intimidad inscrito en los sistemas jurídicos de Estados miembros. Esta

9 Conviene destacar que las garantías fundamentales reconocidas por el Consejo de Europa en cuanto a intercepta - ción de las comunicaciones generan obligaciones a cargo de los Estados independientemente de las distinciones que existan en la Unión Europea en función del carácter comunitario-intergubernamental de los ámbitos abordados.

10 El Convenio n° 108 del Consejo de Europa prevé también que sólo se tolerará una medida de injerencia cuando constituya una medida necesaria en una sociedad democrática para la protección de los intereses nacionales enume - rados en el apartado 2 de su artículo 9 (se tendrá en cuenta que los intereses nacionales enumerados en el Convenio 108 y en el Convenio de Protección de Derechos Humanos no son exactamente iguales), y cuando esté estrictamente definida respecto a esta finalidad.

11 Véanse a este respecto, más adelante, las obligaciones previstas por el artículo 4 de la recomendación n° 4 del Consejo de Europa sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, respecto, en particular, a los servicios telefónicos, de 7 de febrero de 1995

12 Sentencias Huvig y Kruslin contra Francia de 25 de abril de 1990, serie A n° 176 A y B, p 15 y s.

13 Véanse, en particular, las sentencias Klass, de 6 de septiembre de 1978, serie A n° 28, p 2 y s, y Malone, de 2 de agosto de 1984, serie A n° 82, p 0 y s.

La sentencia Klass, así como la sentencia Leander de 25 de febrero de 1987, hacen hincapié en la necesidad de "garantías suficientes contra los abusos, ya que un sistema de vigilancia secreta destinado a proteger la seguridad nacional crea el riesgo de minar, o incluso de destruir, la democracia pretendiendo defenderla" (Sentencia Leander, serie A n° 116, p 14 y s).

El Tribunal observa en la sentencia Klass (apartados 50 y s) que la valoración de la existencia de garantías adecuadas y suficientes contra los abusos depende de todas las circunstancias de la causa. Considera en la sentencia en cuestión que las medidas de vigilancia previstas por la legislación alemana no autorizan la vigilancia exploratoria o general y no infringen el artículo 8 del Convenio europeo de protección de los derechos humanos. Las garantías previstas por la ley alemana son las siguientes: sólo pueden efectuarse medidas de vigilancia cuando ciertos indicios permitan sospechar que alguien proyecta realizar, realiza o ha realizado infracciones graves; sólo pueden prescribirse si el esclarecimiento de los hechos por otros medios está llamado al fracaso presenta considerables obstáculos; incluso en ese caso la vigi - lancia sólo podrá referirse a la persona del sospechoso a las personas presuntamente en contacto con éste.

6. Directiva precisa los principios contenidos en el Convenio Europeo de Protección de los Derechos Humanos de 4 de noviembre de 1950 y en el Convenio de 2 de enero de 19 1 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales. La Directiva 97/66/C 15 concreta las disposi - ciones de esta Directiva y precisa la obligación de los Estados miembros de proteger el 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. Según el apartado 1 del artículo 13 de la Directiva 95/46/C, un Estado miembro puede adoptar medidas legislativas destinadas a limitar el

alcance de determinadas obligaciones (por ejemplo acerca de la recogida de datos) y determinados derechos (por ejemplo el derecho a ser informado en caso de recogida de datos) previstos por la Directiva 16. Estas excepciones se enumeran taxativamente: la limitación debe constituir una medida necesaria para proteger los intereses públicos enunciados de manera exhaustiva en las letras a) a g) de este artículo, tales como la seguridad del Estado, la defensa, la seguridad pública o la prevención, investigación, detección y represión de infracciones penales. En el apartado 1 del artículo 14, la Directiva 97/66/C precisa también que los Estados miembros sólo pueden restringir la obligación de confidencialidad de las comunicaciones a través de redes públicas cuando tal medida constituya una medida necesaria para salvaguardar la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección y represión de infracciones penales.

C. Obligaciones de lo operadores y de los proveedores de servicios de telecomunicación.

Hay que hacer hincapié en el hecho de que las obligaciones de seguridad y confidencialidad de los datos a las que se somete a los operadores de telecomunicaciones, a los proveedores de servicios y a los stados miembros, respectivamente sobre la base de los apartados 1 y 2 del artículo 17 de la Directiva 95/46 y sobre la base de los artículos 4, 5 y 6 de la Directiva 97/66/C, constituyen el principio y no la excepción.

El grupo recuerda que estas obligaciones se imponen también de manera general a los operadores con arreglo al artículo 7 del Convenio del Consejo de Europa n° 10 para la protección de las personas respecto al tratamiento de los datos personales, de 2 de enero de 19 1, y del artículo 4 de la Recomendación n°4 del Consejo de Europa sobre protección de datos personales en el ámbito de los servicios de telecomunicaciones, de 7 de febrero de 1995 17, que tiene en cuenta, en particular, a los servicios telefónicos.

14 Se deberá tener en cuenta que el artículo de la Directiva 95/46/CE excluye de su ámbito de aplicación los tratamientos de datos personales en el ejercicio de actividades no incluidas en el ámbito de aplicación del Derecho comunitario, y los tratamientos cuyo objeto sea la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado relativas a ámbitos de derecho penal. La mayoría de los Estados miembros que transponen esta Directiva no han establecido sin embargo hasta ahora, en sus leyes nacionales, una distinción según la cual esta ley no se aplicaría a las materias no cubiertas por el Derecho comunitario.

Hay que añadir que, a partir del momento en que se aplica en el marco de la Directiva un tratamiento de datos (por ejemplo, la lista de las llamadas registradas para facturación por un operador), pero que en una segunda fase es objeto de un tratamiento consistente en una interceptación de estos datos, deben aplicarse las disposiciones de Derecho comunitario. La Directiva 95/46/CE prevé a este respecto una serie de garantías que deben respetarse en el marco de estas interceptaciones, y que se exponen a continuación.

15 Directiva de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la pro tección de la intimidad en el sector de las telecomunicaciones, DO L 24 de 0 de enero de 1998, p.1.

16 Previstos en el apartado 1 del artículo 6 - principios relativos a la calidad de los datos, en el artículo 10, en el apartado 1 del artículo 11 - información a la persona en cuestión, y en los artículos 12 - derecho de acceso y 21 - publicidad de los tratamientos.

7. Estas obligaciones implican, por una parte, que los operadores de telecomunicación y los proveedores de servicios sólo pueden tratar los datos relativos al tráfico y a la facturación de las telecomunicaciones cumpliendo determinadas condiciones: a partir del principio de que los datos referentes al tráfico relativos a abonados y usuarios deben borrarse o tornarse anónimos en cuanto termina la comunicación, se deduce que las finalidades para las cuales pueden tratarse los datos, la duración de su posible conservación, así como el acceso a dichos datos están estrictamente limitados18.

10. Por otra parte, los operadores de telecomunicaciones y los proveedores de servicios de telecomunicaciones deben adoptar las medidas necesarias con el fin de hacer técnicamente difíciles o imposibles, según el estado actual de la técnica, la interceptación de las telecomunicaciones por instancias no autorizadas por la ley. El grupo destaca a este respecto que la aplicación de medios eficaces de interceptación de las comunicaciones con fines legítimos, utilizando precisamente las técnicas más avanzadas, no debe tener por consecuencia reducir el nivel general de confidencialidad de las comunicaciones y de protección de la intimidad de las personas.

Estas obligaciones toman un sentido particular cuando las telecomunicaciones entre personas situadas en el territorio de los Estados miembros transiten o puedan transitar por el exterior del territorio europeo, en particular en la utilización de satélites o de Internet.

11. En la medida en que sea de aplicación la Directiva 95/46/C , el hecho de hacer accesibles tales telecomunicaciones en el exterior de la Unión Europea podría por otra parte constituir una violación de su artículo 25, dado que los organismos extranjeros que interceptan los datos no necesariamente pueden pretender garantizar un nivel adecuado de protección.

17 "4.1. No deberían comunicarse los datos personales recogidos y tratados por los concesionarios de red o los proveedores de servicios, a menos que el abonado interesado haya dado por escrito su consentimiento claro y explícito y que la información comunicada no permita identificar a los abonados llamados. El abonado puede retirar su consentimiento en cualquier momento pero no con efecto retroactivo.

4.2. Los datos personales recogidos y tratados por los concesionarios de red o los proveedores de servicios pueden comunicarse a las autoridades públicas si esta comunicación está prevista por la ley y constituye una medida necesaria, en una sociedad democrática:

a. para la protección de la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado la represión de las infracciones penales;

b. para la protección de la persona en cuestión y los derechos y libertades de otros.

4. . En caso de comunicación de datos personales a autoridades públicas, el derecho interno debería regular:

a. el ejercicio de los derechos de acceso y rectificación por parte de la persona interesada;

b. las condiciones en las cuales las autoridades públicas competentes tendrán derecho a negarse a dar información a la persona interesada o a diferirla;

c. la conservación o destrucción de estos datos."

18 Véanse en particular las obligaciones del artículo 6 de la Directiva 97/66/CE. Estas obligaciones plantean algunos interrogantes en cuanto a las prácticas que se desarrollan actualmente entre los prestadores de servicios de telecomu - nicación y que consisten en un examen general y previo de los datos de tráfico de los suscriptores, con objeto de identi - ficar el comportamiento sospechoso de algunos abonados - y eventualmente permitir la interceptación específica del contenido de ciertas telecomunicaciones.

D. Respeto de las libertades fundamentales por parte de las autoridades públicas en el ámbito de las interceptaciones

12. Es importante que el derecho nacional precise de manera rigurosa y tomando en cuenta todas las disposiciones previamente mencionadas:

- Las autoridades habilitadas para permitir la interceptación legal de las telecomunicaciones, los servicios autorizados para proceder a las interceptaciones y el fundamento jurídico de su intervención,

- Las finalidades según las cuales pueden tener lugar tales interceptaciones, que permitan apreciar su proporcionalidad respecto a los intereses nacionales en juego,

- La prohibición de cualquier vigilancia exploratoria o general de las telecomunicaciones a gran escala,

- Las circunstancias y condiciones precisas (por ejemplo elementos de hecho que justifiquen la medida, duración de la medida) a las cuales están sometidas las interceptaciones, en cumplimiento del principio de especificidad al que se supedita toda injerencia en la intimidad de otros 19,

- El respeto de este principio de especificidad, corolario de la prohibición de cualquier vigilancia exploratoria o general, que implica, por lo que se refiere concretamente a los datos de tráfico, que las autoridades públicas no pueden tener acceso a estos datos sino con carácter particular, y no de manera general y proactiva,

- Las medidas de seguridad por lo que se refiere al tratamiento y el almacenamiento de los datos, y la duración de su conservación,

- Por lo que se refiere a las personas implicadas de manera indirecta o aleatoria 20 en las escuchas, las garantías particulares referentes al tratamiento de los datos personales: en particular, los criterios que justifican la conservación de los datos, y las condiciones de la comunicación de estos datos a terceros,

- La información a la persona supervisada, lo antes posible 21,

19 Véase más arriba, nota 1

20 Los datos que aquí se contemplan se refieren a personas que no son objeto de medidas de vigilancia, pero cuyo corresponsal sí es objeto de tales medidas; por ejemplo: número de teléfono marcado por la persona supervisada y correspondiente a uno de los progenitores de este último; localización geográfica de personas en contacto por teléfono móvil con la persona objeto de escucha.

21 La persona bajo vigilancia debería en efecto poder ser informada a partir del momento en que la información no perjudica o ya no perjudicó más a la investigación.

9. - Los tipos de recurso que puede ejercer la persona supervisada 22,

- Las modalidades de vigilancia de estos servicios por una autoridad de control independiente 23,

- La publicidad - por ejemplo en forma de informes estadísticos regulares - de la política de interceptación de las tele - comunicaciones efectivamente practicada 24,

- Las condiciones precisas en las que pueden comunicarse los datos a terceros en el marco de acuerdos bilaterales o multilaterales.

Hecho en Bruselas, a 3 de Mayo de 1999

En nombre del grupo

Peter HUSTINX

Presidente

22 La sentencia Leander antes citada recuerda que el órgano ante el cual puede presentarse el recurso "no es necesario que sea una institución judicial strictu sensu, pero sí que sus poderes y las garantías de procedimiento de que dispone permitan apreciar la eficacia del recurso". Este recurso "debe ser un recurso lo más efectivo posible, habida cuenta de las limitaciones inherentes a todo sistema de vigilancia secreta destinado a proteger la seguridad nacional" (8 y 84).

23 La sentencia Leander contempla el control democrático de las interceptaciones cuando precisa que "incumbe al Parlamento y a instituciones independientes [del Gobierno] velar por el buen funcionamiento del sistema" (64).

24 Esta exigencia de publicidad, así como, en particular, la necesidad de un control de las interceptaciones por una autoridad independiente, se mencionan en el "Common position on public accountability in relation to interceptation of private communications" adoptada en Hong Kong el 15 de abril de 1998 por el grupo internacional de trabajo sobre protección de datos en el sector de las telecomunicaciones.

RECOMENDACION 3/99 SOBRE LA CONSERVACION DE LOS DATOS SOBRE TRAFICO POR LOS PROVEEDORES DE SERVICIO INTERNET A EFECTOS DE CUMPLIMIENTO DE LA LEGISLACION
5085/99/ES/FINAL
WP 25
GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES
Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet

A efectos de cumplimiento de la legislación

Introducción

La persecución del delito informático se considera cada vez más importante a escala internacional

Los países del G8 han adoptado un plan de acción de diez puntos que actualmente están poniendo en práctica con ayuda de un subgrupo especializado en delitos de alta tecnología compuesto por representantes de las autoridades de control de los países del G8. Uno de los partidos más destacados y polémicos es la conservación de los datos sobre tráfico, tanto histórico como futuro, por parte de los proveedores de servicio Internet efectos de cumplimiento de las disposiciones legislativas y su puesta a disposición de las autoridades de control. El subgrupo de delitos de alta tecnología del G8 propondrá recomendaciones para garantizar la posibilidad de conservar y proporcionar dichos datos sobre tráfico. Los Ministros de Justicia e Interior del G8 analizarán estas recomendaciones en la reunión que se celebrará en Moscú los días 19 y 20 de octubre de 1999. El Grupo de protección de las personas en lo que respecta el tratamiento de datos personales es consciente de la importante función que pueden ejercer los datos sobre tráfico en el contexto de la investigación de delitos cometidos a través de Internet, pero desea recordar a los poderes públicos nacionales los principios de protección de los derechos fundamentales y las libertades de las personas, y en particular, el derecho a la intimidad y el secreto de la correspondencia que se deben tener en cuenta en este aspecto.

El Grupo comprende que los Ministros de Justicia e Interior del G8 pueden verse obligados a solicitar una interpretación equilibrada de las dos Directivas comunitarias relativas a la protección de datos en la fase de transposición, interpretación que tendrá en cuenta el interés por el control de su aplicación junto con el interés por el respeto a la intimidad.

El Grupo también es consciente de las cargas adicionales que deberían soportar los operadores de telecomunicaciones y proveedores de servicio.

Por consiguiente, el objetivo de la presente Recomendación es contribuir a una aplicación uniforme de las Directivas 95/46/CE y 97/66/CE con vistas a definir condiciones claras y predecibles para los operadores de telecomunicaciones y los proveedores de servicio Internet, así como para las autoridades de control, que protejan simultáneamente el derecho la intimidad.

Situación jurídica

En la Unión Europea, la Directiva 95/46/CE armoniza las condiciones de protección del derecho a la intimidad consagrado en los sistemas jurídicos de los Estados miembros. Esta Directiva otorga contenido y amplía los principios incluidos en el Convenio Europeo para la protección de los Derechos Humanos de 4 de noviembre de 1950 y en el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981 para la protección de las personas en relación con el

tratamiento automático de datos personales. La Directiva 97/66/CE adapta las disposiciones de dicha Directiva al sector de telecomunicaciones. Ambas Directivas se aplican al tratamiento de los datos personales en Internet, incluidos los datos sobre tráfico relacionados con abonados y a usuarios.

En concreto, los artículos 6, 7, 13 y los apartados 1 y 2 del artículo 17 de la Directiva 95/46/CE y los artículos 4, 5, 6 y 14 de la Directiva 97/66/CE tratan la legitimidad de dicho tratamiento por los operadores de telecomunicaciones y proveedores de servicio.

Estas disposiciones permiten los operadores de telecomunicaciones y los proveedores de servicios de telecomunicación tratar los datos sobre el tráfico de telecomunicaciones en condiciones muy limitadas.

La letra b) del apartado 1 del artículo 6 dispone que estos datos sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines. La letra e) del apartado 1 del artículo 6 establece que los datos personales sean conservados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. El artículo 13 permite los Estados miembros limitar el alcance del apartado 1 del artículo 6, entre otros, cuando tal limitación constituya una medida necesaria para la salvaguardia de la seguridad del Estado, la seguridad pública o la prevención, investigación, detección y represión de infracciones penales.

La aplicación de estos principios se define con mayor precisión en el artículo 5 y en los apartados 2 a 5 del artículo 6 de la Directiva 97/66/CE. El artículo 5 garantiza la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. Los Estados miembros deben prohibir la escucha grabación, almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, solo cuando esté autorizado legalmente, de conformidad con el apartado 1 del artículo 14.

Como norma general, los datos sobre tráfico deben destruirse o hacerse anónimos en cuanto termine la comunicación (apartado 1 del artículo 6 de la Directiva 97/66/CE).

Esto se debe a la confidencialidad de los datos sobre tráfico que permiten obtener perfiles individuales de comunicación incluyendo fuentes de información y ubicación geográfica del usuario de teléfonos fijos o móviles y los posibles efectos perniciosos sobre la intimidad resultantes de la recopilación, difusión o uso posterior de dichos datos. En el apartado 2 del artículo 6 se incluye un excepción relativa al tratamiento de datos sobre tráfico los efectos de la facturación de los usuarios y de los pagos de las interconexiones, pero únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

El apartado 1 del artículo 14 permite los Est dos miembros limitar el alcance de las obligaciones y derechos que se establecen en el artículo 6 cuando dichas limitaciones constituyen una medida necesaria para la salvaguardia de la seguridad nacional y la prevención, investigación, detección y represión de infracciones penales tal como se indica en el apartado 1 del artículo 13 de l Directiva 95/46/CE.

De estas disposiciones se deduce que los operadores de telecomunicaciones y los proveedores de servicio Internet no pueden recopilar y almacenar datos únicamente para controlar el cumplimiento de la legislación, menos que sí se les exige legalmente de conformidad con los motivos y condiciones antes mencionados. Esto coincide con los hábitos tradicionales de la mayoría de los Estados miembros, donde la aplicación de los principios nacionales de protección de datos ha dado lugar a la prohibición al sector privado de conservar datos personales con el único motivo de una posible necesidad posterior expresada por la policía o las fuerzas de seguridad del Estado.

En este contexto, es de observar que efectos de control y en las condiciones incluidas en el artículo 13 de l Directiva 95/46/CE y el artículo 14 de la Directiva 97/66/CE, la mayoría de los Estados miembros tienen disposiciones legislativas que definen las condiciones precisas en las cuales la policía y las fuerzas de seguridad del Estado pueden tener acceso a datos almacenados por operadores privados de telecomunicaciones y proveedores de servicio Internet para sus propios fines civiles.

Como ya indicó el Grupo en su Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones adoptada el 3 de mayo de 1999, el que un tercero llegue a poseer datos sobre tráfico relativos al uso de los servicios de telecomunicación se ha considerado generalmente interceptación de las telecomunicaciones, por lo que constituye una violación del derecho a la intimidad de las personas y la confidencialidad de las comunicaciones tal como está garantizado en el artículo 5 de la Directiva 97/66/CE. Además, la difusión de estos datos sobre tráfico es incompatible con el artículo 6 de la citada Directiva.

Toda violación de estos derechos y obligaciones es inaceptable al menos que cumpla tres criterios fundamentales, de conformidad con el apartado 2 del artículo 8 del Convenio europeo para la protección de los Derechos Humanos y las Libertades Fundamentales de 4 de noviembre de 1950, y se ajuste a la interpretación del Tribunal europeo de Derechos Humanos de tal disposición: un fundamento jurídico, la necesidad de dicha medida en un sociedad democrática y la conformidad con uno de los objetivos legítimos enumerados en el Convenio. El fundamento jurídico debe definir con precisión los límites y medios de aplicación de la medida : los fines para los que se podrán tratar los datos, el plazo durante el cual se podrán conservar (en caso de que se puedan conservar) y el acceso a los mismos deberán estar estrictamente limitados. Es imprescindible prohibir la vigilancia exploratoria o general a gran escala. De ello se deduce que los poderes públicos podrán tener acceso a datos sobre tráfico únicamente de manera individualizada y nunca sistemática ni general.

Estos criterios coinciden con las disposiciones antes citadas del artículo 13 de la Directiva 95/46/CE y del artículo 14 de l Directiva 97/66/CE.

Divergencia entre las normas nacionales

En relación con el periodo durante el cual se pueden conservar los datos sobre tráfico, la Directiva 97/66/CE solamente permite su tratamiento a efectos de facturación y únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura . No obstante, este plazo varía significativamente de un Estado miembro a otro. Por ejemplo, en Alemania los operadores de telecomunicaciones y los proveedores de servicios de telecomunicación pueden almacenar los datos necesarios para facturación durante un plazo máximo de 80 días a efectos de demostrar la corrección de la factura. En Francia , depende del tipo de operador: el operador de telecomunicaciones "tradicional" puede conservar los datos sobre tráfico hasta un año basándose en la ley que fija el plazo durante el cual puede impugnarse la factura . Este plazo queda fijado en 10 años para los demás operadores. En Austria , la ley sobre tele - comunicaciones no fija ningún plazo concreto para guardar los datos sobre tráfico a efectos de facturación, sino que lo limita al plazo durante el cual puede impugnarse la factura o exigirse el pago. En el Reino Unido, de conformidad con la ley, la factura puede impugnarse durante seis años, pero los operadores y proveedores de servicio almacenan los datos pertinentes durante unos 18 meses. En Bélgica, por ejemplo, la ley no define el plazo, pero el mayor proveedor de servicios de telecomunicación lo establece en 3 meses en sus condiciones generales. Otra práctica distinta puede observarse en Portugal pues, dado que el plazo no está fijado por ley, la autoridad nacional de control de la protección de datos decide de manera individualizada. Es interesante destacar que en Noruega el plazo está fijado en 14 días.

Tampoco es homogénea la práctica habitual de los proveedores de servicio Internet: parece que los pequeños proveedores conservan los datos sobre tráfico durante periodos muy breves (unas horas) debido a falta de capacidad de almacenamiento.

Los proveedores más importantes, que pueden permitirse disponer de capacidad de almacenamiento, pueden conservar los datos sobre tráfico durante unos meses (pero todo depende de su política de facturación: por tiempo de conexión o por periodos fijos).

A efectos de aplicación de la legislación, la ley sobre telecomunicaciones holandesa obliga a los operadores de tele - comunicaciones y los proveedores de servicio a recopilar y almacenar los datos sobre tráfico durante tres meses.

Obstáculos para el funcionamiento del mercado interior.

Estas divergencias podrían plantear obstáculos en el mercado interior para la prestación transfronteriza de servicios de telecomunicación e Internet, y la existencia de plazos tan diferentes puede dificultar el control del cumplimiento legisla - tivo. Se puede dar el caso de que un proveedor de servicio Internet establecido en un Estado miembro no tenga dere - cho a almacenar datos sobre tráfico durante más tiempo del permitido en el Estado miembro donde el cliente utiliza sus servicios, o bien que sea obligado a conservar los datos sobre tráfico durante más tiempo del permitido en su propio Estado miembro porque el país de los usuarios así lo exija legalmente. En caso de la facturación en telefonía móvil, quien cobra la factura es el operador nacional del abonado que usa este servicio en lugar del operador extranjero, por lo que los diversos plazos de almacenamiento de datos necesarios para la facturación pueden dar lugar a los mismos problemas que en el caso de los proveedores de servicio Internet. La norma de legislación aplicable definida en el artículo 4 de la Directiva 95/46/CE únicamente resuelve este problema si el proveedor de servicios Internet es el responsable y está establecido en un solo Estado miembro, pero no cuando está establecido en varios Estados miem - bros con distintos plazos o cuando tratan datos sobre tráfico en nombre del responsable.

Recomendación

En visto de lo anterior, el Grupo considera que los medios más eficaces para evitar riesgos inaceptables a la intimidad y reconocer simultáneamente la necesidad de una ejecución eficaz de la ley es que, en principio, los datos sobre tráfico no deberán conservarse a efectos exclusivos de control y que las legislaciones nacionales no deberán obligar a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicios Internet a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación.

El Grupo recomienda que la Comisión Europea proponga medidas apropiadas para una mayor armonización del plazo durante el cual se permite a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicio Internet a conservar los datos sobre tráfico para facturación y pago de interconexiones.

El Grupo considera que este plazo deberá ser suficiente para permitir a los consumidores impugnar la factura , pero lo más breve posible para no sobrecargar a los operadores y proveedores de servicios y para respetar los principios de proporcionalidad y especificidad como componentes del derecho a la intimidad.

Este plazo debe ser conforme con los mayores niveles de protección observados en los Estados miembros. El Grupo llama la atención sobre el hecho de que en varios Estados miembros se han aplicado satisfactoriamente plazos no superiores a tres meses.

Por último, el Grupo recomienda que los gobiernos nacionales tengan en cuenta estas consideraciones.

Hecho en Bruselas 7 de septiembre de 1999

Por el Grupo de Trabajo

El Presidente

Peter HUSTINX

DICTAMEN 4/99: INCLUSION DEL DERECHO FUNDAMENTAL A LA PROTECCION DE DATOS EN EL CATALOGO EUROPEO DE DERECHOS FUNDAMENTALES
5143/99/FR/final.
JT 26
Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos persona - les
Dictamen 4/99
Inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales
Aprobado el 7 de septiembre de 1999. pb 5140

EL GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES establecido por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 1 , vistos el artículo 29 y el apartado 3 del artículo 30 de dicha Directiva, vistos su reglamento interno y, en particular, sus artículos 12 y 14, HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

Con ocasión de su reunión del 4 de junio en Colonia, el Consejo Europeo decidió la elaboración de una carta de derechos fundamentales de la Unión Europea. En su decisión, el Consejo declara lo siguiente: "La evolución actual de la Unión exige la redacción de una Carta de derechos fundamentales que permita poner de manifiesto ante los ciuda - danos de la Unión la importancia sobresaliente de los derechos fundamentales y su alcance".

El grupo, que reúne a las autoridades encargadas de la protección de datos en los Estados miembros de la Unión Europea, aprueba plenamente la iniciativa del Consejo Europeo sobre la realización de una carta comunitaria de derechos fundamentales. Observa que algunos países europeos han integrado un derecho fundamental a la protección de datos en su constitución. En otros países la protección de datos ha adquirido estatuto de derecho fundamental a través de la jurisprudencia.

En sus decisiones y sentencias, la Comisión Europea y el Tribunal Europeo de Derechos Humanos han elaborado y definido un derecho fundamental basándose en distintos derechos humanos vinculados a la protección de datos de carácter personal.

Por último, un nuevo artículo (286) del Tratado de la Unión Europea dispone que los actos comunitarios relativos a la protección de las personas físicas en lo que concierne al tratamiento de los datos personales son aplicables, a partir del 1 de enero de 1999, a las instituciones y órganos de la Unión Europea.

La integración de la protección de datos de carácter personal entre los derechos fundamentales europeos haría apli - cable esta protección en el conjunto de la Unión y pondría de relieve la importancia creciente de la protección de estos datos en la sociedad de la información.

El grupo recomienda por tanto a la Comisión Europea, al Parlamento Europeo y al Consejo de la Unión Europea incluir el derecho fundamental a la protección de los datos de carácter personal en la carta de derechos fundamentales. El grupo está dispuesto a cooperar en la elaboración de dicha carta.

1 DO nº L 281 de 23/11/1995, p. 31..pb 5140

Hecho en Bruselas

el 7 de septiembre de 1999

Por el grupo

El Presidente

PETER J. HUSTINX

DICTAMEN 7/99 RELATIVO AL NIVEL DE PROTECCION DE DATOS PREVISTO POR LOS PRINCIPIOS DE "PUERTO SEGURO" HECHOS PUBLICOS, JUNTO CON LAS PREGUNTAS MAS FRECUENTES Y OTROS DOCUMENTOS RELACIONADOS, EL 15 Y 16 DE NOVIEMBRE DE 1999 POR EL DEPARTAMENTO DE COMERCIO DE LOS EE.UU.
5146/99/ES/final
WP 27
Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Dictamen 7/99, relativo a el nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE.UU.
Aprobado el 3 de diciembre de 1999.
El Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Visto el artículo 29 y la letra b) del artículo 30 de la Directiva,

Vistas sus normas de procedimiento y, en particular, sus artículos 12 y 14,

Ha aprobado el presente Dictamen 7/99:

Introducción

El Grupo de trabajo reafirma su política general sobre la metodología para evaluar la adecuación de la protección de datos en terceros países, resumida en su Documento de trabajo de 24 de julio de 1998 (WP 12: «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE»).

El Grupo de trabajo ha seguido de cerca las conversaciones entre la Comisión y el

Departamento de Comercio de los EE.UU., les otorga importancia y considera útil el enfoque de «puerto seguro». Desea contribuir al éxito de los resultados de estas conversaciones y cree que éste dependerá de que se responda a ciertas preocupaciones básicas.

En este contexto, el Grupo de trabajo recuerda que las versiones anteriores de los principios de «puerto seguro» y de las preguntas más frecuentes (FAQ) han sido objeto de los siguientes documentos:

1. Dictamen 1/99 de 26 de enero de 1999 (WP 15)

2. Dictamen 2/99 de 19 de abril de 1999 (WP 19)

3. Dictamen 4/99 de 7 de junio de 1999 (WP 21) y Documento de trabajo de 7 de septiembre de 1999 relativo a algunas de las FAQ (no hecho público)

4. Documento de trabajo de 7 de julio de 1999 (WP 23)

El presente Dictamen hace referencia a la versión más reciente de los principios de «puerto seguro», las FAQ y los documentos relacionados hechos públicos el 15 y el 16 de noviembre de 1999. El Grupo de trabajo lamenta que, en un asunto de tanta importancia, se le concediera tan poco tiempo para adoptar su posición. Asimismo, observa que ninguno de los documentos se considera «final» y, por lo tanto, se reserva la posibilidad de cambiar de posición en relación con cualquier modificación posterior de los textos.

El Grupo de trabajo observa que se han logrado algunos avances, pero deplora que, en la última versión de la documentación de EE.UU., únicamente se haya incluido una mínima parte de los comentarios que presentó en documentos anteriores. Por consiguiente, el Grupo de trabajo se reafirma en sus motivos generales de preocupación.

En lo tocante a una posible decisión de adecuación, y teniendo presentes los efectos concretos que tal decisión positiva tendría como punto de referencia para terceros países, el Grupo de trabajo considera que la seguridad jurídica de los principios de «puerto seguro» no debería limitarse a las entidades de los EE.UU., sino que debería abarcar también a las partes interesadas de la UE (responsables de ficheros que deseen transmitir datos a los EE.UU., afectados, autoridades de protección de datos). Desde su Dictamen 1/99, el Grupo de trabajo ha defendido constantemente el punto de vista de que, en lo relativo al fondo, «cualquier conjunto aceptable de principios de "puerto seguro" debe, como requisito mínimo, incluir todos los principios establecidos en las directrices sobre protección de la vida privada (Privacy guidelines) de la OCDE, adoptadas entre otros países por Estados Unidos, y que se volvieron a ratificar recientemente en la conferencia de Ottawa de la OCDE» celebrada en octubre de 1998.

Alcance y estructura

El Grupo de trabajo es de la opinión de que los principios de «puerto seguro» están diseñados para controlar el tratamiento de los datos transmitidos a los EE.UU. por responsables de ficheros de la UE. En relación con la recogida de datos personales de los particulares en la UE, el Grupo de trabajo recuerda que normalmente serán de aplicación las disposiciones legislativas nacionales por las que se transpone la Directiva. El Grupo de trabajo recuerda también que el nivel de adecuación establecido en virtud del apartado 6 del artículo 25 de la Directiva únicamente puede hacer referencia a la protección de las personas en relación con el tratamiento de los datos en el tercer país pertinente y no puede afectar al régimen jurídico establecido en la letra c) del artículo 4 de la Directiva.

En lo que respecta al «puerto seguro», el Grupo de trabajo recomienda definir de manera clara y sin ambigüedad su alcance tanto para los beneficiarios como para las categorías de transferencias de datos.

Según el cuarto párrafo de los Principios, los beneficios del «puerto seguro» surten efecto desde la fecha en que la entidad que desee acogerse a ellos notifique mediante autocertificación al Departamento Federal de Comercio o a su mandatario su adhesión a los principios. De acuerdo con la FAQ 6, estas cartas de autocertificación se deben enviar como mínimo una vez al año; el Departamento de Comercio (o su representante) «llevará una lista de las entidades que remitan cartas de autocertificación, dispensándoles los beneficios de "puerto seguro". Asimismo, actualizará la lista con las cartas anuales» y las notificaciones relativas a las decisiones de incumplimiento. De conformidad con la FAQ 11, se indicarán en la lista las decisiones negativas contra participantes en el «puerto seguro». A este respecto, el Grupo de trabajo observa lo siguiente:

1. El Departamento de Comercio no efectúa verificaciones previas para determinar si una entidad concreta cumple los criterios de adecuación (adhesión de su política de protección de la vida privada a los principios, jurisdicción de un órgano similar a la FTC para prácticas fraudulentas).

2. El requisito de la autocertificación anual está pensado para mejorar la fiabilidad de la lista; sin embargo, dado que la renovación de dicha autocertificación no es obligatoria, una entidad podría adherirse a los principios durante un año y, a continuación, retirarse del «puerto seguro». Además, existe la posibilidad de que haya impostores no detectados que tarden un periodo significativo en desaparecer de la lista, periodo durante el cual los datos personales continuarían transfiriéndose con normalidad.

3. Las fusiones y absorciones son cada vez más frecuentes en el mundo empresarial en general y, en especial, en los negocios en línea. Es perfectamente posible que una entidad adherida a los principios se fusione o sea absorbida por otra entidad que no pueda o no desee adherirse al «puerto seguro».

En su definición actual, los principios de «puerto seguro» son un sistema voluntario ofrecido a las entidades de EE.UU., basado en la autocertificación (FAQ 6) y la autoevaluación (FAQ 7), respaldado por disposiciones legales en caso de prácticas desleales o fraudulentas. Esto significa que, a menos que se presente e investigue una queja, y hasta el momento en que esto suceda, cualquier entidad de EE.UU. que afirme respetar los beneficios de «puerto seguro» tendría derecho a recibir datos personales de la UE. Teniendo en cuenta los ejemplos anteriores, el Grupo de trabajo insta a la Comisión a analizar métodos para garantizar la protección continua de los datos personales que puedan transmitirse a los siguientes tipos de entidades:

1. Entidades que nunca tendrían que haber aparecido en la lista porque no cumplen los criterios de aceptabilidad.

2. Entidades que, aunque aparecen en la lista, no cumplen los principios.

3. Entidades que, después de estar en la lista durante un año, dejan de estarlo el siguiente, porque no renuevan su autocertificación o porque dejan de ser aceptables en el «puerto seguro».

4. Entidades que, después de aparecer en la lista, son absorbidas por una empresa que no cumple los requisitos de «puerto seguro» (porque no puede o porque no desea adherirse a los principios).

Entre los posibles métodos para garantizar la protección continua, el Grupo de trabajo invita a la Comisión a considerar la eliminación o supresión de los datos transmitidos a una entidad perteneciente a alguna de las categorías anteriores. Además, el Grupo de trabajo desearía recibir aclaraciones en cuanto a la posibilidad de que sigan siendo aplicables las disposiciones sobre prácticas fraudulentas de la Federal Trade Commission Act (Ley de la Comisión Federal de Comercio).

Por motivos de seguridad jurídica, el Grupo de trabajo reitera su preocupación por que la lista de beneficiarios sea completamente fiable, actualizada y de fácil acceso público.

En su Documento de trabajo de 7 de julio de 1999, el Grupo de trabajo ya solicitó aclaraciones sobre dos puntos específicos:

a) Sectores que quedarían excluidos del alcance del «puerto seguro» porque no están dentro de la jurisdicción de un órgano público similar a la FTC (p. ej.: datos de empleados o actividades de carácter no lucrativo).

b) Actividades que puedan quedar excluidas por la propia entidad adherida al «puerto seguro» gracias a la posibilidad de elección por parte de la empresa.

En relación con el punto **a**), el Grupo de trabajo concede la máxima importancia a las cartas del Presidente de la FTC, de 23 de septiembre de 1998 y 1 de noviembre de 1999. Estas cartas indican claramente que la jurisdicción de la FTC abarca actos desleales o fraudulentos únicamente si "afectan al comercio o a actividades comerciales". Aparentemente, esto excluye la mayor parte de los datos tratados en relación con una relación laboral (FAQ 9), así como los datos tratados sin propósito comercial (p. ej.: actividades de carácter no lucrativo, investigación). Por tanto, el Grupo de trabajo recomienda que las transmisiones de datos pertenecientes a estas categorías se excluyan expresamente del «puerto seguro».

En cuanto al punto **b**), el Grupo de trabajo observa que la FAQ 6 invita a las entidades a indicar las «actividades de la

entidad cubiertas por su compromiso con los principios de "puerto seguro"». Esto implica que una misma entidad podría tener un pie en el «puerto seguro» y dejar el otro fuera de estos principios. El Grupo de trabajo es de la opinión de que esto crea incertidumbre jurídica (en especial en relación con el uso compartido de los datos dentro de una misma entidad) y solicita que se especifique con urgencia la noción de «actividades».

Excepciones y exenciones

El Grupo de trabajo reitera su preocupación por el hecho de que la adhesión a los principios pueda estar limitada por cualquier «disposición legal o reglamentaria, o jurisprudencia» [letra b) del párrafo 5 de los principios] sin más calificación. Esto se aplica, aparentemente, a las leyes estatales así como a las federales, tanto existentes.

6 como futuras. Para garantizar la seguridad jurídica y la no discriminación en relación con otros niveles adecuación, el Grupo de trabajo recomienda facilitar criterios más precisos y ejemplos concretos para dichas excepciones y limitaciones, así como considerar con la adecuada importancia sus efectos. En cuanto a la necesidad de criterios más precisos, el Grupo de trabajo recomienda distinguir claramente entre opciones y obligaciones: la adhesión a los principios solamente debería limitarse en la medida necesaria para cumplir obligaciones legales o reglamentarias (que, en cualquier caso, prevalecen sobre los principios) pero no como resultado de opciones derivadas de la legislación de EE.UU., dado que esto provocaría un grave menoscabo de los principios.

Por motivos de transparencia y seguridad jurídica, el Grupo de trabajo considera esencial que la Comisión permanezca informada de toda normativa legal o administrativa que pueda influir negativamente en la adhesión a los principios.

En relación con la letra c) del párrafo 5, el Grupo de trabajo recomienda limitar dicho párrafo a las excepciones previstas en la Directiva, que incluyen todas las dispensas permisibles en las normas de Derecho interno de los Estados miembros. En cualquier caso, el Grupo de trabajo es de la opinión de que no se puede invocar ninguna excepción fuera de su contexto específico y que toda excepción se podrá utilizar exclusivamente para servir a su propósito específico.

Para el Grupo de trabajo constituye motivo de preocupación el hecho de que, además de las excepciones antes citadas, las FAQ incluyen una larga lista de excepciones adicionales que, en algunos casos, resultan en la exención de categorías de datos completas; esta afirmación se aplica en concreto a la extensa categoría de «datos de dominio público», que pueden ser «de dominio público» de por sí el independientemente de posibles consideraciones de legitimidad de su tratamiento o de su precisión. El Grupo de trabajo observa que las Directrices de la OCDE no incluyen ninguna exención de este tipo y cree que la aceptación de dicha exención crearía un enorme vacío en la cobertura de la protección de datos.

Notificación
El Grupo de trabajo defiende su punto de vista, reiterado en todos sus Dictámenes anteriores, de que el acuerdo de «puerto seguro» (y especialmente cualquier decisión de adecuación) solamente concierne al tratamiento de datos transmitidos a terceros países por responsables de ficheros establecidos en la UE: los responsables de ficheros establecidos en la UE están sujetos a las disposiciones nacionales de transposición de la Directiva, y esto mismo se aplicaría en circunstancias normales en la recogida de datos personales directamente de los particulares en la UE por una entidad de EE.UU. que recurra a medios, automatizados o no, situados en el territorio de un Estado miembro (artículo 4 de la Directiva).

En la actualidad, todo ello queda aceptado por parte de EE.UU. en la pregunta número 1 de la FAQ 14, relativa a productos médicos y farmacéuticos, y en la FAQ 9 relativa a datos sobre recursos humanos. No obstante, el principio de Notificación afirma lo siguiente:

«La notificación se hará (...) la primera vez que se invite a los particulares a proporcionar a la entidad información personal o tan pronto como sea posible».

La cita anterior implica, o podría malinterpretarse en este sentido, que la recogida de datos de particulares en la UE por una entidad de EE.UU. está regida por los principios de «puerto seguro» y no por las disposiciones nacionales por las que se transpone la Directiva. Así, sus consecuencias irían mucho más allá que el principio de Notificación.

El Grupo de trabajo es de la opinión de que esto no cumple lo dispuesto en la

Directiva (artículo 4) y recomienda que la frase citada más arriba sea eliminada y se sustituya por la afirmación clara de los siguientes puntos:

1. Cuando una entidad de EE.UU. tenga la intención de recoger datos personales directamente de particulares de la UE, debe cumplir las disposiciones nacionales de transposición de la Directiva (por ejemplo, los artículos 6, 7, 10, 14 y, cuando sea pertinente, el artículo 8).

2. Cuando el responsable de un fichero establecido en la UE transmita datos personales a la entidad de EE.UU., ésta deberá pedirle que indique los fines para los que se recogieron inicialmente dichos datos (esto es básico para decidir si se ha producido un cambio de los fines después de la transmisión, lo que desencadenaría la aplicación de los principios de Notificación y Opción, y contribuiría a asignar el riesgo y la responsabilidad).

El Grupo de trabajo sugiere que los puntos anteriores sean objeto de una nueva FAQ destinada a esclarecer el principio de Notificación.

Asimismo, el Grupo de trabajo recomienda modificar el principio de Notificación para garantizar que se informe cuando otra entidad haga uso de los datos.

En lo que respecta a la FAQ 4, el Grupo de trabajo observa que no está justificado que los cazatalentos procesen los datos sin el consentimiento de los particulares. Además, se hace referencia a «otras circunstancias en que la aplicación de estos principios perjudicaría los intereses legítimos de la entidad» que el Grupo de trabajo considera una excepción demasiado ambigua.

El Grupo de trabajo hace notar que ha recibido el texto de la FAQ 14 sobre productos médicos y farmacéuticos hace muy poco tiempo y que éste plantea diversas dudas, sobre todo el uso de los datos para fines incompatibles con los relativos a la investigación científica.

Opción

El Grupo de trabajo reitera la opinión expresada en el Documento de trabajo de 7 de julio de 1999: dado que los principios no regulan la legitimidad de los criterios de tratamiento, es necesario reforzar el principio de Opción. En su versión actual, la combinación de los principios de Notificación y Opción permite utilizar los datos para fines distintos de los notificados sin necesidad de ofrecer la posibilidad de opción (a menos que dichos fines sean incompatibles o que los datos sean delicados), lo que incumple las Directrices de la OCDE («Principio de limitación del uso»). El Grupo de trabajo apoya la idea de que se debe ofrecer la posibilidad de Opción cuando se utilicen los datos para un fin compatible pero distinto.

El Grupo de trabajo comparte los puntos de vista de la Comisión expresados en la nota a pie de página referida al principio de Opción. Recomienda que la definición de datos delicados se haga coincidir con la Directiva (artículo 8) y considera que la opción únicamente puede ser la base de un tratamiento legítimo si se ha proporcionado la información adecuada.

Transferencia ulterior

El Grupo de trabajo observa con cierta preocupación la adición a este principio de la última frase, que exime totalmente de responsabilidad a las entidades cuando transmitan la información a determinados terceros. Los particulares pueden verse desprotegidos de recursos jurídicos excepto contra la entidad transmisora de los datos, que podría haber actuado de manera imprudente al transmitir la información. El Grupo de trabajo recomienda considerar la posibilidad de reducir la exención de responsabilidad con objeto de mantener la responsabilidad de la entidad transmisora en casos de negligencia e imprudencia y exigir a dicha entidad transmisora que asista al particular en la satisfacción de sus derechos.

Seguridad

El Grupo de trabajo recomienda modificar la FAQ 10 para eliminar la frase relativa a que es innecesaria la presencia en el contrato de cláusulas sobre seguridad, dado que la legislación de diversos Estados miembros exige estas cláusulas en los contratos para el tratamiento dentro del mismo Estado miembro.

Integridad de los datos

El Grupo de trabajo recuerda que, en virtud del párrafo 8 de las Directrices de la OCDE, «los datos deberán ser pertinentes para los fines a los que se destinan y, en la medida necesaria para dichos fines, deberán ser precisos, completos y actualizados».

Este principio de «puerto seguro» debería reflejar tal afirmación.

Acceso

El Grupo de trabajo recuerda que el Acceso es un principio fundamental para todo régimen de protección de datos que se precie, puesto que el Acceso es la raíz de la que se derivan todos los derechos del sujeto de los datos, y hace énfasis en que las excepciones a este principio fundamental solamente se permitan en circunstancias excepcionales, al tiempo que reitera la preocupación expresada en todos sus documentos anteriores sobre la amplitud y la ambigüedad de las excepciones y condiciones expresadas por los EE.UU. para el ejercicio de este derecho fundamental.

El Grupo de trabajo vuelve a expresar su opinión de que las consideraciones de coste son pertinentes para decidir las condiciones en que se puede ejercer este derecho, pero no pueden condicionar el propio derecho.

A diferencia de las Directrices de la OCDE , los principios de «puerto seguro» no reconocen el derecho del particular a recibir información «de forma fácilmente inteligible». Además, el principio de Acceso limita el derecho de suprimir a los casos en que los datos sean inexactos (lo que es obvio). En su Dictamen 2/99, el Grupo de trabajo ya ha expresado el punto de vista de que, para que tenga sentido, el derecho de suprimir deberá aplicarse a todos los casos de tratamiento ilícito y que debería incluirse en los principios y no en las FAQ.

La FAQ 8 enumera una larga lista de excepciones al principio de Acceso. El Grupo de trabajo se alegra de que algunas de ellas, en comparación con la versión anterior de la FAQ, se hayan especificado o reducido. Sin embargo, la impre-

sión general es que esta FAQ debilita el principio en lugar de ofrecer orientaciones para su aplicación. En particular, el Grupo de trabajo reitera sus objeciones a la pregunta 2 (noción poco clara) y a la pregunta 7. En cuanto a la pregunta 5, el Grupo de trabajo reafirma su opinión de que las circunstancias para denegar el acceso son demasiado amplias y ambiguas, y que el texto implica que tales consideraciones prevalecen automáticamente sobre el derecho de acceso. Le preocupa que esto dé como resultado un grave debilitamiento del nivel general de protección de los datos.

En lo que respecta a la pregunta 6, el Grupo de trabajo considera inadecuada la redacción del segundo párrafo y recomienda que se elimine o bien que se defina con mayor precisión para limitarlo a eliminar los abusos del derecho de acceso.

El Grupo de trabajo reitera asimismo su oposición a la pregunta 8, por los motivos ya expuestos en el Documento de trabajo de 7 de septiembre de 1999; además, el hecho de que la información sea de dominio público no priva al sujeto de los datos de su derecho de acceso.

Aplicación

El Grupo de trabajo agradece la información detallada de los EE.UU. durante las últimas semanas de conversaciones (en especial: carta de la FTC, comparación de los mecanismos de resolución de litigios sobre protección de la intimidad del sector privado de EE.UU., FAQ 11, Memorándum sobre la Fair Credit Reporting Act). Esta información es valiosa y ha permitido al Grupo de trabajo hacerse una idea más global de los instrumentos de aplicación que podrían ponerse a disposición de los sujetos de los datos. Una vez analizada la citada información, el Grupo de trabajo plantea los siguientes motivos de preocupación:

1. Los mecanismos del sector privado existentes abordan exclusivamente las actividades en línea: BBB Online, Web Trust, TRUSTe (el subrayado es nuestro).

2. Se puede ver un énfasis similar en la carta del Presidente de la FTC de 1 de noviembre de 1999 (párrafo 2: «secreto en línea», «entorno Internet»; párrafo 3: mercado en línea, estudio de sitios web; párrafo 4: «políticas de protección de la intimidad en línea», etc.; el subrayado es nuestro).

3. Según el párrafo 4 de los principios, también se podrán acoger a los beneficios de «puerto seguro» las entidades sujetas a «disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones de bolsas nacionales de valores, asociaciones registradas de agentes de valores, organismos de compensación autorizados o comités municipales de regulación de bolsas de valores) que protejan con eficacia el secreto de los datos personales». No obstante, no se ha facilitado información sobre los organismos públicos que garantizarían la aplicación de esta enorme variedad de disposiciones legales.

En estas circunstancias, el Grupo de trabajo considera que el alcance de las decisiones de adecuación debería restringirse expresamente a los sectores para los que se haya recogido información suficiente y sin ambigüedades y ésta se haya analizado en relación con la existencia de mecanismos de aplicación. De hecho, ampliar el alcance más allá de este límite permitiría recurrir judicialmente la decisión, circunstancia no deseable para ninguna de las partes interesadas.

En relación con el principio de Aplicación, el Grupo de trabajo considera que debe incluir, para que resulte significativo, la indemnización por daños y perjuicios sufridos por los particulares como resultado de la vulneración de los principios: este es el punto de vista general del Grupo de trabajo y se aplica a cualquier tercer país (Documento de trabajo sobre transferencias de datos personales a terceros países; WP 12 de 24 de julio de 1998, página 14: «Reparación adecuada»). Cuando la legislación de los EE.UU. en vigor no establezca la reparación de los daños y perjuicios, la entidad privada debe estar preparada para ofrecer esta posibilidad como condición de adhesión al «puerto seguro».

En la FAQ 11 (resolución de litigios y ejecución), el Grupo de trabajo ha observado que el texto aborda una serie de aspectos relativos a la aplicación que son tan fundamentales que deberían incluirse en el propio principio de Aplicación. Para crear la relación entre los distintos niveles de aplicación, es especialmente importante establecer la norma de que los organismos de resolución de conflictos remitan los asuntos no resueltos a la FTC. También se podrían añadir al principio los requisitos de que los mecanismos de resolución de conflictos sean transparentes y ágiles.

Según la FAQ 11, los órganos de resolución de conflictos pueden introducir condiciones de admisibilidad de las quejas. El Grupo de trabajo considera que estas condiciones deberían ser explícitas, objetivas y razonables. Además, la negativa de aceptar a trámite las quejas debe estar debidamente motivada.

En general, el Grupo de trabajo observa que los acuerdos de aplicación en los EE.UU. tienen una estructura muy confusa, en la que no es posible identificar fácilmente los derechos que tienen los ciudadanos en caso de vulneración de los Principios. La FAQ 11 se limita a ofrecer una serie de recomendaciones que pueden dar lugar a una aplicación fragmentada e irregular.

FAQ 5: Función de las autoridades de protección de datos

El Grupo de trabajo ha debatido el texto de la FAQ 5 propuesto por los EE.UU. y su conclusión es que la función de las autoridades de protección de datos descrita en él no es factible práctica ni jurídicamente. En concreto, el Grupo de trabajo observa que la legislación nacional no proporciona a las autoridades nacionales las competencias necesarias para tratar las quejas por infracciones de las normas de protección de datos fuera de su jurisdicción.

Por otra parte, el Grupo de trabajo destaca que las autoridades nacionales están dispuestas a ofrecer su colaboración en forma de información y asesoramiento, si ello puede ser de utilidad en el marco del «puerto seguro». Entiende que los EE.UU. han intentado lograr esta colaboración durante un periodo limitado tras el lanzamiento del «puerto seguro».

En este contexto, el Grupo de trabajo invita a la Comisión a que investigue si esta oferta de información y asesoramiento, más el compromiso unilateral de la entidad de EE.UU. de que seguirá los consejos de las autoridades nacionales (compromiso que, en caso de incumplimiento, daría lugar a acciones de la FTC por fraude), podría ayudar a satisfacer los requisitos de la letra a) del principio de Aplicación del «puerto seguro». En caso afirmativo, observa que las autoridades nacionales podrían estar preparadas para colaborar en este sentido durante un periodo inicial de tres años.

Además, el Grupo de trabajo indica que las autoridades nacionales desearían revisar este compromiso antes del fin de dicho periodo si el número de entidades de EE.UU. que eligen esta opción es tal que se concluya sin duda que este método se emplea como sustituto de los acuerdos adecuados de aplicación en los EE.UU., y no como un medio provisional para cubrir un vacío limitado.

El Grupo de trabajo también invita a la Comisión a investigar la función que podría ejercer un mecanismo a escala europea que, entre otros aspectos, podría facilitar un foro que ayudara a garantizar un enfoque coordinado y armonizado.

Proyecto de Decisión de la Comisión (de 24 de noviembre de 1999)

El Grupo de trabajo desea llamar la atención de la Comisión sobre los siguientes puntos:

1. No hay ninguna referencia al trabajo llevado a cabo por el Grupo de trabajo a fin de establecer los criterios para evaluar la adecuación en terceros países (WP 12).

En opinión del Grupo de trabajo, la evaluación debería realizarse sobre estos criterios para garantizar un enfoque equilibrado y ecuánime en todos los países, independientemente de que sigan un enfoque legislativo o normativo para la protección de los datos. Además, debería incluir una referencia específica a los dictámenes emitidos por el Grupo de trabajo sobre el «puerto seguro» en los EE.UU., así como a sus lugares de publicación.

2. En cuanto al fondo de la Decisión, el Grupo de trabajo observa que los criterios de adhesión al «puerto seguro» no son los mismos en los textos de EE.UU. que en el proyecto de Decisión. Según los párrafos iniciales 3 y 4 de los Principios publicados por los EE.UU., las entidades pueden adherirse al «puerto seguro» por los siguientes métodos:

a) integrándose en un programa de protección de la vida privada elaborado por el sector privado que siga los principios,
b) elaborando sus propias medidas de protección de la vida privada, siempre que se adecuen a dichos principios,
c) estando sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra, que protejan con eficacia el secreto de los datos personales.»

En virtud del artículo 1 del proyecto de Decisión de la Comisión, se consideran pertenecientes al «puerto seguro» las entidades que:

«hayan manifestado de forma pública su compromiso de cumplir los Principios y queden bajo la jurisdicción de un organismo público independiente facultado para investigar las quejas y solicitar medidas provisionales contra las prácticas desleales o fraudulentas.»

Es necesario que los Principios se correspondan con la Decisión.

3. Asimismo, el Grupo de trabajo observa que el considerando 8 establece que la jurisdicción de la Federal Trade Commission está sujeta a diversas exclusiones legales. Sin embargo, no se indican expresamente los sectores excluidos ni tampoco se afirma que todos ellos estén cubiertos por otro organismo público.

Igualmente, debería incluirse una referencia a las disposiciones por las que se faculta al reducido número de organismos públicos mencionados para actuar contra las prácticas fraudulentas o desleales.

Dado que, para las entidades que deseen adherirse al «puerto seguro», es una condición sine qua non estar sujetas a la jurisdicción de un organismo público facultado para actuar contra las prácticas desleales o fraudulentas, el Grupo de trabajo considera fundamental esclarecer este punto y que el alcance del «puerto seguro» se limite a los sectores regidos por un organismo público de este tipo. El proyecto de Decisión de la Comisión no menciona la manera en que las entidades pueden verse privadas de los beneficios de «puerto seguro»; dicho de manera más sencilla, los procedimientos para su eliminación de la lista del Departamento de Comercio.

El único compromiso del texto de EE.UU. es indicar en la lista «toda notificación que reciba de los organismos de resolución de litigios, autorregulación y/o de la administración sobre cualquier incumplimiento sistemático de los principios o de las resoluciones de los organismos mencionados que haya sido cometido por entidades del puerto seguro. No obstante, se concederá un plazo de 30 días para notificar este extremo a dichas entidades así como la oportunidad de alegar».

(FAQ 11)

Según el proyecto de Decisión, esta indicación negativa por parte del Departamento de Comercio de los EE.UU. únicamente puede dar lugar a la suspensión de las transmisiones de datos en virtud de la letra a) del apartado 2 del artículo 2. En la actualidad, aunque se suspenda la transmisión de datos a una entidad en virtud de la letra a) del apartado 2 del artículo 2, esta suspensión no quedaría reflejada porque la lista de EE.UU. no mostrará las decisiones de adecuación negativas tomadas en la UE. Sin embargo, es necesario garantizar que los operadores de la UE pueden confiar en la lista.

Además, en opinión del Grupo de trabajo, las condiciones establecidas en el apartado 2 del artículo 2 para la suspensión de los flujos de datos podrían ser difíciles de cumplir en la práctica, lo que sería inaceptable cuando se están vulnerando los derechos de la persona. Para solucionar este aspecto, las palabras «perjuicio irreparable» del apartado 2 del artículo 2 deberían sustituirse por «perjuicio grave e inminente».

5. El Grupo de trabajo observa que el apartado 3 del artículo 1 incluye el siguiente texto propuesto por los Estados Unidos: «Se considerará que el cumplimiento de la Fair Credit Reporting Act o la Financial Modernization Act estadounidenses garantizan un nivel adecuado de protección, si las actividades de una entidad entran en el ámbito de aplicación de una de ambas leyes». En relación con estas leyes de EE.UU., el Grupo de trabajo llama la atención de la Comisión sobre el hecho de que en el orden del día de la 17º reunión del 7 de junio se incluyó un análisis de la Fair Credit Reporting Act , pero no hubo tiempo de analizar dicha ley ni de evaluar su nivel de adecuación. En lo que respecta a la Financial Modernization Act, el Grupo de trabajo recibió su texto en fechas demasiado recientes.

A la luz de lo anterior, el Grupo de trabajo solamente podrá emitir un dictamen sobre el nivel de adecuación de ambas leyes después de haberlas analizado detalladamente. Mientras no haya una decisión sobre la adecuación de estas leyes, deberá eliminarse de la Decisión toda referencia a las mismas.

6. El Grupo de trabajo también considera que en el apartado 1 del artículo 2 debe incluirse la siguiente modificación:

«El artículo 1 se entenderá sin perjuicio de las facultades de las autoridades competentes de los Estados miembros para emprender acciones destinadas a garantizar el cumplimiento de las disposiciones nacionales adoptadas en virtud de disposiciones distintas a los artículos 25 y 26 de la Directiva.»

Canje de notas

(sin fecha, pero incluidas en el sitio web el 15 de noviembre)

El Grupo de trabajo desea llamar la atención de la Comisión sobre los siguientes aspectos:

1. **El denominado periodo de gracia o fecha de entrada en vigor:** Tanto el proyecto de carta de los EE.UU. como el proyecto de respuesta de la Comisión incluyen fórmulas al efecto de que la Comisión y los Estados miembros utilizarán la flexibilidad del artículo 26 para evitar interrupciones en los flujos de datos hacia las entidades de los EE.UU. durante un periodo determinado de conformidad con la decisión del apartado 6 del artículo 25 sobre el marco del «puerto seguro». Esto proporcionará a las entidades de los EE.UU. la oportunidad de decidir si desean adherirse al «puerto seguro» y, en caso necesario, adaptar sus prácticas de información a los requisitos del «puerto seguro».

Teniendo en cuenta que, de conformidad con la Directiva, la Comisión solamente podrá actuar en relación con transferencias de datos a países terceros en los siguientes casos: a) un tercer país no garantiza un nivel de protección adecuado y la Comisión inicia negociaciones destinadas a remediar la situación (apartados 4, 5 y 6 del artículo 25), o b) cuando la Comisión decida que determinadas cláusulas contractuales tipo ofrecen garantías suficientes (apartado 4 del artículo 26), el Grupo de trabajo se pregunta en qué se piensa basar la Comisión para utilizar la flexibilidad del artículo 26 de la Directiva a fin de otorgar a las entidades de los EE.UU. tiempo suficiente para decidir si desean o no adherirse al «puerto seguro».

2. **Utilización de los contratos - Decisiones tomadas en virtud del artículo 2**6: En el proyecto de carta de los EE.UU. se afirma lo siguiente: «La Comisión y los Estados miembros consideran que los principios (de «puerto seguro» de los EE.UU.) pueden utilizarse en estos acuerdos para las disposiciones materiales sobre protección de datos... La Comisión ha iniciado conversaciones con los Estados miembros en el Comité del artículo 31... para adoptar una decisión en virtud del apartado 4 del artículo 26 que autorice, cuando proceda, los acuerdos tipo...»

Teniendo en cuenta que el Grupo de trabajo siempre ha sostenido que el análisis de la adecuación de las soluciones contractuales exige tomar en consideración un conjunto de cuestiones más amplio que el abordado en las soluciones marco, un compromiso de este tipo sería prematuro. No es preciso resaltar que en primer lugar se deben mejorar los principios de «puerto seguro» hasta que se consideren adecuados y solamente después podrá considerarse su inclusión en el contenido de los contratos tipo.

Conclusiones

En vista de las observaciones y recomendaciones anteriores, el Grupo de trabajo concluye que los acuerdos de «puerto seguro» propuestos, tal como quedan reflejados en las versiones actuales de los diversos documentos, continúan siendo insatisfactorios. El Grupo de trabajo invita a la Comisión a que inste a la parte estadounidense a realizar una serie de mejoras clave, en particular las siguientes:

- Especificar el alcance del «puerto seguro» y, en especial, eliminar todo posible malentendido referido a que las entidades de EE.UU. pueden optar por basarse en los principios de «puerto seguro» en circunstancias en las que es de aplicación la propia Directiva.

- Facilitar acuerdos más fiables que permitan identificar con seguridad a los participantes en el «puerto seguro» y evitar el riesgo de continuar otorgándoles los beneficios del «puerto seguro» cuando, por un motivo u otro, hayan sido eliminados de la lista.

- Afirmar sin ningún asomo de duda que todos los participantes en el «puerto seguro» están sujetos a la jurisdicción de un organismo público con las facultades apropiadas para controlar su aplicación.

- Establecer la norma de que los organismos de resolución de conflictos del sector privado deben remitir las quejas no resueltas a uno de estos organismos públicos.

- Eliminar las generalizaciones y ambigüedades de las excepciones y exenciones permitidas, de manera que las excepciones sean precisamente eso, es decir, que se apliquen solamente cuando sea necesario y en la medida requerida, y que no sean invitaciones generales para hacer caso omiso de los principios. Esto cobra especial importancia en relación con el derecho de acceso.

- Reforzar el principio de Opción, que es el elemento decisivo del enfoque de los EE.UU.

Estos puntos se han desarrollado con mayor detalle en las secciones anteriores del presente Dictamen y el Grupo de trabajo desearía que se tomaran en cuenta las consideraciones pertinentes.

Además, el Grupo de trabajo invita a la Comisión a revisar el artículo 2 del proyecto de Decisión para indicar claramente que ésta no afectará las facultades de aplicación de las autoridades nacionales competentes en lo que respecta a las disposiciones por las que se transpone la Directiva a las legislaciones nacionales, con excepción de sus artículos 25 y 26, así como para permitir la posibilidad de intervenir de conformidad con el apartado 2 del artículo 2 cuando puedan existir perjuicios «graves e inminentes» para los particulares en caso de no intervención.

Por último, el Grupo de trabajo destaca la importancia de continuar e incluso acelerar el trabajo sobre las cláusulas de los contratos tipo, con el objeto de tomar una o varias decisiones en virtud del apartado 4 del artículo 26, lo que constituye una parte importante de la simplificación y transparencia de las salvaguardias necesarias para la transmisión a zonas en las que no hay otros medios de garantizar la protección adecuada.

Hecho en Bruselas, a 3 de diciembre de 1999

Por el Grupo de trabajo

El Presidente

Peter J. HUSTINX

MEMORIA DE 1999 - ANEXO IX - ACTO Nº 1/99 DE LA AUTORIDAD COMÚN DE CONTROL DE EUROPOL de 22 de abril de 1999 por el que se establece su Reglamento interno

29/04/99
ACTO Nº 1/99 DE LA AUTORIDAD COMÚN DE CONTROL DE EUROPOL de 22 de abril de 1999 por el que se establece su Reglamento interno

LA AUTORIDAD COMÚN DE CONTROL

Visto el Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol) y, en particular, el apartado 7 de su artículo 24,

Considerando que corresponde a la Autoridad Común de Control establecer por unanimidad su propio Reglamento interno,

HA APROBADO EL SIGUIENTE REGLAMENTO INTERNO:

REGLAMENTO INTERNO

DE LA

AUTORIDAD COMÚN DE CONTROL

DE EUROPOL

TÍTULO I

FUNCIONES Y COMPETENCIAS DE LA AUTORIDAD COMÚN DE CONTROL

Artículo 1
Funciones

1. La Autoridad Común de Control tendrá por función vigilar, de acuerdo con el Convenio, la actividad de Europol a fin de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que disponga Europol no vulneran los derechos de las personas. La Autoridad Común de Control controlará además la licitud de la transmisión de los datos que procedan de Europol (primera y segunda frases del apartado 1 del artículo 24 del Convenio).

2. A tal efecto, la Autoridad Común de Control desempeñará las siguientes funciones:

a) examinará las disposiciones de creación de ficheros (segunda frase del apartado 1 y tercera frase del apartado 2 del artículo 12 del Convenio);

b) examinará las normas sobre el levantamiento de actas de consultas de datos personales (primera frase del artículo 16 del Convenio);

c) examinará las normas generales sobre la transmisión por Europol de datos personales a Estados y organismos terceros (segunda frase del apartado 2 del artículo 18 del Convenio);

d) examinará las cuestiones relativas:

- a la aplicación e interpretación del Convenio que pudiera plantear la actividad de Europol en relación con el tratamiento y la utilización de datos personales (apartado 3 del artículo 24, primera posibilidad, del Convenio),

- al control independiente efectuado por las autoridades nacionales de control de los Estados miembros (apartado 3 del artículo 24, segunda posibilidad, del Convenio),

- al ejercicio del derecho de información (apartado 3 del artículo 24, tercera posibilidad, del Convenio),

- a la elaboración de propuestas armonizadas con miras a hallar soluciones comunes a los problemas existentes (apartado 3 del artículo 24, cuarta posibilidad, del Convenio);

e) examinará, a petición de cualquier persona, si la recogida, el almacenamiento, el tratamiento y el uso de datos personales efectuados por Europol se han realizado de manera lícita y correcta (apartado 4 del artículo 24 del Convenio);

f) elaborará informes de actividad a intervalos regulares (apartado 6 del artículo 24 del Convenio).

Artículo 2
Competencias

1. Para el desempeño de sus funciones, la Autoridad Común de Control tendrá las competencias establecidas en el Convenio.

2. En particular, la Autoridad Común de Control estará autorizada a obtener información de Europol, se le dará acceso a todos los documentos y expedientes, así como a los datos almacenados por Europol, y se le concederá libre acceso en todo momento a todos los locales de Europol (apartado 2 del artículo 24 del Convenio). Esto incluye información sobre los equipos y programas informáticos y acceso a los mismos, siempre que resulte necesario para el cumplimiento de las funciones de la Autoridad Común de Control. Los detalles podrán definirse mediante acuerdos entre la Autoridad Común de Control y el Consejo de Administración de Europol.

Artículo 3
Comités

1. La Autoridad Común de Control creará el Comité a que se refiere el apartado 7 del artículo 24 del Convenio.

2. La Autoridad Común de Control podrá crear una o varias comisiones internas y determinar su composición y mandato (apartado 8 del artículo 24 del Convenio).

TÍTULO II

REGLAMENTO INTERNO DE LA AUTORIDAD COMÚN DE CONTROL

Artículo 4
Composición

1. La Autoridad Común de Control estará integrada como máximo por dos miembros o representantes de cada una de las autoridades nacionales de control, que constituirán una delegación. Cada miembro podrá tener un suplente. Los miembros de la Autoridad Común de Control y sus suplentes serán nombrados por cada Estado miembro por períodos de cinco años (tercera frase del apartado 1 del artículo 24 del Convenio), que podrán renovarse.

2. Los miembros de la Autoridad Común de Control y sus suplentes serán independientes, no estarán sujetos a instrucciones en el desempeño de sus funciones y sólo estarán sometidos a la ley. En particular, no serán al mismo tiempo miembros de otro órgano creado en virtud del Convenio, ni miembros del personal de Europol.

En caso de que surja un conflicto de intereses, la persona afectada declarará ese interés y se abstendrá de participar en la discusión y en la decisión correspondientes. Podrá, si fuese necesario, ser excluida por mayoría de los votos emitidos en votación secreta por las delegaciones que asistan a la reunión. La persona de que se trate será escuchada antes de la exclusión, pero no tomará parte en la decisión. Si la persona se retira o es excluida, podrá ser sustituida por su suplente.

3. Sólo podrá nombrarse miembros de la Autoridad Común de Control o suplentes de éstos a personas que posean las capacidades exigidas (tercera frase del apartado 1 del artículo 24 del Convenio). Se prestará especial atención a los requisitos necesarios con respecto al Comité de Recursos.

4. Cuando un miembro de la Autoridad Común de Control no pueda asistir a una reunión podrá ser representado por su suplente.

5. La pertenencia de una persona a la Autoridad Común de Control terminará con su dimisión o con su cese como miembro o representante de la autoridad nacional de control, a menos que el Estado miembro de que se trate le renueve el nombramiento. El nombramiento de un miembro únicamente podrá revocarse de conformidad con la legislación nacional. Esta disposición se aplicará también a los suplentes.

Artículo 5
Presidencia

1. La Autoridad Común de Control elegirá a un presidente y a un vicepresidente entre sus miembros por mayoría de dos tercios de los votos emitidos en votación secreta por las delegaciones que asistan a la reunión. El vicepresidente no podrá ser miembro de la delegación del presidente. Si ninguno de los candidatos logra la mayoría requerida en primera votación, se celebrará una segunda votación para elegir entre los dos candidatos que hayan obtenido mayor número de votos. El presidente y el vicepresidente serán elegidos por un mandato de dos años. Podrán ser reelegidos para un segundo mandato de un año.

2. El presidente representará a la Autoridad Común de Control y presidirá sus reuniones. Cuidará de su correcto funcionamiento. Convocará las reuniones de la Autoridad Común de Control y determinará el lugar, la fecha y la hora de las reuniones. Abrirá y clausurará las reuniones. Elaborará el orden del día provisional y velará por la ejecución de las decisiones tomadas por la Autoridad Común de Control.

3. El vicepresidente actuará como presidente si éste no puede asistir. En caso de ausencia del vicepresidente actuará como tal el miembro de mayor edad. Hasta la elección del presidente, el miembro de mayor edad convocará y presidirá

la primera reunión de la Autoridad Común de Control.

4. Con objeto de preparar su trabajo sobre un tema determinado, la Autoridad Común de Control podrá nombrar de entre sus miembros, a propuesta del presidente, uno o varios ponentes. Cuando se trate de un asunto urgente, dicho nombramiento podrá hacerlo el presidente en virtud de sus competencias. En tal caso informará inmediatamente de ello a los miembros de la Autoridad Común de Control.

5. El presidente o una mayoría de las delegaciones podrán solicitar la asistencia del director de Europol a las reuniones e invitar a miembros del personal de Europol, expertos nacionales, funcionarios de enlace y otras personas, a que asistan a las reuniones.

Artículo 6
Métodos de trabajo

1. La Autoridad Común de Control se reunirá al menos cuatro veces al año. Se reunirá además por iniciativa del presidente y siempre que tres delegaciones, como mínimo, presenten una propuesta escrita motivada o formulen una propuesta oral en una reunión anterior. El presidente del Consejo de Administración y el director de Europol podrán proponer la inclusión de puntos en el orden del día y la convocatoria de la Autoridad Común de Control.

2. Con excepción de aquellos casos que el presidente considere urgentes, la convocatoria se comunicará de forma que llegue al menos dos semanas antes de la reunión. La convocatoria incluirá el orden del día provisional y, a menos que la naturaleza de los documentos no lo permita, los documentos necesarios para la reunión. El orden del día definitivo se aprobará al comienzo de cada reunión.

3. Las reuniones de la Autoridad Común de Control sólo serán efectivas si asisten, como mínimo, dos tercios de las delegaciones. Las decisiones se adoptarán por mayoría simple de las delegaciones que asistan a la reunión, salvo disposición en contrario del presente Reglamento interno. Cada delegación tendrá derecho a un voto. En caso de empate, el presidente tendrá voto de calidad.

4. Las reuniones de la Autoridad Común de Control no serán públicas. Sus documentos serán confidenciales, a menos que la Autoridad Común de Control decida lo contrario. En cualquier caso, todos los documentos presentados por Europol estarán sujetos a las normas sobre protección del secreto a que se refiere el apartado 1 del artículo 31 del Convenio.

5. La Autoridad Común de Control celebrará sus reuniones basándose en documentos y proyectos redactados en todas las lenguas oficiales de las Instituciones de las Comunidades Europeas. Solamente en caso de urgencia podrán admitirse excepciones a esta disposición; sin embargo, las delegaciones tendrán derecho a pedir una traducción a su propia lengua.

6. Las decisiones de la Autoridad Común de Control podrán tomarse por procedimiento escrito siempre que las delegaciones hayan aprobado este procedimiento en una reunión. En casos urgentes, el presidente podrá iniciar el procedimiento escrito. En ambos casos el presidente transmitirá un proyecto de decisión a los miembros de la Autoridad Común de Control. Si las delegaciones no recusan el proyecto de decisión, traducido a las respectivas lenguas oficiales, dentro de un plazo especificado por el presidente de al menos catorce días a partir de la recepción, se considerará adoptada la propuesta. Si en un plazo de cinco días hábiles desde la recepción del proyecto de decisión una delegación solicita que la Autoridad Común de Control lo someta a debate oral, el procedimiento escrito se interrumpirá.

Artículo 7
Control de los locales y expertos

1. En el marco de sus competencias con arreglo al artículo 24 del Convenio, la Autoridad Común de Control podrá llevar a cabo controles sobre la protección de datos en Europol.

2. La Autoridad Común de Control podrá nombrar a uno o más miembros para que efectúen dichos controles. Cuando la Autoridad Común de Control lo estime necesario, dichos miembros podrán ser asistidos por expertos elegidos únicamente entre los que figuren en una lista de expertos que la Autoridad Común de Control habrá elaborado de antemano y comunicado a Europol. Los expertos de dicha lista procederán de las autoridades nacionales de control y de organismos gubernativos, a menos que no se pueda contar con tales expertos. Todos los expertos tendrán que reunir los requisitos de seguridad aplicables conforme a su legislación nacional.

3. Cuando el presidente considere que un asunto es urgente, podrá nombrar, en virtud de sus competencias, a dichos miembros y expertos. En este caso informará inmediatamente a los miembros de la Autoridad Común de Control.

4. Los miembros de la Autoridad Común de Control encargados de un control informarán a la Autoridad Común de Control de los resultados de su labor.

Artículo 8
Procedimiento en caso de infracción

Si la Autoridad Común de Control advierte que se han infringido las disposiciones del Convenio sobre el almacenamiento, el tratamiento o la utilización de datos personales, informará de ello al director de Europol y le solicitará por

escrito que responda en un plazo determinado. Si la Autoridad Común de Control considera que la respuesta es insuficiente o que no se ha recibido en el plazo oportuno, o si surge cualquier otra dificultad, someterá la cuestión por escrito al Consejo de Administración (tercera frase del apartado 5 del artículo 24 del Convenio). El incumplimiento de una decisión definitiva del Comité de Recursos se considerará como una violación del Convenio.

Artículo 9
Actas

Se levantará acta de todas las reuniones de la Autoridad Común de Control. La Secretaría, bajo la dirección del presidente, preparará los proyectos de acta, que se someterán a la Autoridad Común de Control para que los apruebe en su siguiente reunión. Cada miembro tendrá derecho a hacer que se modifique el proyecto de acta para que refleje los comentarios efectuados por dicho miembro en la reunión.

Artículo 10
Informe de actividad

1. La Autoridad Común de Control elaborará informes de actividad al menos una vez cada dos años. Al menos un mes antes de remitir al Consejo el informe de actividad, el Consejo de Administración podrá formular su posición, que se adjuntará al informe (apartado 6 del artículo 24 del Convenio).

2. La Autoridad Común de Control decidirá si publica o no su informe de actividad y, en caso afirmativo, determinará la manera en que deba publicarse.

TÍTULO III

REGLAMENTO INTERNO DEL COMITÉ DE RECURSOS

Artículo 11
Funciones del Comité de Recursos

1. El Comité de Recursos (denominado en lo sucesivo "el Comité") examinará los recursos a que se refieren los apartados 6 a 8 del artículo 19, el apartado 4 del artículo 20 y el apartado 3 del artículo 22 del Convenio.

2. El Comité adoptará decisiones finales con respecto a las materias mencionadas en el apartado 1.

3. Además de las competencias mencionadas en el apartado 2 del artículo 2, el Comité tendrá las competencias que se disponen en el presente capítulo.

Artículo 12
Composición

1. El Comité estará compuesto por un miembro de cada una de las delegaciones que componen la Autoridad Común de Control. Cada miembro tendrá un suplente. Los miembros del Comité y sus suplentes serán nombrados por períodos de cinco años por la Autoridad Común de Control, previa designación de la delegación correspondiente. Su mandato será renovable.

2. Los miembros del Comité y sus suplentes deberán poseer las capacidades exigidas para examinar y decidir sobre los recursos a que se refiere el apartado 1 del artículo 11; dichas capacidades deberán incluir, entre otras cosas, conocimientos y experiencia jurídica, experiencia en resolución de litigios y experiencia en cuestiones de protección de datos.

3. Cuando un miembro del Comité no pueda asistir a una reunión podrá ser representado por su suplente.

4. La pertenencia de una persona al Comité terminará con su dimisión o con su cese como miembro de la Autoridad Común de Control. Esta disposición se aplicará también a los suplentes.

Artículo 13
Independencia e imparcialidad

1. Los miembros del Comité serán independientes e imparciales, no estarán sujetos a instrucciones de la Autoridad Común de Control ni de nadie, en el ejercicio de sus funciones y sólo estarán sometidos a la ley. Mientras dure su mandato no podrán dedicarse a actividad alguna que sea incompatible con su independencia e imparcialidad como miembros del Comité ni con su necesaria disponibilidad al servicio del Comité. Las actividades que se lleven o se hayan llevado a cabo en nombre de la autoridad nacional de control no se considerarán incompatibles con la pertenencia al Comité. Las disposiciones del presente apartado se aplicarán también a los suplentes.

2. Cuando un miembro del Comité o un suplente haya estado implicado en un asunto de tal manera que puedan suscitarse serias dudas sobre su imparcialidad, o si surge cualquier otra circunstancia que pueda perjudicar la adecuada resolución de un recurso, el miembro o suplente declarará que se encuentra en esa situación y se retirará del asunto.

3. Si un miembro o suplente es recusado por una parte por motivos relacionados con lo dispuesto en los apartados 1 y 2, el Comité oirá a la persona de que se trate y a las otras partes y luego decidirá sobre la impugnación, en ausencia de dicha persona, mediante votación secreta.

4. Si una persona se retira o queda excluida del asunto en virtud del apartado 3, será sustituida por su suplente.

Artículo 14
Presidencia

1. El Comité elegirá entre sus miembros un presidente y un vicepresidente, por mayoría de dos tercios de los votos emitidos en votación secreta por los miembros que asistan a la reunión. Si ninguno de los candidatos logra la mayoría requerida en primera votación, se celebrará una segunda votación para elegir entre los dos candidatos que hayan obtenido mayor número de votos. Ni el presidente ni el vicepresidente de la Autoridad Común de Control podrán ser elegidos ni presidente ni vicepresidente del Comité. Tampoco podrán pertenecer los dos a la misma delegación. El presidente y el vicepresidente serán elegidos para un mandato de dos años. Podrán ser reelegidos para un segundo mandato de un año.

2. El presidente presidirá las reuniones del Comité. Supervisará el adecuado funcionamiento del Comité. Convocará las reuniones del Comité y fijará la sede, la fecha y la hora de dichas reuniones. Preparará el orden del día provisional.

3. Cuando el presidente no pueda asistir a una reunión lo suplirá el vicepresidente. En ausencia del vicepresidente, actuará como tal el miembro de mayor edad. Hasta la elección del presidente, la primera reunión del Comité será convocada y presidida por el miembro de mayor edad.

4. Con objeto de preparar sus deliberaciones, el Comité podrá nombrar de entre sus miembros, a propuesta del presidente, uno o varios ponentes. En ese caso, el miembro al que se nombre ponente será, en principio, del Estado miembro del que proceda el demandante o, si el demandante no procede de un Estado miembro, del Estado miembro con el que más relación tenga el caso. Cuando se trate de un asunto urgente, el nombramiento podrá hacerlo el presidente en virtud de sus competencias. En tal caso, informará inmediatamente de ello a los miembros del Comité. El ponente examinará el recurso y someterá al Comité un informe sobre su admisibilidad y una propuesta para la prosecución del procedimiento, en particular por lo que se refiere a las medidas preparatorias que sean necesarias.

Artículo 15
Representación

El demandante podrá estar asistido o representado por un abogado u otro asesor. El Comité podrá excluir del procedimiento a un abogado o asesor en caso de falta grave. En caso de que un abogado o asesor sea excluido, el presidente fijará un plazo para que la parte afectada pueda designar otro abogado o asesor; el procedimiento se suspenderá hasta la expiración de dicho plazo. El abogado o asesor deberá presentar una autorización adecuada del demandante en caso de que le sea requerida por el Comité.

Artículo 16
Lenguas

1. El procedimiento se desarrollará en una de las lenguas oficiales de las Instituciones de las Comunidades Europeas. El demandante elegirá la lengua oficial en la cual deba desarrollarse el procedimiento. La lengua del procedimiento se utilizará en las declaraciones orales y en la documentación escrita de las partes, así como en las actas y decisiones del Comité.

2. Los documentos escritos en una lengua distinta de la lengua del procedimiento irán acompañados de una traducción a la lengua del procedimiento. En caso de documentos extensos, la traducción presentada podrá limitarse a extractos o resúmenes. En virtud de sus competencias o a solicitud de una parte, el Comité podrá requerir una traducción completa en cualquier momento.

3. Cuando sea necesario, se proporcionarán gratuitamente servicios de interpretación y traducciones a cada miembro del Comité y a las partes. Las decisiones del Comité se traducirán a todas las lenguas oficiales de la Unión Europea.

4. Cuando el demandante no conozca ninguna de las lenguas oficiales de las Instituciones de las Comunidades Europeas, podrá presentar la reclamación en otra lengua. El demandante estará obligado a presentar un resumen en una de las lenguas oficiales. El presidente o el ponente deberán encargarse de que la reclamación se traduzca a la lengua elegida.

Artículo 17
Instrucción del procedimiento

1. El recurso deberá interponerse mediante la presentación de una reclamación escrita en la Secretaría de la Autoridad Común de Control en un plazo de tres meses a partir de la recepción, por parte del demandante, de la decisión de Europol. En ausencia de decisión, el recurso deberá interponerse en los tres meses siguientes a la expiración del plazo a que se refieren el apartado 6 del artículo 19, el apartado 4 del artículo 20 y el apartado 3 del artículo 22 del Convenio. Toda duda con respecto al cumplimiento de los plazos se resolverá en favor del demandante.

2. El demandante deberá exponer sucintamente el fundamento de su reclamación. Debe quedar claro quién reclama, cuál es el objeto de la reclamación y en qué se funda. La reclamación deberá ir acompañada de cualquier documentación que la justifique. El demandante podrá retirar su reclamación en cualquier momento.

3. La Secretaría acusará recibo de la reclamación dentro de un plazo de cuatro semanas y facilitará información general sobre el curso del procedimiento.

4. Si la reclamación no reúne los requisitos establecidos en las frases primera y segunda del anterior apartado 2 y en la segunda frase del apartado 4 del artículo 16, la Secretaría invitará al demandante a que rectifique cualquier omisión en el plazo de cuatro semanas.

5. Los recursos que no cumplan los requisitos serán desestimados por el Comité a propuesta del presidente o del ponente. Podrán aceptarse los recursos que no cumplan el plazo mencionado en el apartado 1 cuando se den circunstancias especiales que justifiquen el retraso.

Artículo 18
Consideración preliminar

1. Si la reclamación cumple los requisitos, el Comité la examinará basándose en las siguientes disposiciones y teniendo en cuenta el Convenio, especialmente sus artículos 19, 20 y 22.

2. Se transmitirá una copia de la reclamación a Europol para que formule sus observaciones, que deberán presentarse en un plazo de cuatro semanas, con posibilidad de prórroga de otras dos semanas.

3. El Comité podrá decidir, atendiendo a las circunstancias de cada caso, hacer intervenir, además, en el procedimiento del recurso a una o varias unidades nacionales. El demandante y Europol serán informados de dicha decisión. Se transmitirá una copia de las observaciones de Europol y del demandante a las unidades nacionales afectadas, para que puedan formular sus propias observaciones, que deberán presentarse en un plazo de cuatro semanas, con posibilidad de prórroga de otras dos semanas.

4. Cuando se hayan recibido las observaciones o hayan expirado los plazos, el Comité deberá ver la reclamación en los tres meses siguientes.

Artículo 19
Información adicional

1. El Comité podrá pedir al demandante, a Europol, a las unidades nacionales, a las autoridades nacionales de control o a cualquier otra autoridad, que transmitan información, pruebas u observaciones al Comité. Las partes tendrán derecho a hacer sugerencias al Comité acerca de la obtención de pruebas o a solicitar la admisión de pruebas. El Comité aceptará tales sugerencias y solicitudes de admisión en la medida necesaria para el examen del caso.

2. El Comité podrá decidir también que se lleve a cabo una investigación en los locales de Europol. Será asimismo de aplicación el artículo 7. En ese caso, se informará al demandante o a su asesor sobre el resultado de la investigación.

Artículo 20
Acceso al expediente del procedimiento

1. Todas las partes que lo deseen tendrán acceso al expediente del procedimiento y podrán pedir a la Secretaría de la Autoridad Común de Control que les proporcione extractos o fotocopias, que correrán por cuenta de quien los haya solicitado. Se denegará el acceso cuando sea necesario para:

- permitir a Europol cumplir debidamente sus funciones
- proteger la seguridad y el orden público de los Estados miembros o efectuar la prevención del delito
- proteger los derechos y libertades de terceros

consideraciones que no pueden supeditarse a los intereses de la persona afectada.

2. Europol, las unidades nacionales y las autoridades nacionales de control podrán indicar en qué medida la información que faciliten no debe transmitirse al demandante, así como las razones de esta restricción. El Comité podrá solicitar que se aduzcan más razones. Si el Comité considera que las razones son aceptables, la información en cuestión será retenida. El Comité sólo podrá resolver en sentido contrario por falta de razones aceptables y si en su seno hay unanimidad al respecto. En tal caso el Comité podrá acordar que se ponga a disposición del demandante un resumen o que se le facilite cierta información.

Artículo 21
Audiencia

1. El Comité oirá a las partes si lo piden. El Comité informará en la debida forma a las partes de su derecho de ser oídas. Este derecho se ejercerá por escrito.
A instancia de una de las partes del procedimiento, el Comité podrá decidir que se celebre una vista, en la medida en

que se considere necesaria para examinar el caso. El Comité informará debidamente a las partes de su derecho de solicitar una vista. Se notificará oportunamente la vista a todas las partes y éstas tendrán derecho a estar presentes.

2. La vista será pública a menos que el Comité decida, en virtud de sus competencias o a instancia de una de las partes, excluir total o parcialmente al público cuando lo exijan los intereses de la seguridad pública, sobre todo por los motivos a que se refiere el apartado 3 del artículo 19 del Convenio, o la protección de la intimidad de un individuo o en el grado estrictamente necesario, a juicio del Comité, en circunstancias especiales en que la publicidad pueda perjudicar la debida resolución del recurso. Si un Estado miembro, que sea parte en el procedimiento o Europol solicitan que se excluya al público de la vista, el Comité sólo podrá resolver en contrario si estima que no concurren las razones mencionadas en la primera frase y si en su seno hay unanimidad al respecto.

3. El Comité podrá decidir, a instancia de parte o por iniciativa propia, oír a una parte sin que otras partes estén presentes, cuando lo considere necesario para garantizar el correcto funcionamiento de Europol, para proteger la seguridad de un Estado miembro, los intereses del demandante o de terceros. Las partes ausentes serán informadas de las actuaciones que hayan tenido lugar en su ausencia.

Artículo 22
Audiencia de testigos y peritos

1. El Comité podrá decidir, a instancia de parte o por iniciativa propia, oír a testigos. Se notificará oportunamente la vista a todas las partes y testigos en cuestión. Se aplicará también lo dispuesto en los apartados 2 y 3 del artículo 21.

2. Los testigos citados por el Comité tendrán derecho al reembolso de todos sus gastos de viaje y alojamiento y a que se les indemnice, en el grado que el Comité considere equitativo, por los ingresos que hayan dejado de percibir. Podrán cobrar los anticipos necesarios. Todos los pagos se efectuarán con cargo al presupuesto de la Autoridad Común de Control.

3. Los testigos serán oídos por el Comité. Los miembros del Comité podrán hacerles preguntas. Previa autorización del presidente, las partes podrán hacer preguntas a los testigos. Antes de que comience la vista, el presidente recordará a los testigos que deben decir la verdad.

4. El Comité podrá nombrar un perito y definir su cometido. El perito tendrá derecho a ser remunerado por su trabajo. El Comité podrá decidir oír al perito. Se aplicarán igualmente las normas relativas a la declaración de los testigos.

Artículo 23
Declaraciones finales

Antes de tomar una decisión final, el Comité invitará a todas las partes a que presenten sus observaciones finales.

Artículo 24
Actas

1. El Comité levantará acta de sus actuaciones y recogerá en ellas el desarrollo de cada vista y las declaraciones realizadas en ella. Las partes podrán solicitar que consten en acta la totalidad o parte de determinados documentos o declaraciones. El acta será firmada por el presidente, se remitirá a las partes y se adjuntará al expediente del caso. En los casos a que se refieren el apartado 2 del artículo 21 o el apartado 1 del artículo 22, el Comité impondrá restricciones.

2. Las disposiciones del artículo 9 se aplicarán igualmente a todas las reuniones del Comité a las que no asistan las partes.

Artículo 25
Decisiones y confidencialidad

1. Las reuniones del Comité sólo serán válidas si asisten cuatro quintos de los miembros o sus suplentes.

2. Las decisiones se tomarán por mayoría simple de los miembros o suplentes que asistan a la reunión, salvo disposición en contrario del presente Reglamento interno o del Convenio. En caso de empate, el presidente tendrá voto de calidad. Todas las personas que participen en la decisión final deberán haber asistido a una vista.

3. Las deliberaciones del Comité serán confidenciales.

4. La decisión final del Comité recogerá los nombres de las partes y de sus representantes, los nombres de los miembros del Comité que hayan participado en la decisión, la fecha en que se haya hecho pública, la parte dispositiva de la decisión, una exposición sucinta de los hechos del caso y los motivos de la decisión. La decisión final se dará a conocer en una reunión pública y se transmitirá a las partes. Se remitirá una copia de dicha decisión a la Autoridad Común de Control.

Artículo 26
Notificaciones

Las notificaciones y otras comunicaciones a las partes, testigos y peritos se harán por medios que garanticen, dentro de

lo razonable, que éstos han sido debidamente informados y que puede, en caso necesario, comprobarse.

Artículo 27
Costas

1. El Comité incluirá en su decisión final una decisión sobre las costas del procedimiento. El procedimiento ante el Comité será gratuito. Si se admite el recurso, en su totalidad o en parte, los gastos que haya ocasionado al demandante la presentación y tramitación de la reclamación correrán por cuenta de Europol en la medida en que el Comité lo considere justo.

2. Si un demandante no puede sufragar la totalidad o una parte de los gastos del procedimiento, podrá solicitar, en cualquier momento, ayuda para hacerles frente. Cuando presente su solicitud, el demandante adjuntará documentación que demuestre que necesita asistencia. El Comité podrá retirar la ayuda en cualquier momento si durante el procedimiento dejan de cumplirse las condiciones en virtud de las cuales le fue concedida. De aprobarse la concesión de ayuda, los gastos se sufragarán con cargo al presupuesto de la Autoridad Común de Control. Cuando sea justo, en la decisión final podrá exigirse a una parte que reintegre al presupuesto de la Autoridad Común de Control los anticipos recibidos. Al presentar su solicitud, el demandante deberá declarar que acepta reintegrar las costas si la decisión final lo exige.

Artículo 28
Garantías de procedimiento

En los casos no previstos en las presentes disposiciones, el Comité procederá de acuerdo con los principios generales del Derecho comunitario a que se hace referencia en el apartado 2 del artículo F del Tratado de la Unión Europea.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 29
Secretaría

1. La Autoridad Común de Control contará, en su sede, con una Secretaría que la asista en el cumplimiento de su cometido. La Secretaría será un cuerpo permanente cuyos miembros serán contratados exclusivamente en función de su competencia. Los miembros de la Secretaría sólo actuarán en defensa de los intereses de la Autoridad Común de Control, serán plenamente independientes de Europol y no aceptarán instrucciones de ninguna otra autoridad. La contratación y el envío de personal a la Secretaría se llevará a cabo a propuesta de la Autoridad Común de Control. El personal de la Secretaría no desempeñará otras funciones sin el permiso del presidente de la Autoridad Común de Control.

2. La Secretaría actuará bajo la dirección del presidente de la Autoridad Común de Control de acuerdo con las normas establecidas por la Autoridad Común de Control. La Secretaría prestará también sus servicios al Comité de Recursos; para estas funciones estará bajo la dirección del presidente de dicho Comité. La Secretaría llevará un registro de los recursos y de todos los demás documentos.

3. La Secretaría garantizará que las obligaciones contraídas en virtud del artículo 32 del Convenio se respeten también en el desempeño de las funciones de la Autoridad Común de Control.

Artículo 30
Confidencialidad

1. Los miembros de la Autoridad Común de Control, los suplentes, los peritos y los miembros de la Secretaría tendrán la obligación de tratar de manera confidencial los datos que conozcan en el ejercicio de su actividad, a menos que el correcto desempeño de sus funciones exija que actúen de otra manera. Esta obligación continuará aplicándose también cuando cesen en sus funciones.

2. En el momento de su nombramiento, los miembros de la Autoridad Común de Control, los suplentes, los peritos y los miembros de la Secretaría declararán que aceptan estas obligaciones.

3. El miembro o suplente de la Autoridad Común de Control que incumpla la obligación de confidencialidad podrá ser suspendido por decisión tomada en votación secreta por mayoría de dos tercios de los votos emitidos por las delegaciones que asistan a una reunión de la Autoridad Común de Control. Con anterioridad, se oirá al interesado, que no tomará parte en la decisión. Esta disposición se aplicará también al Comité de Recursos cuando el incumplimiento de la obligación de confidencialidad se refiera al trabajo de dicho Comité. En este caso, se informará sin demora a la Autoridad Común de Control.

En caso de suspensión, el puesto del miembro suspendido será ocupado por su suplente. La suspensión se comunicará a la Autoridad Nacional de Control responsable del nombramiento del miembro suspendido.

Artículo 31
Presupuesto y gastos

1. La Secretaría elaborará propuestas de presupuesto anual para la Autoridad Común de Control, que, tras su aprobación, serán transmitidas al Consejo de Administración con antelación a la consulta a que se refiere el apartado 9 del artículo 24 del Convenio.

2. La Autoridad Común de Control decidirá que se efectúen los pagos a cargo del presupuesto que le haya sido asignado, que será administrado por la Secretaría.

3. Los gastos de la Autoridad Común de Control y del Comité de Recursos, incluidos los correspondientes a los miembros del Comité y a sus suplentes, que sean necesarios para el correcto ejercicio de sus funciones, se sufragarán con cargo al presupuesto de la Autoridad Común de Control de acuerdo con las normas establecidas por la misma.

Artículo 32
Modificación del Reglamento interno

Las modificaciones del presente Reglamento interno deberán ser adoptadas por unanimidad por la Autoridad Común de Control (primera frase del apartado 7 del artículo 24 del Convenio) y serán presentadas al Consejo, que deberá aprobarlas por unanimidad.

Artículo 33
Evaluación

La Autoridad Común de Control evaluará el presente Reglamento Interno entre uno y tres años después de su entrada en vigor.

Artículo 34
Entrada en vigor del Reglamento Interno

El presente Reglamento Interno entrará en vigor al día siguiente de su aprobación por el Consejo, de conformidad con lo dispuesto en el apartado 7 del artículo 24 del Convenio.

Hecho en Bruselas, el 22 de abril de 1999

Por la Autoridad Común de Control

El Presidente,

Fergus GLAVEY

DECLARACIÓN DEL CONSEJO
sobre el apartado 5 del artículo 4 y sobre el apartado 4 del artículo 12
del Reglamento interno, aprobada al adoptar el Reglamento interno
de la Autoridad Común de Control de Europol

Los Estados miembros convienen en que la destitución de un miembro titular o suplente de la Autoridad Común de Control antes del término del mandato no podrá producirse por motivos vinculados al ejercicio de sus funciones en el Comité de recursos.

MEMORIA DE 1999 - ANEXO X - POSICIONES COMUNES DEL GRUPO DE BERLIN

Posición Común sobre tecnologías de reconocimiento del interlocutor y de análisis de voz en telecomunicaciones.

(adoptada en la 25 reunión del Grupo de Trabajo el 29 de abril de 1999 en Noruega).

Entre los métodos de identificación biométricos desarrollados actualmente, el utilizado para reconocer al hablante es probablemente el más avanzado y de especial relevancia en el campo de las telecomunicaciones.

El reconocimiento del hablante es un método que analiza determinadas características de la voz de una persona con el fin de:

* Identificar la voz de un hablante desconocido.
* Verificar que un hablante es quien dice ser (autenticación).
* Reconocer la voz de una persona concreta en un entorno con diversos hablantes.

Los mejores resultados en reconocimiento de hablante, en términos de tasa de fallos, se consiguen cuando se utiliza el mismo conjunto de palabras en el proceso de reconocimiento *(sistemas dependientes del texto).* Este es el caso de una clave o identificador predeterminado y que una vez introducido en el sistema se compara con el registro patrón previamente grabado.

En otros sistemas se requiere que los hablantes repitan de forma aleatoria una serie de palabras seleccionadas y que son sugeridas por el sistema. Estas palabras son comparadas con los patrones *(sistemas de texto requerido).* Una ventaja de estos sistemas es la robustez que ofrecen frente a impostores que utilizan ejemplos de voces previamente grabadas.

Finalmente, en los *sistemas independientes del texto* se requiere al hablante para que hable, comparándose sus palabras con los patrones previamente registrados y que contienen diferentes palabras. Esta situación puede dar lugar a un mayor número de contingencias, a la vez que la comparación con los patrones se hace más complicada, sobre todo en los casos en los que existe ruido de fondo o la comunicación se produce a través de líneas telefónicas con ruido. Por otro lado, el potencial de estos sistemas es elevado: combinado con una gran base de datos de patrones de voces, un sistema independiente del texto permite la identificación de múltiples personas en muy diversas circunstancias.

Los sistemas de reconocimiento del hablante pueden ser utilizados para la identificación y autenticación tanto para el acceso a la red como para el acceso a los servicios ofrecidos por la misma. Obviamente, los operadores de telecomunicaciones tienen un especial interés en mejorar los sistemas de identificación y autenticación de voz por diferente motivos, como por ejemplo la lucha contra el fraude en las telecomunicaciones o la promoción de nuevos servicios. En la prestación de servicios a través de las redes de telecomunicaciones, la identificación de los clientes se considera cada vez más un factor muy importante a la hora de tomar decisiones sobre la manera en que el cliente va a ser tratado.

Es necesario hacer notar que, al contrario que en la mayoría de los sistemas de identificación biométricos, los sistemas de reconocimiento del hablante no necesitan una nueva infraestructura y pueden ser integrados en las redes de telecomunicación existentes.

Aunque el uso de los sistemas de reconocimiento del hablante se circunscribe actualmente a aplicaciones muy concretas, se espera que su implantación se generalice rápidamente como consecuencia de la disminución del coste de ésta tecnología y de la mejora en la calidad de estos sistemas.

Los Responsables de Privacidad y Protección de Patos han establecido en diversas ocasiones como elementos esenciales para el anonimato en las redes el disponer de medios de acceso y de pago anónimos.

El Grupo de Trabajo Internacional de Protección de Datos en Telecomunicaciones está especialmente sensibilizado por el riesgo que conlleva la implantación de estas tecnologías en las redes de telecomunicaciones sin el conocimiento de los usuarios o sin mecanismos que les permitan evitar su empleo.

Recomendaciones:

1. La introducción y el empleo de las tecnologías de reconocimiento del hablante en las redes de telecomunicaciones deberían estar limitadas a las circunstancias donde los mecanismos de autenticación sean esenciales.

2. Dado que estos mecanismos de identificación presentan inevitablemente cierto margen de error en el reconocimiento del hablante, no deberían ser utilizados sin establecer los mecanismos adecuados de corrección..

3. Se debe requerir el consentimiento previo de las personas antes de aplicar las tecnologías de análisis de voz. En principio, estas tecnologías no se deberían de aplicar con el fin de obtener el estado emocional o mental de una persona aunque se haya obtenido previamente su consentimiento.

4. Siempre que sea apropiado se debe facilitar al afectado la posibilidad de acceso anónimo.

5. Se deberá informar a los afectados en aquellos casos en los que sus patrones de voz se almacenen en bases de

datos. Se deberá informar también sobre las circunstancias en que dichos datos van a ser utilizados.

6. Quienes apliquen las técnicas de reconocimiento del hablante deberán informar al afectado de su identidad y de la finalidad en base a la cual se van a utilizar dichas técnicas.

Posición Común sobre

Agentes de Programa Inteligente.

(adoptada en la 25 reunión del Grupo de Trabajo el 29 de abril de 1999 en Noruega).

Se define un Agente de Programa Inteligente (Intelligent Software Agent) como una porción de programa que actúa por medio de un usuario con el fin de cumplir determinados objetivos realizando determinadas tareas y sin que exista ningún control o supervisión directo por parte del usuario para el que actúa. Este tipo de agentes presentan numerosas aplicaciones en el campo de las telecomunicaciones, pudiéndose realizar con ellos un uso más efectivo de las redes de telecomunicaciones si los recursos de la red se adaptan a la demanda de los usuarios. Los Agentes pueden realizar estas tareas para sus usuarios.

Otra aplicación de los agentes está relacionada con los servicios de contenido de valor añadido que se facilitan a través de las redes de telecomunicaciones. En este caso, los agentes pueden ser utilizados para seleccionar y obtener información (ej. en Internet) y para actuar como intermediarios frente a terceros en transacciones electrónicas. Actualmente empiezan a estar disponibles servicios de este tipo, que van desde los sencillos sistemas denominados de *"tecnología push"*, que extraen fácilmente la información de interés especificada por el usuario, hasta sofisticados sistemas que permiten la personalización de las sesiones de red del usuario y el seguimiento y registro de sus actividades en la propia red.

El desarrollo de la tecnología de agentes llevará al desarrollo de los Agentes de Programas Inteligentes, o programas, a veces apoyados en desarrollos específicos de equipos físicos, diseñados para realizar tareas para su usuario. Al realizar su función en representación del usuario, el agente genera y recopila abundante información personal sobre el usuario para quien actúa, información que puede ser intercambiada por el agente. La privacidad y la confidencialidad de las acciones se encuentran entre los principales asuntos a los que debe hacer frente en el futuro el uso de los agentes.

Esta Posición Común pretende concienciar sobre los riesgos a la privacidad asociados con el uso de los agentes y animar a los diseñadores de sistemas a incorporar medidas de protección de la privacidad. Los riesgos asociados a la utilización de agentes pueden ser agrupados de la siguiente manera:

1. En primer lugar, los riesgos asociados con el hecho de que un agente actúa en nombre de un usuario y que por lo tanto, es el perfil del usuario el núcleo en torno al cual el agente realiza las actividades que se le encomiendan. Típicamente, el perfil del usuario contiene la identidad y la información de contacto, así como una gran cantidad de información sobre las preferencias personales. Cuando un agente opere en una red, los datos personales serán intercambiados con el entorno y podrán ser cedidos a terceras partes no autorizadas.

2. En segundo lugar, los riesgos asociados con los agentes externos que actúan para sus usuarios. Los agentes, o generalmente los usuarios, deben enfrentarse con los demás agentes que actúan para otros usuarios. Éstos, recogerán datos personales de los individuos realizando análisis de tráfico de información, accediendo a bases de datos que contienen información sobre el individuo o recabando el perfil de usuario definido en un agente. También pueden incluso aparecer enmascarados o anulando otros agentes.

Recomendaciones:

Se deberían de tomar medidas con el fin de reducir el impacto de los riesgos que para la privacidad presentan los Agentes de Programa Inteligente. El Grupo de Trabajo recomienda que se tengan en cuentan además de los requerimientos necesarios para asegurar el cumplimiento de los principios de protección de datos, los siguientes:

1. Los fabricantes de programas deberían reflejar en las fases previas de sus diseños las implicaciones que la utilización de los agentes tiene para la privacidad de los usuarios. Este aspecto es necesario para controlar las consecuencias que puedan surgir en un futuro a corto plazo.

2. Los que desarrollen agentes deberían facilitar los mecanismos que permitan al usuario mantener el control sobre el sistema y la información contenida en él. Deberían también facilitar, con la máxima transparencia y claridad posible, las especificaciones funcionales del agente. El añadir mecanismos de control y salvaguarda ayudaría a incrementar la confianza en el empleo de la tecnología de agentes.

3. Los que desarrollen agentes inteligentes deberían de garantizar la existencia de mecanismos adecuados para proteger la privacidad de los usuarios y para permitir que éstos puedan controlar el uso que se da a sus datos personales.

4. Se recomienda la utilización de Tecnologias Avanzadas de Privacidad (PET) en conjunción con los programas de agente. En este sentido se proponen las siguientes medidas:

- Desarrollo de un esquema de Tercera Parte Segura (TTP) para la identificación y autenticación de todos los agentes.

- Mecanismos de control de acceso.

- Desarrollo de herramientas que proporcionen al usuario el control sobre la recogida que terceros agentes puedan realizar de sus datos personales.

- Mecanismos para poder auditar los registros de actividades (Logs).

- Mecanismos de integridad sobre los datos almacenados e intercambiados, así como sobre los métodos de trabajo de los agentes, como por ejemplo los mecanismos de firma digital.

Las medidas mencionadas pueden ser integradas en los agentes y pueden ser utilizadas también en la construcción de una arquitectura de componentes seguros.

5. El diseñador o proveedor de un agente debería de verificar el grado de cumplimiento de los criterios de privacidad mediante la utilización de listas de comprobación y debería diseñar o equipar el agente con las adecuadas tecnologías avanzadas de privacidad. En este sentido se considera necesario el establecer un marco de certificación de privacidad para los agentes.

Posición Común sobre la protección de datos
en bases de datos de imágenes de edificios
(adoptada en la 25 reunión del Grupo de Trabajo el 29 de abril de 1999 en Noruega).

Los ordenadores tienen la capacidad de integrar, a la vez que facilitar el acceso, a la información procedente de diversas fuentes incluidas los registros públicos. En el caso de los sistemas basados en *Sistemas de Información Geográfica* (GIS) que permiten la localización por referencias geográficas, el uso del ordenador puede permitir la captación de una gran cantidad de información a partir de direcciones o referencias en un mapa, pudiendo representar una amenaza creciente a la privacidad de los ciudadanos. Recientemente se ha desarrollado un sistema que recoge las imágenes en formato digital de las viviendas con el fin de crear una base de datos de edificios de una ciudad para fines comerciales. Si bien los sistemas de información geográfica permiten el desarrollo de importantes y legítimas aplicaciones, como por ejemplo la construcción de una base de datos de viviendas para el planeamiento urbano, la posición del afectado con respecto a la utilización comercial de estas bases de datos debe ser reforzada.

A modo de ejemplo, en algunos países, determinadas compañías están actualmente utilizando cámaras digitales móviles montadas sobre vehículos con el fin de recoger las imágenes de los edificios de las principales ciudades. Los datos recogidos pueden ser almacenados en un soporte tipo CD-ROM y ofrecidos a servicios de emergencia, bomberos, policía, etc. con el fin de ayudarles en sus operaciones. Es evidente también, que estas bases de datos pueden ser utilizadas también con fines comerciales. Se pueden asociar las imágenes con los números de las viviendas y con los nombres de los propietarios o habitantes con el fin de catalogar a la población y realizar valoraciones del riesgo (condición de la vivienda, clasificaciones de barrios) por los bancos y compañías de seguros y para fines de publicidad directa. Los datos podrían ser utilizados también por la televisiones y por profesionales del transporte (empresas de transporte de paquetes, taxis, etc.). También pueden ser procesados estos datos junto con datos recogidos de satélites (*Sistemas de Posicionamiento Global* o GPS) y ser utilizados para generar mapas digitales reales y para crear una nueva generación de sistemas de información geográfica. Aunque actualmente y dependiendo del sistema utilizado pueden presentarse problemas de capacidad de almacenamiento y de rendimiento, que pueden hacer inviable el poner estos datos en Internet a un coste razonable, es previsible que la situación cambie.

Parece claro que el registrar de forma completa las imágenes de todos los edificios de una ciudad o país conlleva el tratamiento de datos personales puesto que mucha de la información se refiere a personas físicas que son identificables por factores específicos a su identidad física, económica, cultural y social en un fichero de datos [Art. 2 a) y c) de la Directiva 95/46/CE], y puede ser referenciado directa o indirectamente en directorios. Por consiguiente, la creación de bases de datos de imágenes como las descritas quedarían dentro del ámbito de aplicación de las legislaciones nacionales de protección de datos de acuerdo con la Directiva Europea de Protección de Datos. Donde no sea aplicable todavía, la legislación nacional debería al menos reconocer al afectado el derecho de oposición a la recogida sistemática y posterior almacenamiento de las imágenes de su vivienda para fines comerciales. El hecho de que esta información sea de alguna manera pública no la excluye del ámbito de aplicación de la normativa de protección de datos. Además, la publicación de tales bases de datos puede causar problemas de seguridad al afectado (propietarios, inquilinos o habitantes). Existe una gran diferencia entre una persona que realiza fotografías de una casa específica por razones personales y una compañía que sistemáticamente recoge imágenes de las edificaciones de una ciudad para fines comerciales. En este caso, el afectado debería disponer del derecho de oposición en cualquier momento a que estos datos sean publicados ya sea a través de Internet o a través de cualquier otro medio electrónico (ej. CD-ROM).