AGENCIA DE PROTECCIÓN DE DATOS

MEMORIA 1997

MEMORIA DE 1997 - PRESENTACIÓN

Me corresponde a mí, como actual Director de la Agencia de Protección de Datos, el presentar la memoria correspondiente al pasado año 1997, en el que la Agencia era dirigida por otra persona. La meritoria labor desarrollada en el pasado ejercicio, según se constata en la Memoria, es pues obra del anterior Director, D. Juan José Martín-Casallo López, y de todo el equipo de funcionarios que trabajaron en la Agencia de Protección de Datos en dicho período.

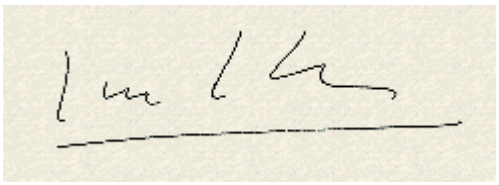
La memoria refleja fielmente las principales actividades llevadas a cabo en el año 1997 en el que se aprecia la consolidación de la Agencia, según se deriva del aumento en todas ellas. La cifra de ficheros inscritos en el Registro General de Protección de Datos llegó a 229.804. De igual forma la actividad de la Inspección de Datos se ha visto notablemente incrementada, tanto por la mayor denuncia de posibles infracciones por parte de los ciudadanos, como por las inspecciones realizadas de oficio, que ascendieron a un total de 375, consecuencia de lo cual es el incremento de procedimientos sancionadores en un porcentaje del 125%.

Las consultas evacuadas por el Área de Atención al Ciudadano han experimentado un incremento del 65% lo que hace que hayan llegado a 1009, a las que hay que añadir las realizadas para las administraciones y diversas entidades públicas y privadas a las que la Agencia está siempre dispuesta a ayudar para el mejor cumplimiento de las obligaciones que les exige la Ley Orgánica 5/1992. Todo esto supone como principal resultado, el que se comprueba, como la Ley va calando en la sociedad, y los ciudadanos son cada día más conscientes de sus derechos y de la existencia de la Agencia de Protección de Datos como garantía de su derecho a la intimidad ante un tratamiento automatizado de datos personales que protege el art. 18.4 de la Constitución Española.

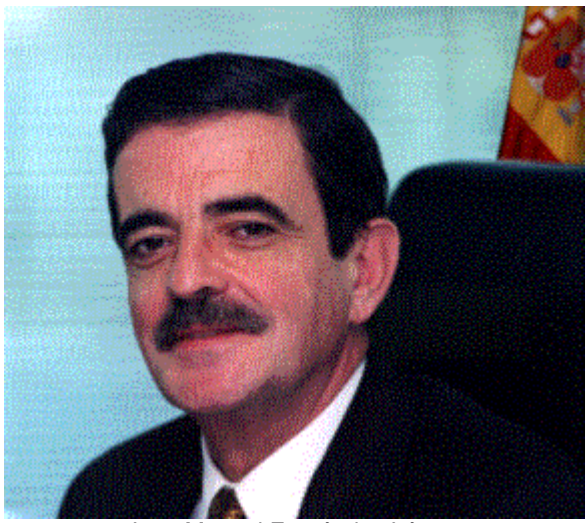
No menos desdeñable es la activa presencia de la Agencia en Organismos Internacionales, principalmente en aquellos que nuestra integración en la Unión Europea exige.

Toda esta labor llevada a cabo durante 1997, ha de constituir sin duda para mí, recientemente nombrado Director de la Agencia de Protección de Datos, un estímulo en el desempeño de las funciones que la LORTAD me encomienda y que he acometido ya con el mayor entusiasmo y dedicación en el mejor servicio a los ciudadanos.

El Director de la Agencia de Protección de Datos.



Juan Manuel Fernández López.



Juan Manuel Fernández López.

MEMORIA DE 1997 - FUNCIONAMIENTO DE LA AGENCIA

1. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

El número de informes efectuado por la Agencia, sobre Proyectos de disposiciones, ha sido de 20, cifra ligeramente inferior a los efectuados en el año anterior (21).

Dentro de los mismos, merecen destacarse el relativo al anteproyecto de Ley de Medidas Fiscales, Administrativas y de Orden Social, y addenda del mismo; el informe al Anteproyecto de Ley de incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo por el que se regula la protección jurídica de las bases de datos.

En el Anexo I de la Memoria se contiene una relación completa de todos los que fueron objeto de informe.

2. CONSEJO CONSULTIVO

* El Consejo Consultivo, previsto en el articulo 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.

* En su composición, está integrada por los siguientes miembros:

- Presidente:
D. Juan José Martin-Casallo López, Director de la Agencia de Protección de Datos.

- Vocales:
D. Carlos Navarrete Merino, Diputado propuesto por Congreso de los Diputados
Dª. Rosa Vindel López, Senadora propuesta por el Senado
D. José Antonio India Gotor, 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. Eduardo Vilariño Pintos, Vocal propuesto por el Consejo de Universidades .
D. Adolfo Varela Cea, 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 Cámara de Comercio, Industria y Navegación.
D. José Ramón Recalde Díez, Representante de la Administración Central, designado por el Gobierno.

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

* Un estricto cumplimiento de los artículos antes referenciados exigiría la designación de los Vocales que seguidamente se relacionan:

- Un 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:

- Planes de actuación de la Inspección de Datos y del Registro General de Protección de Datos a lo largo de 1997.

- Convocatoria de la primera edición del Premio Protección de Datos Personales, así como fallo del mismo.

- Reunión en España de Autoridades de Protección de Datos Europeas con representantes de los países Iberoamericanos en el marco de la Conferencia de Ministros de Justicia de los Países Hispano-Luso-Americanos.

- Reuniones con la Consejería de Interior del Gobierno Vasco en relación con los ficheros de la Ertzaina.

- Posible reforma legislativa de la Ley Orgánica 5/1985 de Régimen Electoral general, sobre uso y utilización del censo electoral, en relación con la Ley 7/1996 de Ordenación del Comercio Minorista.

- Designación de la Agencia de Protección de Datos española como organizadora de la XX Conferencia Internacional de Autoridades de Protección de Datos que se celebrará en Santiago de Compostela en septiembre de 1998.

- Elaboración por la Agencia de un Manual de Recomendaciones a usuarios de Internet.

- Próxima expiración del mandato de la mayoría de los miembros del consejo Consultivo y del Director de la Agencia.

3. EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

3. 1. INTRODUCCIÓN

El Registro General de Protección de Datos, es el órgano al que le corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con la finalidad de que los ciudadanos puedan 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, asi como 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 en el Registro General se pueden resumir en los siguientes puntos:

* El responsable del tratamiento, 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 tratamiento de datos no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la Ley.

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

* La notificación de los tratamientos de datos al Registro, supone una obligación para los responsables del tratamiento que posibilita el ejercicio de los derechos otorgados a las personas.

* La notificación de los tratamientos de datos personales, tiene como objeto principal asegurar la publicidad de los fines de los tratamientos y de sus principales características.

A lo largo del cuarto año de actividad del Registro General, se han seguido estableciendo las actuaciones precisas para implantar las mejoras necesarias en los sistemas de organización y control con el fin de racionalizar y simplificar los trámites y métodos de los procedimientos de notificación e inscripción de ficheros. 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 3.312 nuevos ficheros, se han modificado 8.023 inscripciones y se han suprimido 1.971.

Para cumplir con el precepto de dar publicidad a la existencia de ficheros se ha realizado una publicación del catálogo de ficheros en la red Internet, lo que permite completar las publicaciones que se vienen realizando en papel y en CD-ROM, permitiendo con este medio que los ciudadanos puedan conocer la situación de los ficheros a efectos de inscripción con una actualización mensual.

3. 2. PUBLICACIÓN DEL CATÁLOGO DE FICHEROS INSCRITOS EN SOPORTE CD-ROM Y EN INTERNET

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, correspondiente al año 1997.

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

Desde la puesta en marcha de la Agencia se han realizado dos publicaciones de este tipo, las correspondientes a 1995 y a 1996.

La primera de ellas en soporte papel se editó en colaboración con el Boletín Oficial del Estado, resultando excesivamente voluminosa y por tanto poco manejable.

Debido a ello, en la publicación del siguiente catálogo, correspondiente a 1996, 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 y para la publicación del catálogo correspondiente a 1997, se optó por continuar utilizando el soporte en CD-ROM, y además se ha completado con la publicación del mismo en la red Internet.

Los datos publicados en el soporte CD-ROM para el Catálogo 1997, por 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 al fichero

- 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.

En la publicación en CD-ROM del Catálogo de ficheros 1997, se mantienen los criterios y facilidades de consulta del año anterior por uno o varios de los campos que se publican por cada fichero, permitiendo además la consulta por texto libre.

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 son:

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

* 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 sobre Protección de Datos, respectivamente.

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

Sin embargo, la gran novedad de este año, ha sido la publicación del Catálogo de ficheros en Internet, pues no se puede obviar el impacto que la red ha supuesto últimamente en nuestra sociedad.

La publicación en Internet se incluye como una opción mas dentro de la Web institucional de la Agencia, en la que se ha abierto un nuevo apartado dedicado al Registro, donde se puede encontrar en primer lugar, información con carácter general, también se facilitan las instrucciones necesarias para inscribir nuevos ficheros en el Registro, facilitando incluso, el modelo normalizado de inscripción tanto de ficheros de titularidad pública, como de titularidad privada. Y por supuesto el catálogo de ficheros propiamente dicho.

En el catálogo de ficheros a través de Internet, se incluye de cada inscripción de fichero el nombre del responsable y/o encuadramiento administrativo, en función de la titularidad, dirección en la que se pueden ejercer los derechos de acceso al fichero, nombre del fichero y su descripción y el tipo, número y fecha del Boletín en el que se ha publicado la disposición de creación del fichero, para los ficheros de titularidad pública, tal como aparece en la publicación en CD-ROM, y además se amplia esta información con la publicación de la finalidad y los usos previstos declarados en la inscripción de cada fichero, resultando más completa la publicación en Internet.

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 contenga dicho texto en cualquiera de los campos del formulario de búsqueda.

Además, para los ficheros de titularidad pública se ha implementado una consulta que reproduce la estructura jerárquica 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, pudiendo ampliar la información detallada declarada en su inscripción en el Registro, y publicada para un fichero concreto.

Finalmente, tiene especial relevancia en este soporte de publicación, la ventaja que ofrece al ciudadano el hecho de disponer de la información obrante en el Registro General de Protección de Datos prácticamente puesta al día, pues con una periodicidad mensual se realiza la actualización de la misma.

3. 3. FICHEROS DE TITULARIDAD PÚBLICA

3. 3. 1. EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS

A lo largo del año 1997, ha ascendido a 4.374, el número de movimientos registrales efectuados sobre ficheros de titularidad pública en el Registro. Mediante recepción de notificación por parte de cada responsable, se han realizado 1.524 inscripciones, al cierre del ejercicio 1.523, debido a la supresión posterior de una inscripción, 344 modificaciones y se han suprimido 39 ficheros, correspondiendo el resto, 2.468, a operaciones de oficio, de ellas 2.457 modificaciones y 11 supresiones, una de estas operaciones se corresponde con un fichero inscrito en el mismo 97, de normalización y adecuación del Registro a las disposiciones de regulación de los ficheros.

De las inscripciones realizadas en el año, 1.115, es decir, el 73% aproximadamente, corresponde a ficheros de la Administración Local y Organismos Públicos de las Entidades Locales, sector en el que aún no se ha alcanzado la estabilidad respecto a la inscripción de ficheros, debido al gran número de Ayuntamientos existentes en España, 8.087, de los que el 58,07% aún no ha formalizado la inscripción de sus ficheros. Por tanto, el número de inscripciones a pesar de ser el más elevado respecto a otras Administraciones, sólo supone un crecimiento aproximado del 5% respecto al año anterior. La mayor parte de estas inscripciones pertenece a Ayuntamientos, con poblaciones superiorese a 4.000 habitantes, a los que se les ha dedicado mayor atención, reiterándoles los requerimientos efectuados ya en años anteriores, con la intención de concienciar en el cumplimiento de las exigencias de la Ley.

En la Administración General del Estado, aún cuando no se puede asegurar la inscripción de la totalidad de sus ficheros automatizados de datos personales, sí parece encontrarse estabilizada, al haber declarado prácticamente todos sus ficheros en años anteriores. El incremento de ficheros en 1997, respecto a las cifras con que se finalizaba 1996, no supera el 3%. En cambio, ha alcanzando un crecimiento mayor, cercano al 9%, la Administración de Comunidades Autónomas, que ha continuado formalizando la inscripción de ficheros omitidos en su momento, contribuyendo a que este porcentaje sea mayor, el hecho de haberse practicado la inscripción durante 1997 de la totalidad de los ficheros de la Ciudad Autónoma de Melilla.

Aún ha sido más alto el incremento de la inscripción de ficheros de Universidades, que se deduce del 20,84% que ha crecido la inscripción de Otras Personas Jurídico-Públicas donde se engloban las Universidades. Este hecho se ha debido a la respuesta a los requerimientos efectuados desde la Agencia a este sector. Aunque respecto del total de las inscripciones solo representan el 1,61% de los ficheros de titularidad pública.

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 mas elevados se corresponden con los ficheros destinados a la gestión de procedimientos administrativos (28,34%), gestión de estadísticas internas (27,12%), gestión tributaria y de recaudación (22,61%), gestión económica con terceros (20,31%), seguidos de la gestión de la función estadística pública (17,81%), gestión del padrón (14,74%) y gestión de personal (14,28%), indicando que la mayor parte de ficheros pertenecientes a la Administración Pública y Organismos de titularidad pública corresponden a gestión administrativa. No obstante, si estudiamos la inscripción durante el año 1997, podemos observar un crecimiento considerable, del 15,76%, de la gestión de educación universitaria, consecuencia del requerimiento de la Agencia a las Universidades pendientes de inscripción, ya comentado anteriormente.

Respecto al número de ficheros conteniendo datos especialmente protegidos regulados en el artículo 7 de la Ley Orgánica 5/92, referidos a ideología, religión o creencias, inscritos en el Registro durante el año 1997, nos encontramos con cuatro nuevos ficheros de la Administración Local, destinados a recoger las relaciones de concejales y/o alcaldes, incluyendo el partido político al que pertenecen, y un quinto fichero, perteneciente al Instituto de Migración y Servicios Sociales, destinado a la gestión de refugiados y desplazados, en el que se recogen datos de ideología, además de salud necesarios para gestionar las estancias en los diferentes tipos de centros de atención a refugiados en función de su ideología y estado de salud.

Sigue siendo más elevado el número de ficheros conteniendo otros datos sensibles de salud, origen racial o vida sexual, que asciende en 1997 a 82, e indica la continuidad en la progresiva implantación del 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 para su implantación 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 paquete 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, pérfiles de usuarios, siempre tratando de mejorar la

adecuación de los recursos existentes a las necesidades y demandas planteadas por los ciudadanos.

3. 3. 2. OPERACIONES DE OFICIO

A pesar de la tarea de filtrado de la base de datos del Registro General de Protección de Datos, que se ha venido practicando desde su puesta en marcha, aún continúa siendo ésta una tarea importante, que origina un alto número de operaciones de oficio y concretamente, durante 1997, ha dado lugar a 2.457 modificaciones de ficheros de titularidad pública.

La distribución de estos movimientos a lo largo del año es uniforme, y es debida, como ya se señalaba en la memoria del anterior ejercicio, 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 observa una punta en el mes de abril, correspondiendo precisamente, con la publicación del Catálogo de Ficheros-1997, cerrada a 30 de abril. También coincide con este hecho y la revisión que se efectúa para intentar depurar al máximo la información de la base de datos del Registro, la supresión de once ficheros por encontrarse inscritos por duplicado. Estas duplicidades se originan cuando el responsable intenta modificar un fichero y en vez de enviar una notificación de modificación envía una nueva inscripción.

3. 3.2.1. Actuaciones relacionadas con la Administración General del Estado

La disposición general de creación o modificación de los ficheros automatizados de datos de carácter personal de la Administración General del Estado se publica en el Boletín Oficial del Estado, permitiendo realizar un seguimiento de su inscripción. Durante 1997 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, encontrándose todos ellos inscritos al finalizar el año:

- Resolución de 17 de diciembre de 1996, de la Comisión del Sistema Eléctrico Nacional, por la que se crean ficheros automatizados de datos de carácter personal, (BOE nº 27, de 31 de enero de 1997)

- Orden de 16 de septiembre de 1997, del Ministerio de Trabajo y Asuntos Sociales, por la que se crean, modifican y suprimen ficheros automatizados de datos de carácter personal del Ministerio, (BOE nº 231, de 26 de septiembre de 1997)

- Orden de 3 de julio de 1997, del Ministerio de Sanidad y Consumo, por la que se amplia la Orden de 21 de julio de 1994, creando el fichero con datos de carácter personal de gestión del Registro Nacional de Donantes de Gametos y Preembriones.

- Orden de 4 de julio de 1997, del Ministerio del Interior, por la que se crean ficheros automatizados con datos de carácter personal en la Delegación del Gobierno para el Plan Nacional sobre Drogas y en las Delegaciones del Gobierno en las Comunidades Autónomas, (BOE nº 167, de 14 de julio de 1997)

- Orden de 14 de marzo de 1997, del Ministerio de Presidencia, por la que se modifican y suprimen ficheros del anexo de la Orden de 26 de julio de 1994, que regula los ficheros automatizados de datos de carácter personal, (BOE nº 74, de 27 de marzo de 1997)

- Orden de 14 de marzo de 1997, del Ministerio de Presidencia, por la que se crean nuevos ficheros automatizados de datos de carácter personal, (BOE nº 74, de 27 de marzo de 1997)

El Consejo General del Poder Judicial publica en el Boletín Oficial del Estado nº 241, de 8 de octubre de 1997, el acuerdo de 28 de julio de 1997, por el que se regulan los ficheros de datos relativos a la solvencia patrimonial de personas incursas en procedimientos penales por delito existente en el Decanato de los Juzgados de Santander.

A los ficheros de los que son titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional no les es de aplicación lo dispuesto en los Títulos VI y VII de la Ley, que tratan de la Agencia de Protección de Datos e Infracciones y Sanciones, respectivamente, y por lo tanto no son objeto de inscripción en el Registro aunque sí están obligados a la publicación de la disposición general que habilite la creación del fichero.

3. 3.2.2. Actuaciones relacionadas con la Administración de las Comunidades Autónomas.

Durante el año 1997, se han continuado recibiendo contestaciones de las Comunidades Autónomas a los requerimientos efectuados anteriormente, como consecuencia de la revisión de oficio llevada a cabo desde la Agencia, con la finalidad de recordar a los órganos responsables de ficheros sus obligaciones en relación con la inscripción y en los que se indicaban:

- las discrepancias encontradas entre las disposiciones que regulan la existencia de los ficheros, publicadas en los diarios oficiales correspondientes y las notificaciones de inscripción declaradas al Registro,

- las disposiciones que regulan ficheros que habiéndose publicado en un boletín oficial, no se han notificado al Registro en cumplimiento de lo dispuesto en el artículo 5 del Real Decreto 1332/1994.

- También se solicitaba una revisión del encuadramiento del órgano responsable de cada fichero, dado el cambio de estructuras orgánicas que se han producido en la Comunidades Autónomas desde la creación de la Agencia de Protección de Datos.

Las Comunidades Autónomas que han mantenido mayor actividad en la actualización de la inscripción de sus ficheros en el Registro han sido las de Andalucía, País Vasco y Canarias. Además, la Ciudad Autónoma de Melilla ha realizado la inscripción en este año de los 59 ficheros de que dispone.

Durante el año 1997, las disposiciones de carácter general de creación, modificación o supresión de ficheros bajo responsabilidad de la Administración de Comunidades Autónomas, que han sido publicadas en los Diarios Oficiales respectivos, y que han sido notificados a la Agencia para su inscripción, han sido las que se relacionan a continuación:

- Decreto 189/1997, de 22 de julio, de la Consejería de Economía y Hacienda, por el que se crea el Registro de Licitadores de la Comunidad Autónoma de Andalucía, (BOJA nº 94, de 14 de agosto de 1997)

- Orden de 27 de febrero de 1997, de la Consejería de Salud de Andalucía, por la que se crean ficheros automatizados de datos de carácter personal de la Escuela Andaluza de Salud Pública, (BOJA nº 35, de 22 de marzo de 1997). De esta disposición aún están pendientes de inscripción 9 ficheros.

- Orden de 23 de abril de 1997, de la Consejería de Salud de Andalucía, por la que se modifican las de 6 de marzo de 1996, que crean y modifican ficheros automatizados de datos de carácter personal gestionados por esta Consejería, (BOJA nº 55, de 13 de mayo de 1997)

- Corrección de errores al Decreto 167/1994, de 18 de julio, del Departamento de Presidencia y Relaciones Institucionales de la Diputación General de Aragón, de regulación de los ficheros automatizados de datos de carácter personal de la Administración de la Comunidad Autónoma de Aragón, (BOA nº 7, de 20 de enero de 1997)

- Resolución de 31 de octubre de 1997, de la Consejería de Economía, del Principado de Asturias, por la que se regulan los ficheros automatizados de la Consejería sobre datos de carácter personal destinados a la gestión del sistema tributario, (BOPA nº 262, de 12 de noviembre de 1997)

- Resolución de 31 de octubre de 1997, de la Consejería de Economía del Principado de Asturias, por la que se regulan los ficheros automatizados de dicha Consejería sobre datos de carácter personal, excluidos los de gestión del sistema tributario, (BOPA nº 262, de 12 de noviembre de 1997)

- Resolución de 3 de diciembre de 1997, de rectificación de error en la Resolución de 31 de octubre de 1997 de la Consejería de Economía del Principado de Asturias, por la que se regulan sus ficheros automatizados sobre datos de carácter personal destinados a la gestión del sistema tributario, (BOPA nº 293, de 20 de diciembre de 1997)

- Corrección de la Resolución de 31 de octubre de 1997, por la que se regulan los ficheros automatizados de la Consejería de Economía del Principado de Asturias, sobre datos de carácter personal excluidos los de gestión del sistema tributario, (BOPA nº 274, de 26 de noviembre de 1997)

- Orden de 16 de julio de 1997, de la Consejería de Empleo y Asuntos Sociales de Canarias, por la que se crean y regulan los ficheros de tratamiento automatizado de datos de carácter personal en materia de intermediación en el mercado de trabajo de la Agencia Canaria de Empleo, (BOC nº 117, de 8 de septiembre de 1997). Esta disposición al cierre del ejercicio 1997 aún no había sido notificada.

- Orden de 4 de febrero de 1997, de la Consejería de Economía y Administraciones Públicas, por la que se crea el fichero automatizado de datos de carácter personal de Altos Cargos, Delegados Provinciales y Personal Eventual dela Junta de Comunidades de Castilla-La Mancha, (DOCM nº 7, de 14 de febrero de 1997)

- Orden de 4 de marzo de 1997, de la Consejería de Pesca, Marisqueo y Acuicultura de la Junta de Galicia, por la que se regulan los ficheros automatizados de datos de carácter personal de nueva creación en la Consejería de Pesca, Marisqueo y Acuicultura, (DOGA nº 54, de 19 de marzo de 1997)

- Decreto 133/97 de la Consejería de la Presidencia de la Comunidad de Madrid, de 16 de octubre, de creación de nuevos ficheros de datos de carácter personal y de adaptación de las normas reguladoras de los ficheros existentes que contienen datos de carácter personal a las determinaciones de la Ley 13/95, de 21 de abril, de Regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid (BOCAM nº 259, de 31 de octubre de 1997).

- Orden de la Consejería de Presidencia de 14 de julio de 1997, por la que se crea la Base de Datos de profesorado colaborador de la Escuela de la Policía Local de la Región de Murcia, experto en Áreas y Materias relativas a la Seguridad Pública y se hacen públicas las bases de los concursos de méritos para la selección del personal que integrará la Base de Datos, (BORM nº 171, de 26 de julio de 1997)

- Orden Foral de 17 de febrero de 1997, del Consejero de Agricultura, Ganadería y Alimentación de Navarra, por la que

se modifica la unidad responsable de los ficheros automatizados dependientes del Departamento de Agricultura, Ganadería y Alimentación, (BON nº 27, de 03 de marzo de 1997)

- Orden Foral 14/1997, de 27 de enero, del Consejero de Economía y Hacienda de Navarra, por la que se introducen diversas modificaciones en el Decreto Foral 143/1994, de 26 de julio, por el que se regulan los ficheros informatizados con datos de carácter personal, dependientes de los órganos de la Administración de la Comunidad Foral y de sus Organismos Autónomos, (BON nº 17, de 07 de febrero de 1997)

- Orden Foral 4/1997, de 23 de enero, del Consejero de Presidencia e Interior, por la que se modifican características de ficheros informatizados del Instituto Navarro de Administración Pública, (BON nº 21, de 17 de febrero de 1997)

- Orden Foral 57/1997, de 21 de mayo, del Consejero de Presidencia e Interior de Navarra, por la que se modifican los ficheros informatizados, con datos de carácter personal denominados Asociaciones e Indemnización por daños ocasionados por atentados terroristas, y se crea el fichero Fundaciones, (BON nº 67, de 04 de junio de 1997)

- Orden de 20 de marzo de 1997, de la Consejera de Cultura del Gobierno Vasco, de modificación de la Orden de 5 de octubre de 1995, por la que se relacionan y regulan los ficheros automatizados con datos de carácter personal gestionados por el Departamento de Cultura y Organismos Autónomos adscritos al mismo, (BOPV nº 62, de 03 de abril de 1997)

- Orden de 8 de octubre de 1997, del Consejero de Educación, Universidades e Investigación del Gobierno Vasco, por la que se modifica la de 24 de septiembre de 1996, que regula los ficheros automatizados con datos de carácter personal del Departamento de Educación, Universidades e Investigación, (BOPV nº 206, de 28 de octubre de 1997)

- Orden de 17 de noviembre de 1997, del Vicepresidente del Gobierno Vasco y Consejero de Hacienda y Administración Pública, por la que se regulan los ficheros automatizados de datos de carácter personal de la Vicepresidencia del Gobierno del Departamento de Hacienda y Administración Pública y los Organismos Autónomos adscritos al mismo, (BOPV nº 239, de 15 de diciembre de 1997)

Por otra parte, y respecto al requerimiento efectuado a aquellas Comunidades Autónomas que teniendo transferidas las competencias en materia de sanidad, no habían notificado la existencia de ficheros de gestión sanitaria a la Agencia de Protección de Datos al finalizar el año 1996, no había cumplido con lo solicitado la Comunidad de Canarias. Durante 1997, tampoco se ha notificado a efectos de inscripción la notificación de estos ficheros, habiendo dado traslado a la Inspección de Datos a los efectos oportunos.

3. 3.2.3. Actuaciones relacionadas con Administración Local

La inscripción en el Registro de los ficheros automatizados pertenecientes a las Entidades de la Administración Local ha superado, en 1997, el 70% de las altas registrales de ficheros de titularidad pública.

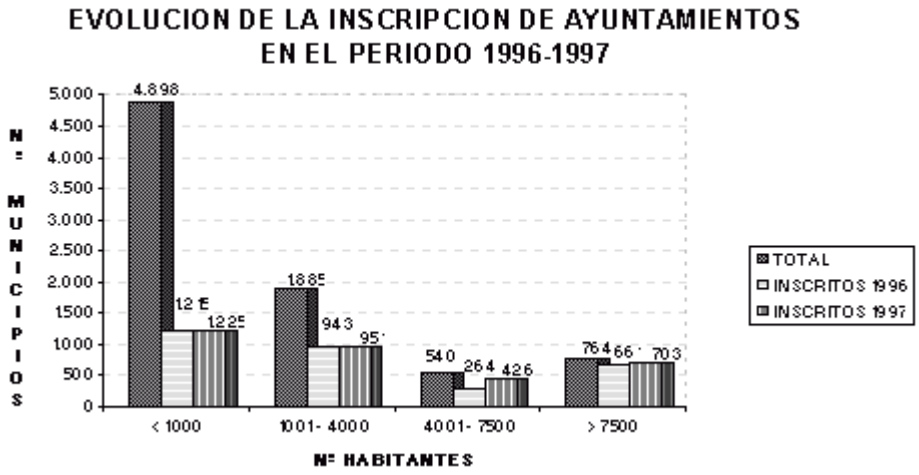
No obstante, pese a este volumen de operaciones que, al finalizar 1997, supone se encuentren inscritos 22.370 nuevos ficheros de Administración Local, continúa siendo el sector en el que podemos encontrar un número más alto de organismos que no ha notificado sus ficheros, según dispone el artículo 5 del Real Decreto 1332/1994, y no se tiene constancia de que haya cumplido la exigencia del artículo 18.2 de la Ley, publicando en el diario oficial correspondiente la disposición general de creación de sus ficheros.

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 a continuación, en función del número de habitantes de sus municipios.

HABITANTES	MUNICIPIOS	INSCRITOS	POR INSCRIBIR	% PENDIENTES
< 1000	4.898	1.225	3.673	74,99
1001 - 4000	1.885	951	934	49,55
4001 - 7500	540	426	114	21,11
>7500	764	703	61	7,98
Total	8.087	3.305	4.782	59,13

Durante el año 1997 se ha continuado requeriendo a los responsables de los Ayuntamientos con una población superior a los 4.000 habitantes, para recordar sus obligaciones en relación con la notificación e inscripción de los ficheros de datos de carácter personal que existieran en sus Ayuntamientos.

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



En el sector de municipios con población comprendida en el tramo de 4.000 a 7.500 habitantes, los requerimientos solicitando la inscripción de ficheros se iniciaron a finales de 1995, y aunque no se ha conseguido la inscripción total de estos Organismos, se puede apreciar un fuerte incremento en este último año, en el que, además de reiterar con una nueva notificación, la falta de inscripción, se ha incidido más en la concienciación en el tema que nos ocupa, la protección de datos, de una forma más personalizada a través de conversaciones telefónicas, envío de información aclarando los extremos necesarios para la tramitación del procedimiento de inscripción, así como los modelos de notificación de ficheros de titularidad pública, entre otros documentos.

Asimismo, ha disminuido el número de Ayuntamientos pendientes de inscripción con población superior a 7.500 habitantes, para los que además de dar traslado a Inspección de Datos, se ha empleado la misma táctica, más dirigida a concienciar a los responsables acerca de las exigencias de la Ley Orgánica y las repercusiones que puede ocasionar su incumplimiento. Es de resaltar, en este apartado, por tratarse de la única capital de provincia, que no ha notificado sus ficheros a efectos de inscripción, el Ayuntamiento de Ourense.

Ha contribuido a facilitar la información necesaria para llevar a cabo la inscripción, la puesta en Internet de la web de la Agencia de Protección de Datos, donde el responsable es informado al respecto y encuentra la documentación necesaria.

Para poblaciones inferiores a 4.000 habitantes la inscripción de nuevos Ayuntamientos ha sido mínima en 1997, debido, por una parte, a no haber sido requeridos desde la Agencia, pues sería deseable conseguir previamente la inscripción de los Ayuntamientos de mayor población, y por otra, íntimamente relacionada con la anterior, debido a su tamaño, los medios técnicos de que disponen son ínfimos, y en muchos casos, probablemente carezcan de ellos. No obstante, se espera que en el próximo año se vea incrementado el número de inscripciones, debido a la colaboración de las Diputaciones Provinciales entre ellas con una mención aparte por su estimable colaboración la Diputación de Barcelona.

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 dice: *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 Ministerio de la Presidencia, ha establecido el procedimiento de tramitación del padrón municipal.

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, aprueba 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, 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, 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.

Este Convenio del año 1997, ya ha sido formalizado por la Diputación de Barcelona, con 68 Ayuntamientos de la provincia, publicados en el Boletín Oficial de la Provincia de Barcelona nº 274 y 304, de 15 de noviembre y 20 de diciembre de 1997, respectivamente, que han aceptado por tanto, la encomienda de 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. Dadas las fechas de publicación coincidentes con el cierre del ejercicio, la notificación de las mismas se ha procedido a realizar a comienzos de 1998.

** Policía Local*

Otra actuación llevada a cabo desde el Registro en el ámbito de la Administración local ha estado en relación con las actividades efectuadas en una muestra de Ayuntamientos seleccionados por la Inspección de Datos, sobre ficheros que preveían como fines y usos, la gestión policial. De las inspecciones realizadas, se recibió información en el tercer trimestre de 1997, de la existencia de ficheros no inscritos en el Registro de los Ayuntamientos de Barcelona, Bilbao, Marbella, Murcia, Sevilla, Valladolid, Vigo y Zaragoza.

Como consecuencia de dicha comunicación se procedió a requerir en el mes de Septiembre, a los Ayuntamientos anteriormente mencionados para que efectuasen la inscripción de estos ficheros. Al finalizar el ejercicio, Sevilla ya había inscrito parte de los ficheros localizados, y Barcelona, Bilbao, Valladolid, Vigo y Zaragoza han contestado al requerimiento indicando que se encontraban tramitando la disposición de creación de los ficheros. Se espera que a comienzos del año 1998 estos Ayuntamientos hayan realizado la inscripción, así como el Ayuntamiento de Marbella, que esperamos también se encuentre tramitando la correspondiente disposición, aunque no haya contestado formalmente. De no hacerlo así, se devolverá el asunto a la Inspección de Datos, para que adopte las medidas que considere convenientes.

3. 3.2.4. Actuaciones relacionadas con Universidades

Al comenzar el año 1997 continuaban 17 Universidades públicas, sin inscribir sus ficheros en el Registro, tras el requerimiento efectuado en el año 1996. Durante este año, se ha realizado un seguimiento, a través del Boletín Oficial del Estado, dónde se encuentran la mayor parte de las disposiciones generales de regulación de ficheros de Universidades, y dónde, a lo largo del año 1997, se han publicado las siguientes:

- Resolución de 5 de junio de 1997, del Rectorado de la Universidad de Las Palmas de Gran Canaria, por la que se regula los ficheros automatizados de datos de carácter personal (BOE nº 159, de 4 de julio de 1997)

- Resolución de 7 de octubre de 1996, del Rectorado de la Universidad Autónoma de Barcelona, por la que se regulan los ficheros automatizados de datos de carácter personal, correspondientes al personal de administración y servicios, al personal docente e investigador y a los alumnos, (BOE nº 148, de 21 de junio de 1997)

- Resolución de 31 de marzo de 1997, del Rectorado de la Universidad de Granada, por la que se regulan los ficheros de tratamiento automatizado de datos de carácter personal, (BOE nº 93, de 18 de abril de 1997)

- Resolución de 5 de febrero de 1997, del Rectorado de la Universidad de Burgos, por la que se regulan los ficheros automatizados de datos de carácter personal de la Universidad, (BOE nº 49, de 26 de febrero de 1997)

- Resolución de 3 de febrero de 1997, de la Presidencia de la Comisión Gestora de la Universidad de Jaén, reguladora de los ficheros automatizados de datos de carácter personal, (BOE nº 49, de 26 de febrero de 1997)

- Resolución de 11 de febrero de 1997, del Rectorado de la Universidad de La Rioja, reguladora de los ficheros automatizados de datos de carácter personal, (BOE nº 43, de 19 de febrero de 1997)

- Resolución de 9 de septiembre de 1997, del Rectorado de la Universidad de Zaragoza, por la que se modifica la Resolución de 27 de julio de 1994, que regula los ficheros de tratamiento automatizado de datos de carácter personal (BOE nº 243, de 10 de octubre de 1997)

Todos los ficheros publicados en estas resoluciones han quedado inscritos al finalizar 1997, quedando por inscribir los ficheros de las Universidades de Huelva y de La Coruña, si bien, se espera queden inscritos en el primer trimestre de 1998, al encontrarse bastante avanzado el trámite de publicación de la disposición general de regulación de los ficheros. De esta forma se daría por concluido el estudio iniciado en 1996, y quedaría pendiente iniciar un nuevo análisis, pues se está produciendo la creación de nuevas Universidades, tanto públicas como privadas.

3. 3.2.5. Otras actividades

* Requerimientos de nuevas inscripciones

Se continua la tarea iniciada en 1996, de análisis de la legislación reciente por la que se regulan determinados Registros o Bases de Datos a nivel nacional, que claramente se encuentran dentro del ámbito de aplicación de la Ley, por contener datos de carácter personal, y por la que se determina la utilización de medios informáticos, y las cesiones de datos a realizar. Nos dirigimos a cada órgano competente de la Administración responsable de estos ficheros solicitándoles información acerca de su puesta en marcha y las actuaciones seguidas a efectos de la notificación de los mismos a la Agencia.

En este sentido, se requirió al Ministerio de Sanidad y Consumo, para que procediera a publicar la disposición de creación del ficheros, en relación a la creación y organización del del Registro Nacional Informatizado de Donantes de Gametos y Preembriones con fines de reproducción humana. En fecha 15 de julio de 1997, se dictó la Orden de creación del fichero, quedando inscrito en el Registro General de Protección de Datos, con fecha 5 de noviembre.

Por otra parte, se dirigió un requerimiento a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, en relación con la Ley 19/1993, de Medidas de Prevención del Blanqueo de Capitales y normas que la desarrollan, para que procedieran a publicar la disposición de creación del fichero resultante del tratamiento automatizado de datos de carácter personal. La Comisión Ejecutiva dictó la Resolución de regulación, que se publicó en el Boletín Oficial del Estado nº 153 de 27 de junio de 1997, por la que se hacen públicos los ficheros con datos de carácter personal bajo responsabilidad de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias gestionados por el Servicio Ejecutivo de la misma, inscribiéndose los ficheros con fecha 15 de julio de 1997.

* Delegaciones y Subdelegaciones del Gobierno.

Durante 1997, ha sido objeto de estudio por parte del Registro, la nueva organización de Delegaciones y Subdelegaciones del Gobierno.

Por una parte, la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE), modifica y reforma la estructura y competencias de las Delegaciones y Subdelegaciones del Gobierno (que asumen entre otras las competencias de los anteriores Gobiernos Civiles) y cambia la adscripción orgánica de las Delegaciones del Gobierno.

Posteriormente, se modifican las estructuras orgánicas básicas de los Ministerios de Administraciones Públicas y del Interior, afectando a la denominación de los responsables de los ficheros inscritos por el Ministerio del Interior correspondientes a Delegaciones del Gobierno y Gobiernos Civiles.

- En primer lugar, desaparecen las unidades responsables con denominación "Gobierno Civil", que pasan a llamarse "Subdelegaciones de Gobierno"

- Por otra parte, queda sin determinar en que Ministerio se encuadran los responsables de ficheros de estos Centros Directivos, al depender orgánicamente del Ministerio de Administraciones Públicas, y funcionalmente, en algunas ocasiones, de Interior, surgiendo la duda sobre qué dependencia determina la responsabilidad de un fichero, la funcional o la orgánica.

Con este planteamiento nos dirigimos a la Subsecretaría de Interior, estando pendientes de su resolución para adecuar, a la nueva estructura, la inscripción de estos ficheros en el Registro General de Protección de Datos.

3. 4. FICHEROS DE TITULARIDAD PRIVADA

3. 4.1. EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN

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

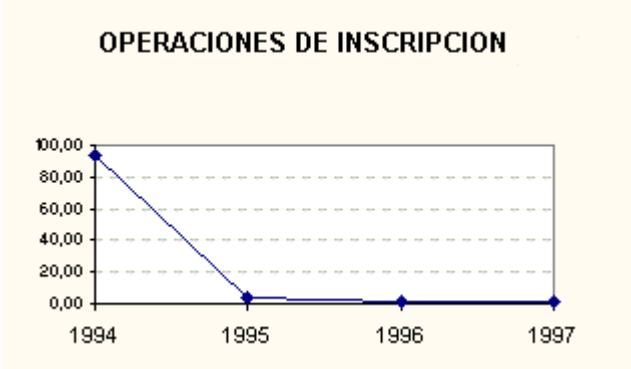
Los trabajos referentes a los movimientos en los asientos registrales constituyen el núcleo de la actividad diaria del Registro. Pueden distinguirse tres grandes apartados, los movimientos de inscirpción de ficheros, los de modificación de la inscripción y los de supresión.

3. 4.1.1. Inscripción de ficheros

** Cifras generales.*

A lo largo de 1997 se han tramitado 1.789 operaciones de alta de ficheros de titularidad privada, permaneciendo inscritos al final del ejercicio 1.760 ficheros, lo que supone solamente un 0,87% de las 201.835 inscripciones que constituyen, al cierre del año, la cifra total de ficheros privados inscritos en el Registro. Si contrastamos la cifra de operaciones de alta de ficheros privados de 1997 con las 2.408 altas de 1996, las 8.275 de 1995 y las 200.908 de 1994, se observa la tendencia decreciente de este tipo de operaciones. Estos resultados son lógicos porque el mayor número de ficheros se inscribió en el proceso masivo inicial que comprendió la inscripción del año 1994 y que también influyó en parte en la inscripción de 1995. Es de preveer que en años venideros las cifras de inscripción se sitúen en valores uniformes estabilizándose en cifras similares a las actuales.

El gráfico que se presenta a continuación muestra la evolución de la inscripción en porcentaje a lo largo de los años.



Por otra parte, el número de empresas que ha inscrito ficheros en 1997 es de 901, lo que supone una media de inscripción de prácticamente dos ficheros por empresa, cifra que coincide con la relativa a 1996 y 1994 y que supera ligeramente a la del año 1995 (1,5 ficheros por empresa).

** Modelo de notificación.*

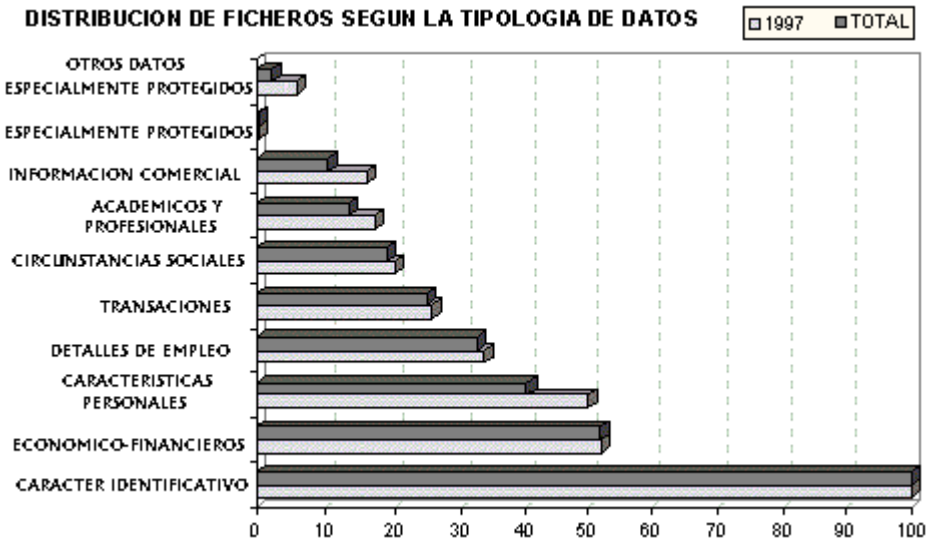
Es de resaltar que el 57,6% de las operaciones de alta de ficheros privados del 97 se ha notificado en soporte magnético, con lo que la tendencia a utilizar este tipo de modelo sigue siendo superior al cuestionario en soporte papel, al igual que en años anteriores (en 1996 el porcentaje de operaciones de alta por disquete fue del 53,6%, en 1995 fue del 76,2% y en 1994 fue del 56,1%).

** Tipos de datos.*

En cuanto a la tipología de datos declarados en los ficheros privados inscritos en el ejercicio del 97, aparte de los datos de carácter identificativo que aparecen lógicamente en el 100% de la inscripción, predominan los datos económico-financieros (51,7% de la inscripción) y los de características personales (50%), seguidos de los datos de detalles de empleo (32,5%), los de transacciones (26,2%), los de circunstancias sociales (20%), los académicos y profesionales (17,6%) y los de información comercial (16,6%). En una escala bastante más inferior se encuentran otros datos especialmente protegidos con un 6,4% y datos especialmente protegidos con un 0,17%. Es de destacar el predominio de las notificaciones que declaran datos económico-financieros, de características personales y de detalles de empleo. Estas cifras presentan un grado de similitud elevado con las referentes a los años anteriores, lo que indica que el tipo de datos que contienen los ficheros privados que se inscriben en los diferentes años se mantiene prácticamente constante a lo largo de tiempo.

Si los datos sobre tipología se calculan referidos al total de la inscripción en vez de a la inscripción del año 1997, se obtienen resultados similares (51,5% con datos económico financieros, 40,1% con datos de características personales, 31,7% con datos de características de empleo, 25,6% con datos de transaciones, 19% con datos de información comercial, 12,7% con datos académicos y profesionales, 10,2% con datos de circunstancias sociales, 1,7% con otros datos especialmente protegidos y 0,15% con datos especialmente protegidos). Se observa que estas cifras coinciden con las referentes al año anterior, lo que corrobora que la tipología de datos que declaran los responsables de ficheros privados se mantiene prácticamente constante a lo largo del tiempo.

En la gráfica siguiente se comparan estas cifras totales con las relativas al año 1997 observándose una tendencia similar, excepto en otros datos especialmente protegidos, que constituyen una cifra prácticamente despreciable respecto de la inscripción total y que aún no han sido objeto de un proceso de depuración intensivo similar al llevado a cabo con los datos especialmente protegidos.



** Datos especialmente protegidos.*

Se observa que en cuanto a la inscripción de ficheros con datos especialmente protegidos relativos al artículo 7 de la Ley 5/1992, las cifras del año 1997 pueden considerarse poco significativas respecto de las cifras de inscripción del año. Lo mismo ocurre con la cifra total de ficheros inscritos con este tipo de datos respecto de la cifra total de ficheros inscritos en el Registro General de Protección de Datos.

Respecto a los datos especialmente protegidos relativos al apartado 1 del artículo 7 (ideología, religión o creencias), se han inscrito dos ficheros con datos de ideología y un único fichero con datos de religión. El fichero con datos de religión corresponde a una empresa del sector de actividad de agencias matrimoniales. Los ficheros que declaran datos de ideología son los que contienen datos relativos a la afiliación sindical de los empleados, esta información se recoge y gestiona según lo dispuesto en el artículo 11 de la Ley Orgánica 11/1985 de 2 de Agosto, de Libertad Sindical, con el consentimiento del afectado y con el fin específico de la recaudación de cuotas de los afiliados por pertenencia a un sindicato y control de horario de trabajo con fines sindicales.

En relación a los datos de salud, origen racial y vida sexual recogidos en el artículo 7.3 de la Ley, se han inscrito 113 ficheros consignando datos de salud en todos ellos. Estos ficheros con datos de salud corresponden a entidades del sector asegurador que ofrecen seguros de vida y salud o que gestinan pólizas de asistencia sanitaria o decesos. También incluyen a las entidades de diagnóstico y centros médicos de empresas que ofrecen este tipo de servicios a sus trabajadores. Por otra parte, responsables del sector de la medicina, como hospitales, clínicas y médicos particula - res también reflejan datos de salud en sus ficheros de historiales clínicos, seguimiento de pacientes y proyectos de investigación. Otras entidades que declaran ficheros con datos de salud son los laboratorios químicos, farmacéuticos y ópticos que necesitan tratar este tipo de datos con la finalidad de realizar ensayos clínicos. También se contemplan datos de salud en ficheros de asociaciones y entidades cuya actividad es la prestación de servicios sociales. No existen ficheros notificados en 1997 que declaren datos de origen racial ni de vida sexual.

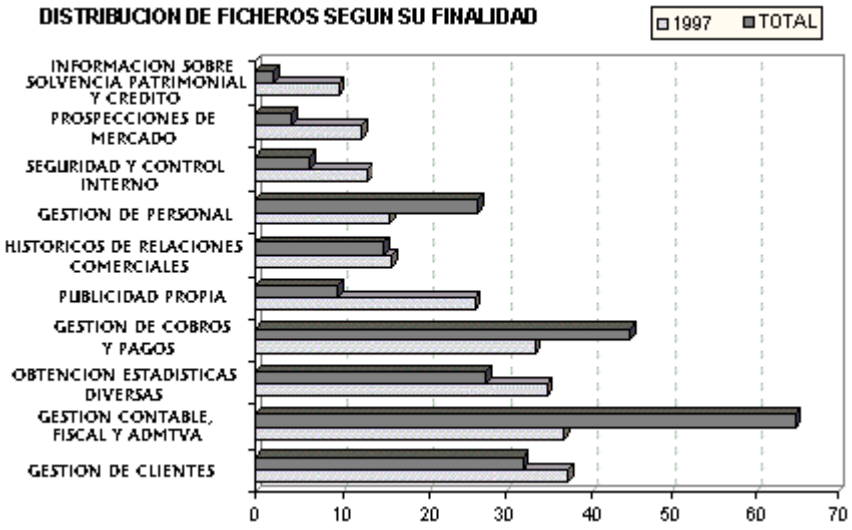
Según imperativo legal todos los datos especialmente protegidos de ideología, creencias y religión, se declaran con consentimiento expreso y por escrito del afectado. Con otros datos especialmente protegidos (origen racial, salud y vida sexual), prácticamente la totalidad de los responsables declaran el consentimiento expreso del afectado, salvo en porcentaje insignificante que declaran datos de salud amparándose en la Ley General de Sanidad.

** Finalidades y usos*

En cuanto a las finalidades y usos de los ficheros inscritos en 1997 destacan la gestión de clientes (36,4%), la gestión contable fiscal y administrativa (36,1%), obtención de estadísticas diversas (34,5%), gestión de cobros y pagos (32,7%), publicidad propia (25,9%), históricos de relaciones comerciales (16,6%), gestión de personal (16,3%), seguridad y control interno (12,3%), prospecciones de mercado (11,8%), información sobre la solvencia patrimonial y el crédito (9, 7%), encuestas de opinión (8,3%), publicidad para terceros (7%), asesorías, auditorías y servicios relacionados (6%), seguros de vida y salud (5%), otro tipo de seguros (4,4%), selección de personal (4,3%), gestión de tarjetas de crédito y similares (3,8%) cuentas de crédito (3,6%), prestaciones sociales (3,5%), cuentas de depósito (3,2%) y gestión y control sanitario (2,9%) . Estas cifras ponen de manifiesto el predominio de los ficheros cuya finalidad declarada es la gestión de clientes, contabilidad, fiscalidad, gestión de personal y nóminas, cifras lógicas ya que la mayoría de las empresas dispone de este tipo de información mecanizada o contrata la automatización de la misma. En líneas generales se mantiene la distribución de la inscripción por finalidades respecto del año anterior, con un ligero aumento de declara -

ción de ficheros con finalidad de gestión de clientes, seguridad y control interno, información sobre la solvencia patrimonial y el crédito, publicidad para terceros y asesorías y servicios relacionados. Alternativamente, se produce un descenso de inscripción de ficheros con finalidades de gestión contable, fiscal y administrativa, gestión de cobros y pagos y encuestas de opinión.

En cuanto a las finalidades y usos referidos al total de la inscripción predomina la gestión contable, fiscal y administrativa (66%), la gestión de cobros y pagos (43,5)%, la gestión de clientes (31,6%), la obtención de estadísticas diversas (26,9%), la gestión de personal (26,2%), históricos de relaciones comerciales (15,8%), publicidad propia (9,5%), prestaciones sociales (6,8%), asesorías y servicios relacionados (6,6%), seguridad y control interno (4,9%), prospecciones de mercado (3,3%), otro tipo de seguros (2,7%), seguros de vida y salud (2,6%) y cuentas de crédito (2,1%). En líneas generales la inscripción por finalidades durante el año 1997 no se desvía significativamente de la inscripción por finalidades total en la base de datos, salvo para aquéllas rúbricas que han sido objeto de un seguimiento o requerimientos por su pertenencia a un sector determinado, como en el caso de los ficheros con finalidad de prestación de servicios de información sobre solvencia patrimonial y crédito y ficheros con la finalidad de controlar el acceso a los edificios, ambos encuadrados en las Instrucciones 1/1995 y 1/1996 del Director de la Agencia. El gráfico siguiente contrasta las cifras de 1997 y totales relativas a finalidad.



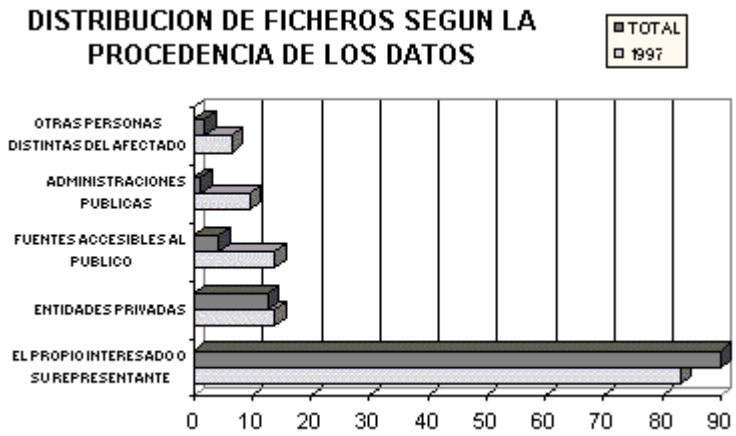
** Origen y procedencia de los datos*

En cuanto a la procedencia de los datos declarados en los ficheros inscritos en 1997, destacan aquellos que declaran el origen de sus datos del propio interesado o su representante legal (83,1% de los ficheros declarados), seguido de aquellos que declaran el origen de entidades privadas (14%), fuentes accesibles al público (14%), administraciones públicas (9,6 %) y otras personas distintas del afectado o su representante legal (6,5%).

En la mayoría de los casos es el propio interesado el que aporta voluntariamente la información, lo cual concuerda con la elevada cifra de ficheros inscritos cuya finalidad declarada es el uso en 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 no resulta demasiado fiable, debido a la dificultad de interpretación de este concepto por parte de los declarantes, produciéndose confusión con fuentes accesibles al público. Evidentemente, la misma dificultad de interpretación existe con el concepto de fuente accesible al público pero en menor grado, por lo que la cifra referente a este apartado es más fiable que la de administraciones públicas.

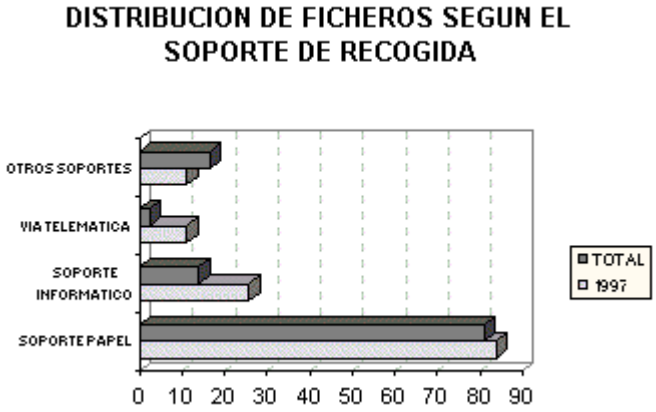
Estos datos concuerdan con las referentes a la inscripción total (89,9% de ficheros cuya procedencia es el propio interesado o su representante legal, 12,7% procedentes de entidades privadas, 4,3% procedentes de fuentes accesibles al público, 2% procedentes de otras personas distintas del afectado o su representante y 1,2% procedente de las Administraciones Públicas. El gráfico siguiente presenta las cifras de inscripción total por procedencia y las compara con las relativas al año 1997. Se observa un aumento significativo de procedencia de los datos de fuentes accesibles al público, de Administraciones Públicas y de otras personas distintas del afectado, originado posiblemente por la utilización creciente de la red Internet y la proliferación de páginas web tanto de organismos públicos como de entidades privadas cuya información alimenta todo tipo de ficheros.



** Soporte utilizado en la recogida de los datos*

En cuanto al soporte de recogida de los datos declarados en los ficheros inscritos en 1997 predomina el soporte papel (83,8% de los ficheros inscritos), seguido con apreciable diferencia por el soporte informático magnético (25,6%), la vía telemática y otros soportes (11%). Estas cifras están en línea con los párrafos anteriores, ya que los datos de los ficheros de contabilidad, fiscalidad, gestión de personal y nóminas, que son los predominantes, suelen recogerse inicialmente a través de formularios en papel.

Si consideramos la inscripción por tipo de soporte de recogida de datos referida al total de la inscripción (81% en soporte papel, 14% en soporte magnético, 16,6% en otros soportes y 2,5% por vía telemática) y se compara con la inscripción relativa al año 1997 destaca el aumento de las nuevas tecnologías en la recogida del dato, 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 de procedencia de los datos.



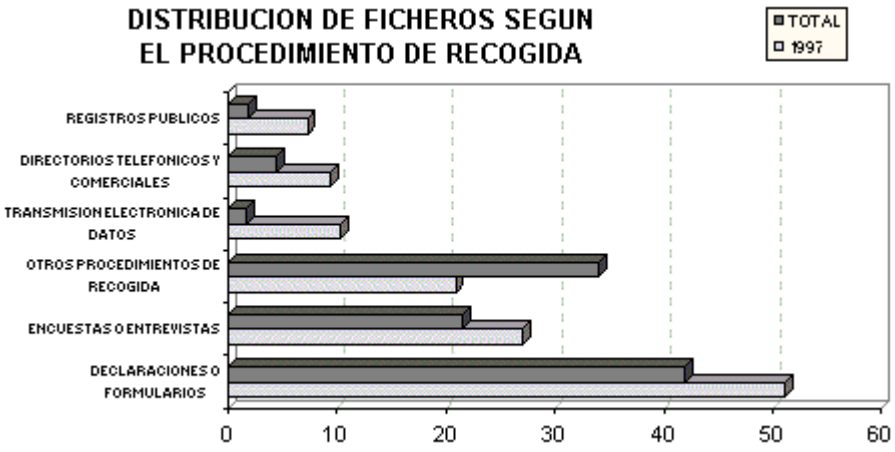
** Procedimiento de recogida.*

En cuanto al procedimiento de recogida de los datos de los ficheros inscritos en 1997 predominan declaraciones o formularios (51,2%) seguido de encuestas o entrevistas (27,1%) otros procedimientos de recogida (20,9%), transmisión electrónica de datos (10,3%), directorios telefónicos y comerciales (9,4%) y registros públicos (7,3%). Estas cifras concuerdan 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 recogidos del 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. Al comparar con las cifras de procedimiento de recogida del año anterior se observa un nivel de concordancia elevado, lo que indica un asentamiento en la tendencia de la cifras relativas al procedimiento de recogida.

Este procedimiento, engloba distintas formas de obtención de información que no se recogen normalizados expresa-

mente en el formulario 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 curriculums, encuestas telefónicas, fax, sistemas audiotext, etc.

Al considerar los datos de procedimiento de recogida referidos a la inscripción total (42% del total de ficheros con información procedente de declaraciones o formularios, 34,1% de otros procedimientos de recogida, 21,6% de encuestas o entrevistas, 4,5% de directorios telefónicos, comerciales, catálogos y memorias, 1,9% de registros públicos y 1,7% de transmisión electrónica de datos y compararlos con los relativos a 1997, se observa un aumento de recogida de datos de registros públicos, directorios telefónicos y comerciales y por transmisión electrónica de datos, lo que viene motivado en parte por la fuerte irrupción de las nuevas tecnologías de la información y la comunicación. Estos datos están en línea con las cifras de los apartados anteriores y se presentan en la gráfica siguiente.



** Cesiones de datos.*

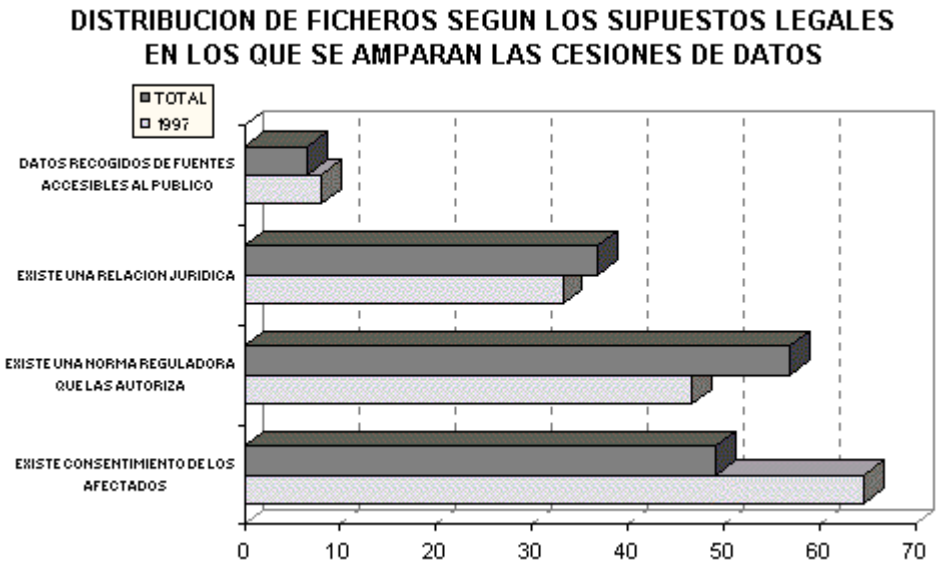
En cuanto a las cesiones de datos, en 1997 se han inscrito 467 ficheros que contemplan este apartado, lo que supone un 26,5% del dato total de ficheros inscritos en el ejercicio. Este porcentaje es similar al del ejercicio anterior (26%). El mayor porcentaje de cesiones se justifican por la existencia del consentimiento de los afectados (64,7% del total de ficheros inscritos con cesiones en el ejercicio), seguido por la existencia de una norma reguladora que las autoriza (46, 7%), la existencia de una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros (33,2%) y los que realizan la cesión amparándose en que los datos cedidos fueron recogidos de fuentes accesibles al público (8,1%).

El consentimiento de los afectados como justificación de la cesión se refleja en ficheros de gestión de clientes, históricos de relaciones comerciales y publicidad. La inscripción de ficheros que justifican las cesiones por la existencia de una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros está en cosonancia con la inscripción de ficheros que declaran como finalidad 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 corresponde con el uso para servicios de marketing, envios de publicidad, prospección de mercados y fines relacionados con este sector de actividad.

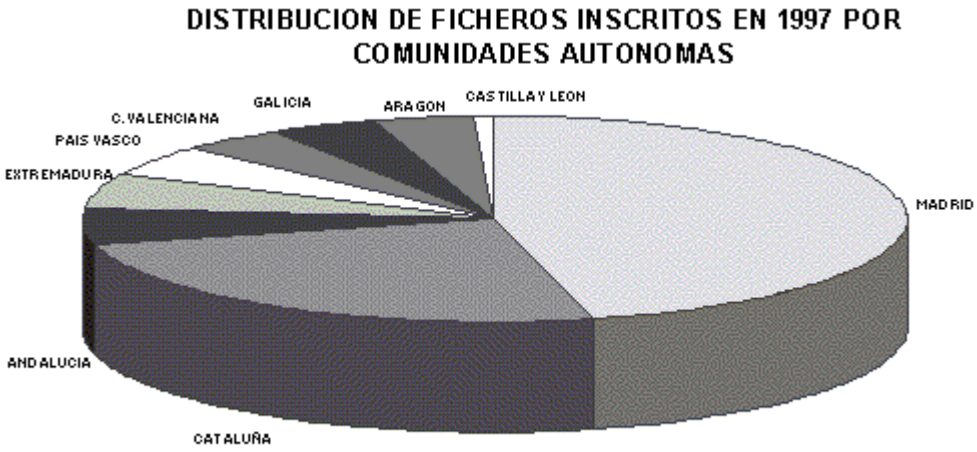
En cuanto a las cifras de inscripción total relativas a los supuestos legales en los que se amparan las cesiones de datos, actualmente el 57% del total de ficheros inscritos con cesiones las justifican por la existencia de una norma reguladora que las autoriza, el 49,2% se basan en el consentimiento de los afectados, el 36,9% las justifican por la existencia de una relación jurídica para conectar el fichero con ficheros de terceros y el 6,6% se basan en la recogida de datos de fuentes accesibles al público.

El gráfico siguiente compara los datos sobre cesiones para la inscripción total y para la inscripción del año 1997 según los supuestos legales en los que se amparan. En este gráfico se observa un aumento leve de cesiones justificadas en fuentes accesibles al público durante el año 1997, lo que está en consonancia con el aumento de la inscripción de ficheros con esta finalidad durante ese año.

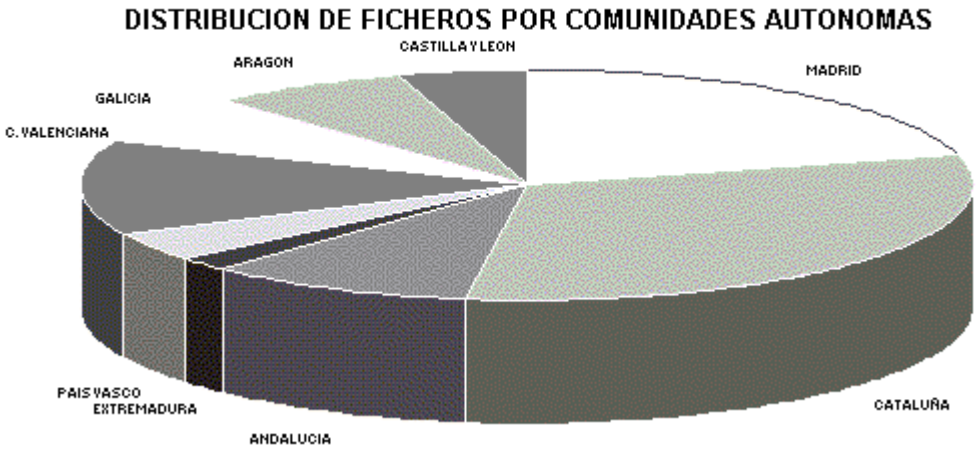


** Inscripción por Comunidades Autónomas.*

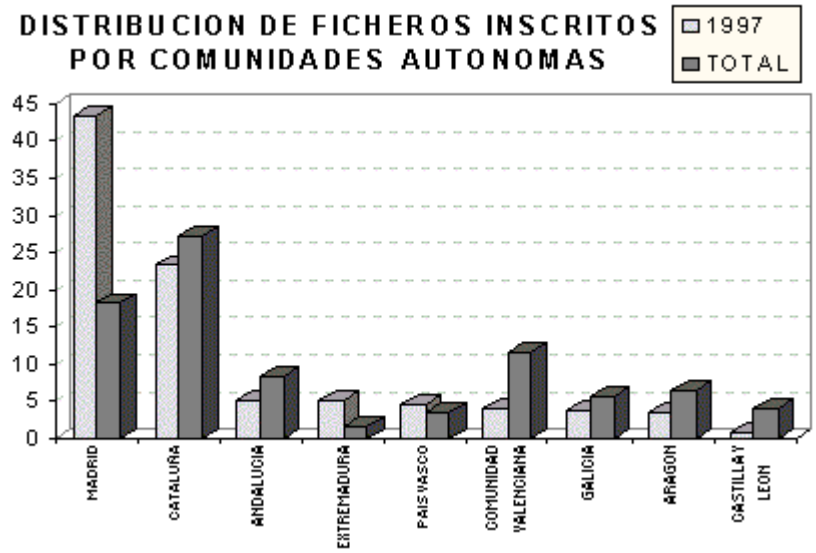
En cuanto a la distribución geográfica de la inscripción de ficheros durante el año 1997 por Comunidades Autónomas, se observa que Madrid ha inscrito el 43,3% del total de ficheros del ejercicio, Cataluña ha inscrito el 23,3% del total, Andalucía el 5,2%, Extremadura el 5,1%, País Vasco el 4,1%, Comunidad Valenciana el 4%, Galicia el 3,75% y Aragón el 3,6%. 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 para estas dos comunidades se asemejan a las del año anterior e indican una posible evolución paralela en el tiempo. En este aspecto, Cataluña presentaba cifras más altas de inscripción en los primeros años, pero a partir del ejercicio del 96 la inscripción de Madrid presentó un fuerte aumento, quizá debido al retraso inicial de las entidades, sobre todo en el sector predominante de las pequeñas y medianas empresas (PYMES), en conocer y asumir sus obligaciones respecto de la Ley en años anteriores. También es de resaltar que hay comunidades como Extremadura y la Comunidad Valenciana, que han presentado un aumento significativo de inscripción en contraste con el año anterior. El gráfico siguiente muestra las cifras de inscripción de ficheros durante el año 1997 por Comunidades Autónomas.



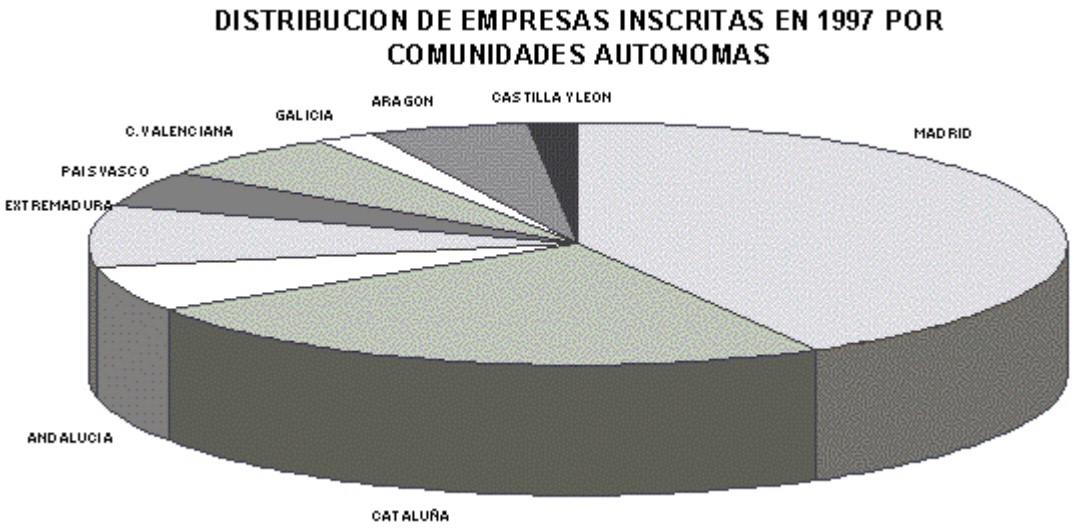
En cuanto a la inscripción total de ficheros por Comunidades Autónomas encabeza Cataluña con el 27,2%, seguida de Madrid con un 18,2%, Comunidad Valenciana con un 11,7%, Andalucía con un 8,4%, Aragón con un 6,4% , Galicia con un 5,7%, Castilla y León con un 4,1% y el País Vasco con un 3,6%. Estas cifras de inscripción total por Comunidades se presentan en el gráfico siguiente:



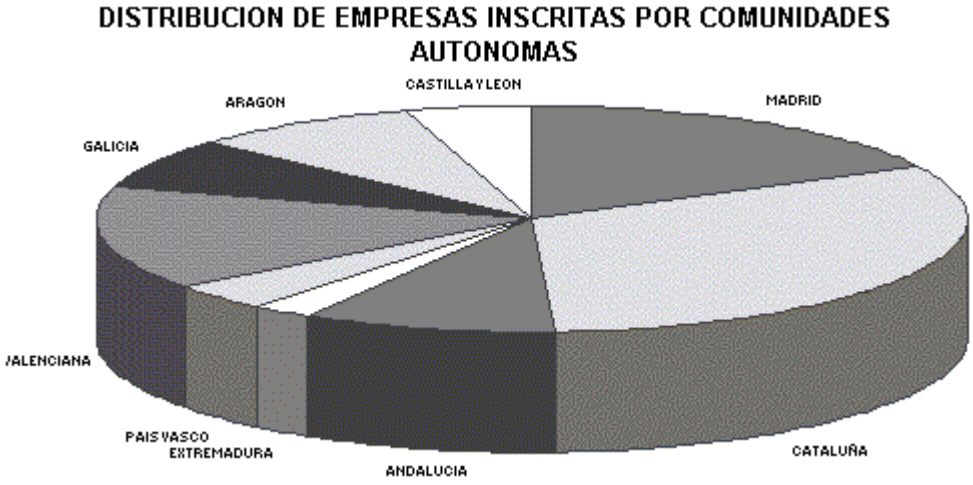
Si comparamos las cifras de inscripción de ficheros por Comunidades Autónomas para la inscripción total y la de 1997, se observa un cierto paralelismo, siendo notorio el aumento de inscripción en el último año en Madrid (aumento que se ha acentuado desde 1996) y Extremadura (debido al retraso en inscripción en años anteriores).



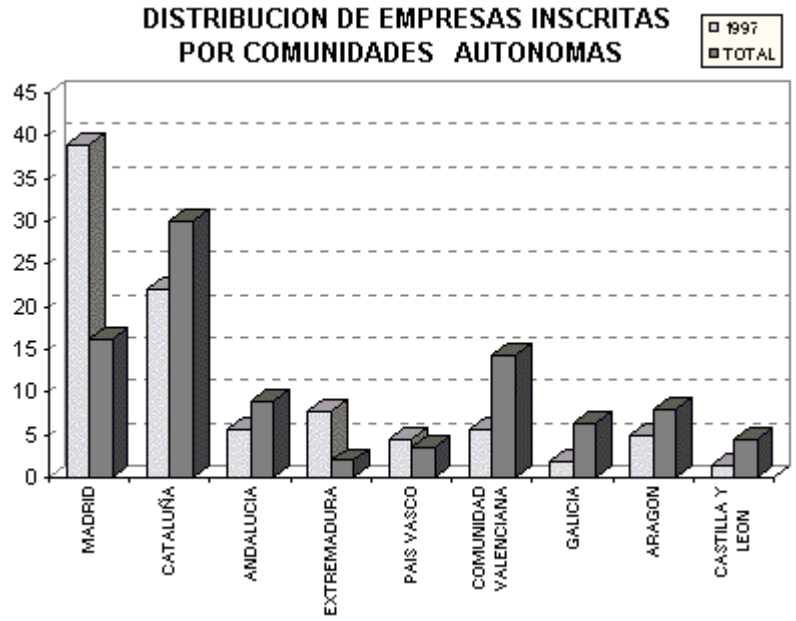
Si se analiza la distribución geográfica de la **inscripción por empresas** y por Comunidades Autónomas en el año 1997, se observa que los resultados son paralelos a los relativos a la inscripción de ficheros en el mismo año, tal y como se muestra en el siguiente gráfico.



En cuanto a la inscripción total por empresas y Comunidades Autónomas se obtienen los datos reflejados en la siguiente gráfica.



Si comparamos las cifras de inscripción de empresas por Comunidades Autónomas para la inscripción total y la de 1997, se observa un cierto paralelismo, siendo notorio el aumento de inscripción en el último año en Madrid y Extremadura, al igual que ocurría para las cifras de inscripción por ficheros.



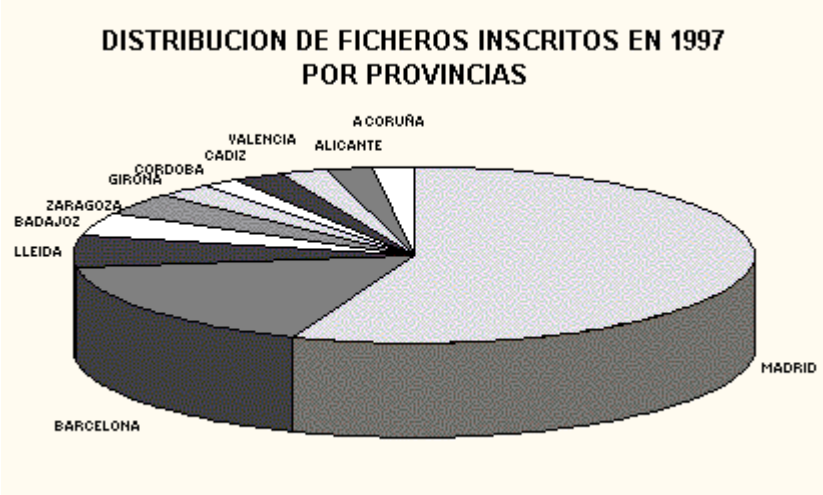
Según estos datos, es evidente la relación directa entre las cifras totales de inscripción de ficheros por Comunidades Autónomas y del número de empresas que la realizan. A su vez, las cifras de porcentajes de inscripción de empresas por Comunidades Autónomas referidas al total de la inscripción son muy aproximadas a las cifras ya expresadas para ficheros.

** Inscripción por Provincias.*

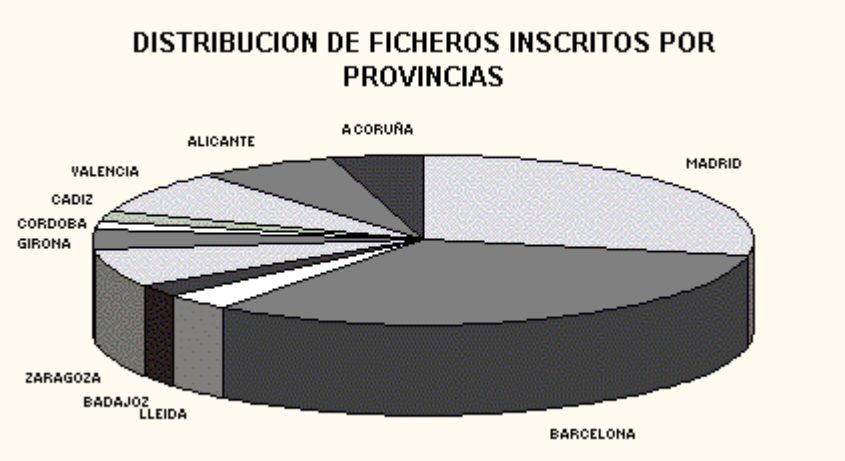
En cuanto a la distribución geográfica de la inscripción de ficheros por provincias en el año 1997, destacan Madrid con el 43,3% de la inscripción total del año, Barcelona con el 14,8%, Lleida con el 5,1%, Badajoz con el 3,8%, Zaragoza con el 3,5%, Girona con el 2,3%, Córdoba con el 1,5% y Cádiz con el 2,2%, Valencia con el 1,9% y Alicante, A Coruña y Vizcaya con el 1,8%. Estos datos concuerdan básicamente con las cifras de la distribución por Comunidades Autóno - mas presentadas en el epígrafe anterior. Respecto de las cifras del año anterior se observa una evolución pareja. Por otra parte, ya no existen diferencias tan fuertes entre la inscripción de las distintas provincias como en años anteriores y las cifras tienden a ser más uniformes.

En cuanto a la distribución geográfica de la inscripción total de ficheros por provincias en el Registro General hasta la fecha, encabeza la inscripción Barcelona con un 21,1% del total de ficheros inscritos, seguida de Madrid con un 18,2%, Valencia con un 5,2%, Zaragoza con un 4,75%, Alicante con un 4,5%, A Coruña con un 2,9%, Girona con un 2,4% , Murcia y Lleida con un 2,2%, Castellón de la Plana con un 2% y Sevilla y Guipúzcoa con un 1,8%.

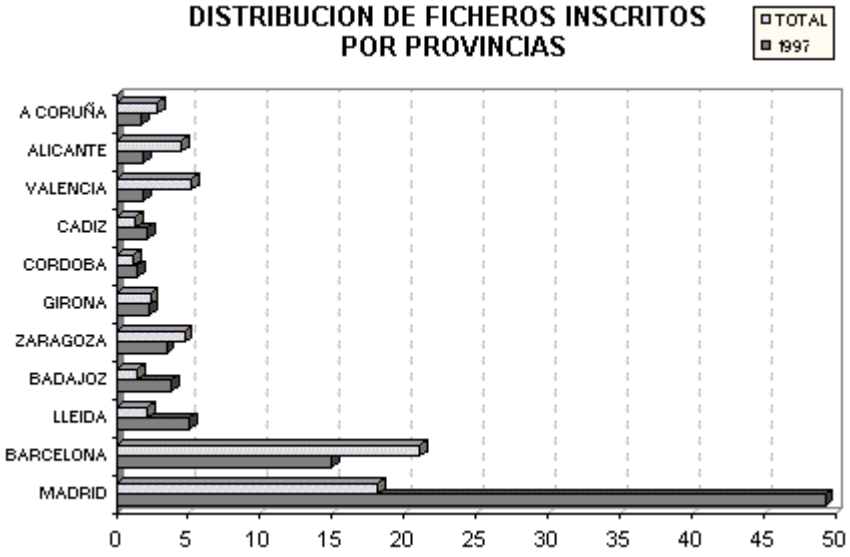
Estos datos concuerdan básicamente con las cifras de la distribución por Comunidades Autónomas presentadas en el epígrafe anterior. Respecto de las cifras del año anterior se observa una evolución pareja. Por otra parte, ya no existen diferencias tan fuertes entre la inscripción de las distintas provincias como en años anteriores y las cifras tienden a ser más uniformes. El siguiente gráfico ilustra las cifras.



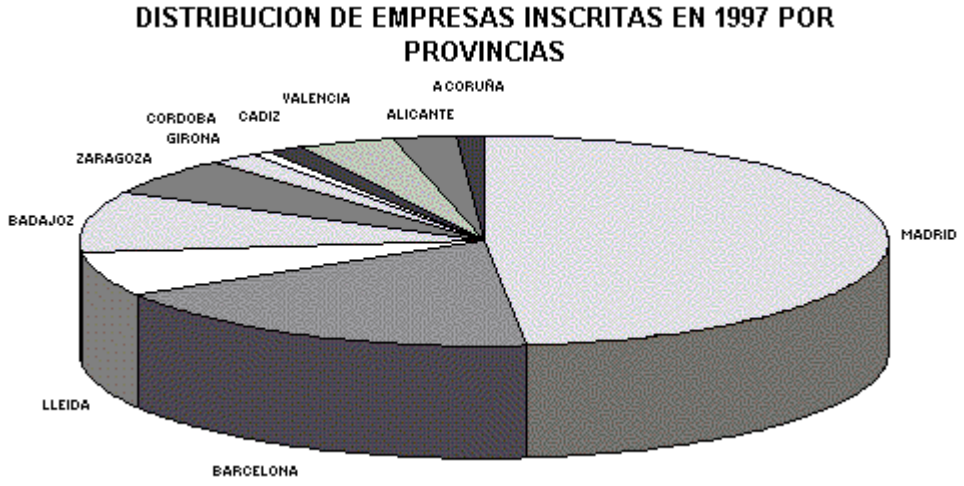
En cuanto a la distribución geográfica de la inscripción total de ficheros por provincias, se obtienen los datos reflejados en la siguiente gráfica, que muestran el equilibrio entre Barcelona y Madrid como provincias de mayor inscripción. También se observa un equilibrio entre las provincias que siguen a Madrid y Barcelona (A Coruña, Alicante, Valencia y Zaragoza).



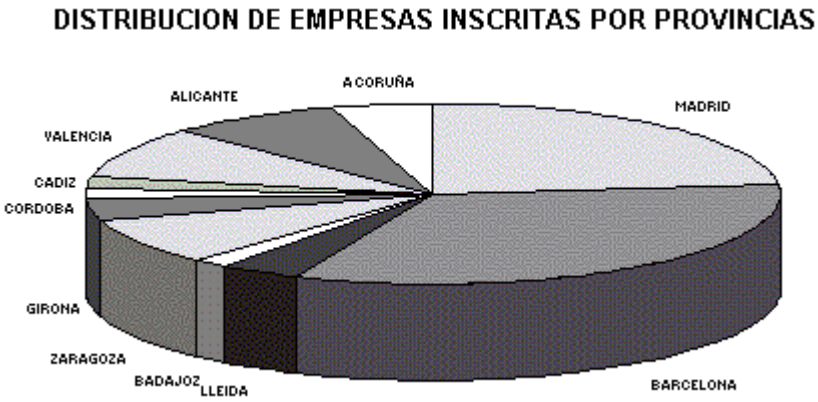
Si comparamos las cifras de inscripción de ficheros por provincias para la inscripción total y la de 1997, se observa un cierto paralelismo, siendo notorio el aumento de inscripción en el último año en Madrid y Badajoz, al igual que ocurría para las cifras de inscripción por Comunidades Autónomas.



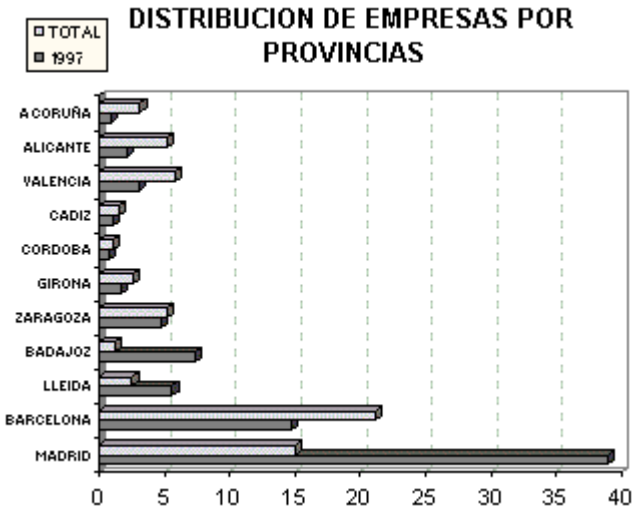
En cuanto a las cifras de empresas por Provincias del ejercicio de 1997, también la tendencia es similar a la inscripción de ficheros, como indica el gráfico siguiente, lo que indica la relación positiva entre las cifras de inscripción de ficheros por Provincias y del número de empresas que las realizan.



A su vez los porcentajes de inscripción de empresas por provincias referidos al total de la inscripción son similares a las cifras ya expresadas para ficheros, tal y como se indica en el gráfico siguiente, que también refleja la relación positiva entre las cifras de inscripción de ficheros por Provincias y del número de empresas que las realizan.



Si comparamos las cifras de inscripción de empresas por Provincias para la inscripción total y la de 1997, se observa un cierto paralelismo, siendo notorio el aumento de inscripción en el último año en Madrid y Extremadura, al igual que ocurría para las cifras de inscripción por ficheros.



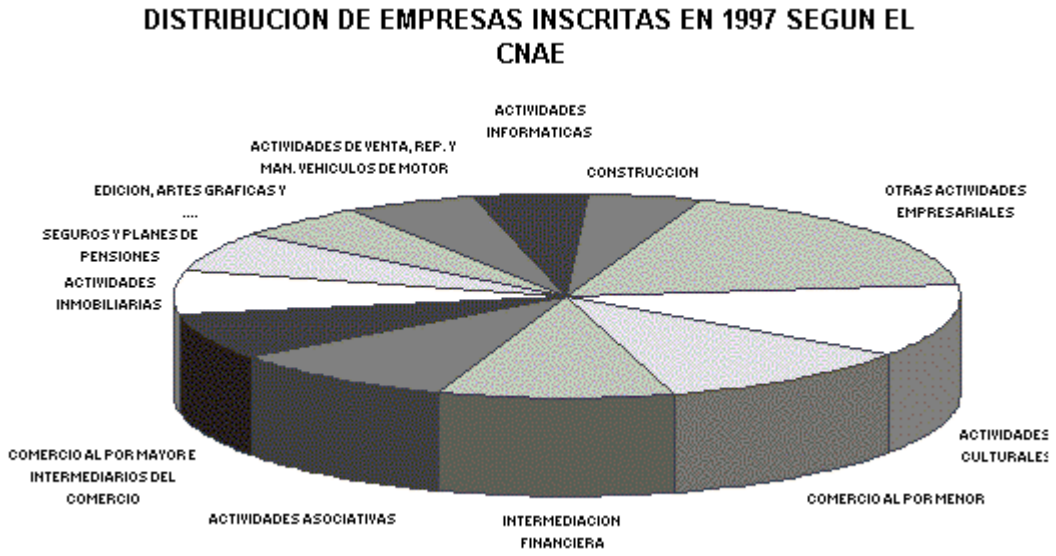
** Distribución temporal de la inscripción.*

En cuanto a la distribución temporal de la inscripción en 1997, se observa que los meses más fuertes han sido Julio, Diciembre, Noviembre, Abril, Enero y Febrero, por este orden, siendo Agosto el que presenta las menores cifras de inscripción. El resto de los meses presentan cifras smilares. Puede constatarse que las épocas de mayor inscripción son el primer y último trimestre del año, seguido del segundo trimestre que también presenta cifras altas. En el tercer trimestre se nota una bajada acentuda en la inscripción. Estas cifras son lógicas si consideramos que en los primeros trimestres del año inscriben todas aquellas empresas que por ignorancia de la ley u otras causas no lo habían hecho en el ejercicio anterior. Los cierres de ejercicio en las empresas originan las altas cifras de inscripción en el último trimestre, y la época vacacional es la causa de que la inscripción en el tercer trimestre sea menor. Hay otros factores aleatorios en el tiempo que también inciden sobre la evolución temporal de la inscripción, como pueden ser la publicidad institucional en los medios de comunicación, los artículos en prensa relativos a la intimidad y protección de datos, y los requeri - mientos que realiza la propia Agencia temporalmente demandando información a determinados sectores. Ante la presencia de cualquiera de estos factores, la inscripción aumenta en corto plazo.

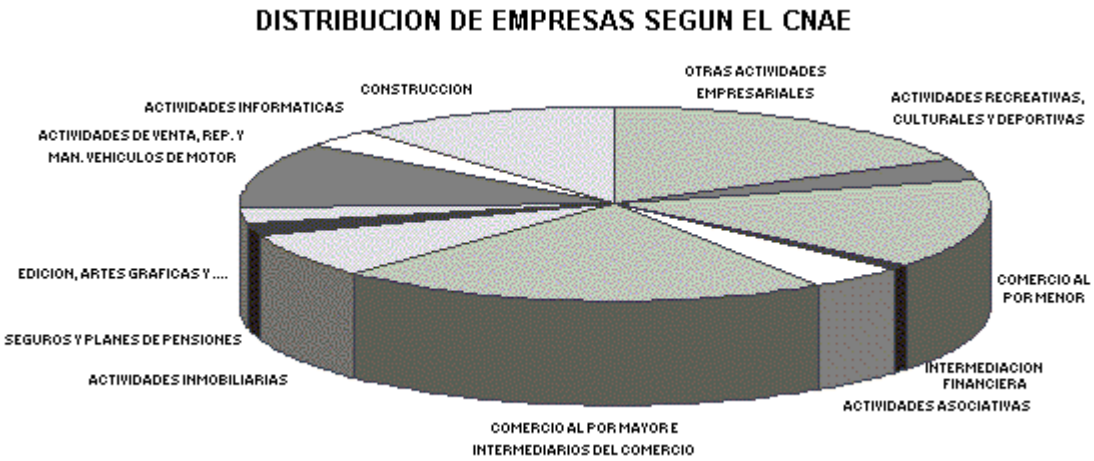
** Inscripción por Sectores Económicos.*

En cuanto a la inscripción por sectores económicos de actividad en el año 1997, predomina el sector de otras activi - dades empresariales que incluye las actividades jurídicas, de contabilidad, auditoría, asesoría fiscal, estudios de mercado, encuestas de opinión y asesoramiento sobre dirección y gestión empresarial con un 12,5% del total de empresas inscritas en el ejercicio. Le siguen las actividades recreativas, culturales y deportivas con un 8%, el comercio

al por menor con un 7,6%, la intermediación financiera con un 6,8%, las actividades asociativas con un 6,5%, el comercio al por mayor e intermediarios del comercio con un 5,2%, actividades immobiliarias con un 4,8%, seguros y planes de pensiones con un 4,4%, edición, artes gráficas y reproducción de soportes grabados con un 4%, actividades de venta, reparación y mantenimiento de vehículos de motor con un 3,6%, actividades informáticas con un 3,4%, construcción con un 3,25%, actividades sanitarias, veterinarias y servicio social con un 2,6%, actividades auxiliares a la intermediación financiera con un 2,2%, industria de productos alimenticios y bebidas con un 2,2%, y hostelería con un 1,9%. Estos datos se resumen en el gráfico siguiente:

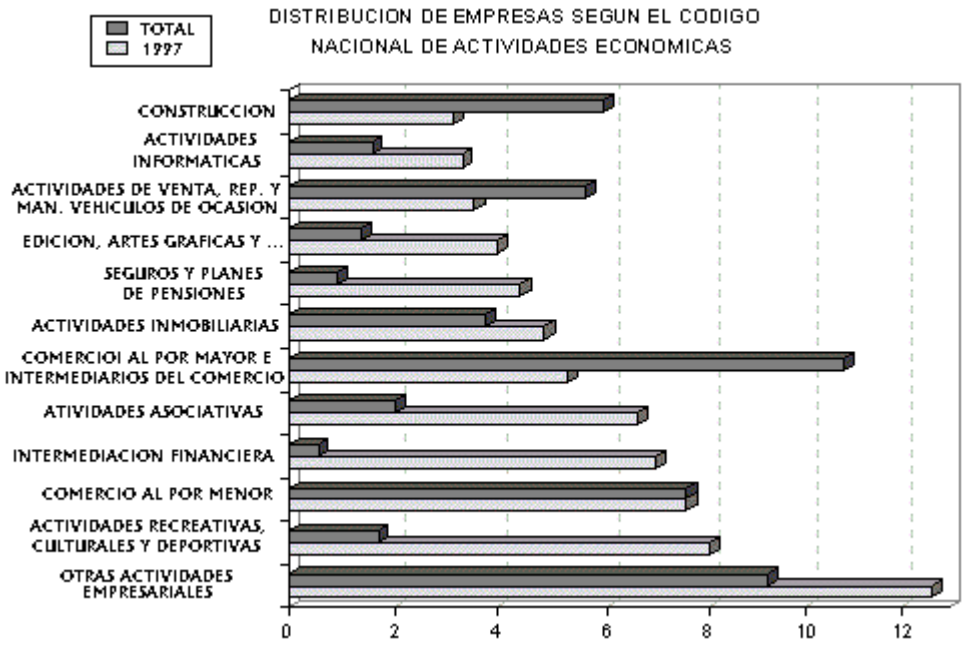


En cuanto a la inscripción total en el Registro General de Protección de Datos por sectores económicos de actividad, predomina el comercio al por mayor e intermediarios del comercio con un 11% del total de empresas inscritas. Le sigue el sector de otras actividades empresariales con un 9%, el comercio al por menor con un 7,6%, la construcción con un 5, 9%, las actividades de venta, reparación y mantenimiento de vehículos de motor con un 5,6%, las actividades inmobiliarias con un 3,8%, la hostelería con un 3,4%, la industria de productos alimenticios y bebidas con un 2,6%, las actividades auxiliares a la intermediación financiera con un 2,25%, las actividades asociativas con un 2% y las actividades de agricultura, ganadería, caza y actividaes de los servicios relacionados con las mismas con un 1,9%. Estos datos se reflejan en el siguiente gráfico.



Si comparamos las cifras de inscripción por Sectores Económicos para la inscripción total y la de 1997, se observa un aumento de la inscripción en el último año en los sectores de intermediación financiera, seguros y planes de pensiones, actividades recreativas, culturales y deportivas y actividades asociativas. Este aumento está directamente relacionado con la depuración de la inscripción de estos sectores realizada el año anterior y con los requerimientos a los responsables derivados de los resultados del análisis de la inscripción. El aumento de la inscipción el sector actividades

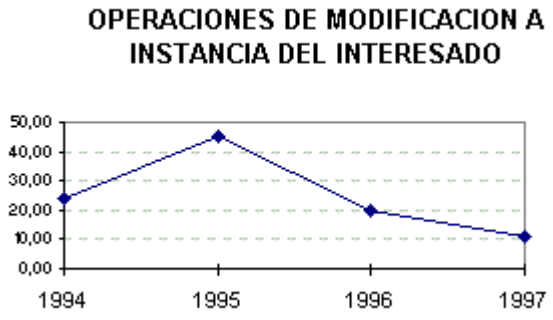
informáticas puede deberse al desarrollo continuo de esta rama de actividad en la actualidad.



3. 4.1.2. Modificación 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 1.597 ficheros, que suponen cerca del 1% del total de la inscripción de ficheros privados inscritos en el Registro. A diferencia de la inscripción de altas, el mayor porcentaje de modificaciones se ha solicitado a través de soporte papel (91,3%), mientras que el 8,7% restante solicitó la modificación a efectos de inscripción en soporte magnético.

La cifra de modificaciones es inferior a la de años anteriores debido a que el procedimiento de inscripción de nuevos ficheros se está notificando por responsables con un conocimiento superior de los principios de protección de datos y la interpretación de la Ley ofrece menos dificultades para los notificantes a medida que aumenta su difusión y su puesta en práctica. El siguiente gráfico refleja la evolución de las operaciones de modificación a instancia del interesado a lo largo de los años.



En cuanto a las cifras de modificaciones relativas a la inscripción total de ficheros, se han modificado hasta la fecha 14. 266 inscripciones de ficheros, lo que supone el 7,1% del total de los ficheros inscritos en el Registro General de Protección de Datos. El 86,6% de las modificaciones se han solicitado en soporte papel, y el 13,4% restante, en soporte magnético.

Se observa que, el apartado que ha sufrido mayores modificaciones como consecuencia de errores producidos en la inscripción, ha sido el de cesiones, quizá por la dificultad que supone la interpretación de la Ley en esta faceta o por las

dificultades prácticas para justificarlas legalmente. 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 esta parte de los formularios, o bien por la dificultad de plasmar en la notificación la procedencia real de los datos que originan los ficheros automatizados. En el apartado de responsable se producen errores de forma en la consignación del Código de Identificación Fiscal y en el Código Nacional de Actividad Económica (CNAE).

El apartado de responsable también ha generado confusión en la declaración de los ficheros, debido a que desde la perspectiva de los propios notificantes, han existido interpretaciones erróneas derivadas de situaciones como la falta de delimitación clara entre 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.

Otro problema adicional se presenta cuando se solicitan modificaciones del apartado de responsable del fichero originadas por cambio de titular, absorción por otra empresa, fusiones de empresas o cambios en los nombres de la razón social. En estos casos, además de producrise un problema en relación a 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 poder cumplir las exigencias legales en relación con lo dispuesto en el artículo 25 de la Ley, sobre la comunicación de nuevas cesiones a los afectados.

3. 4.1.3. Supresión de ficheros

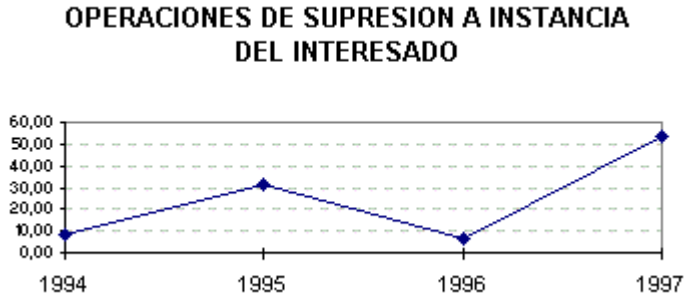
El artículo 8 apartado 2 del Real Decreto que desarrolla determinados aspectos de la Ley en relación a la modificación y cancelación de la inscripción de ficheros, dispone que cualquier modificación posterior en el contenido de los apartados declarados en la notificación inicial de ficheros, se deberá comunicar, a efectos de inscripción, igualmente se deberá comunicar la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

Durante el año 1997 se han realizado 1.571 operaciones de supresión de la inscripción de ficheros a petición de sus responsables lo que supone cerca del 1% del total de la inscripción de ficheros privados en el Registro General de Protección de Datos. Al igual que las modificaciones y a diferencia de la inscripción de nuevos ficheros, el mayor porcentaje de supresiones se ha solicitado en soporte papel (96,5%), mientras que el 3,5% restante se ha notificado en modelo magnético, dado que para este tipo de movimiento es mucho más sencilla la notificación realizada en el modelo convencional.

En cuanto a las cifras totales, se han suprimido hasta la fecha 2.923 inscripciones de ficheros, lo que supone un 1,5% de la inscipción total. En cuanto a la evolución en el tiempo, el 53,75% de las supresiones se han realizado durante el período que abarca el año 1997, el 7% se han realizado en 1996, el 31,3% se han realizado en 1995 y el 8,2% restante se han realizado en 1994.

La alta cifra de este tipo de operaciones que se han realizado durante 1997 se debe, según se detallará posteriormente, a la implantación de un nuevo procedimiento ´que evite errores en relación con la notificación de inscripción de ficheros realizada por las gestorías y asesorías que por cuenta de terceros, tramitan la notificación de ficheros al Registro. La elevada cifra que se produjo durante el año 1995 se debió a las supresiones realizadas en los procesos de depuración de la inscripción masiva que se llevaron a cabo en el citado año.

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 supresión física de los ficheros con datos personales. En estos casos, se solicita al responsable que garantice las medidas de destrucción y aclaren las circunstancias por las que se ha tomado la decisión de destruir el fichero. Además,

se anota, en su caso, la existencia de copias de seguridad, para 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 fusionado 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 de la operación de fusión que sustituyen a los suprimidos. Por otra parte, no se inscriben las supresiones hasta que no se constata la inscripción previa de los nuevos ficheros. Además los responsables han de garantizar las medidas de destrucción de los ficheros suprimidos.

- 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 no se garantice que no hay una cesión enmascarada, para lo cual han de aportarse las suficientes garantías que justifiquen el cumplimiento de los preceptos prescritos en 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 necesaria la inscripción previa de los nuevos ficheros de la empresa resultante, anotando 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 demasiados 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 o que nunca han estado automatizados ni lo van a estar. En estos casos se indica en los asientos 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 está duplicado. En el caso de la supresión de un fichero por titularidad errónea o por demasiados apartados incorrectos, 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 1.259 supresiones de inscripción realizadas durante 1997, con el fin de subsanar un error de interpretación de la norma en relación con la notificación de ficheros a efectos de inscripción, que se produce como resultado de una gestión automatizada de la contabilidad, fiscalidad y nóminas, cuando estos servicios son encomendados por pequeñas empresas o personas físicas a gestorías y asesorías que se dedican a prestar este tipo de servicio. En la mayoría de los casos, se ha solicitado una inscripción por cada uno de los clientes que componen los ficheros de las empresas que prestan estos servicios por cuenta de terceros, cuando la norma determina que, únicamente se tendría que solicitar una única inscripción por responsable y fichero con finalidades de uso conexa, ya que realmente, son las propias empresas prestadoras de estos servicios a terceros los que toman la decisión de automatizar la gestión y por lo tanto son los responsables de los ficheros según lo dispuesto en el artículo 3. c) de la Ley.

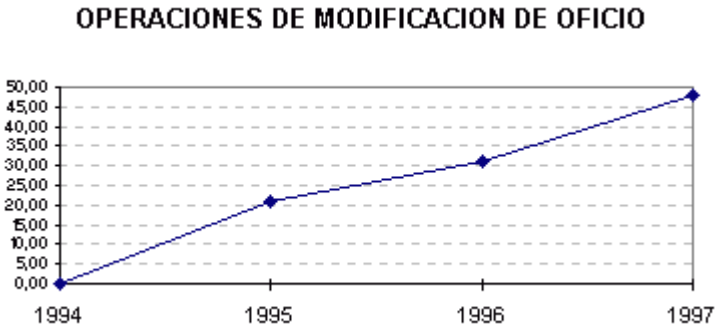
No obstante, no hay que confundir la situación anteriormente expuesta, con la que se desprendería de encargar a terceros la gestión de los servicios de tratamiento informático. En este caso, surge la figura definida en la Directiva 95/46/CE, como "encargado del tratamiento" recogida en la Ley en su artículo 27 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 objetivo de modificar los apartados de ubicación de los ficheros y sistemas de tratamiento.

3. 4.2. 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 1997 se han realizado un número de operaciones de oficio que han afectado a un total de 3.975 inscripciones de ficheros, lo que supone cerca de un 2% del total de ficheros inscritos en el Registro. El 91,2% de las operaciones de oficio corresponden a modificaciones de los asientos y un 8,8% a cancelaciones o supresiones de inscripciones.

La evolución temporal de las operaciones de oficio se presenta en los siguientes gráficos.



Estas operaciones de oficio, corresponden a procesos de control preventivo o planificados al efecto que se han llevado a cabo a lo largo del año.

3. 4.2.1. 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 ha procedido a la depuración de la base de datos con el fin de suprimir y eliminar todas aquellas inscripciones que correspondan a un mismo fichero.

El procedimiento establecido para realizar esta depuración ha sido seleccionar los ficheros del mismo responsable cuyo nombre y finalidad se repetía más de una vez en la base de datos, agrupándolos por responsables. Se detectó la existencia de ficheros que se encontraban inscritos dos veces en la base de datos, 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 184 inscripciones de ficheros.

Un hecho que ha dificultado este tipo de depuración, es el gran número de ellos que tenían cumplimentados los apartados de acceso y ubicación con información diferente ya que se trataba de empresas que tenían delegaciones en distintas localidades, y habían declarado sus ficheros con el mismo nombre y estructura, pero ubicación en localidades diferentes. En estos casos, se ha subsanado de oficio y de forma normalizada la denominación del nombre y descripción del fichero, unas veces incluyendo en la denominación del fichero el nombre de la localidad o bien el nombre de la sucursal o delegación. Este proceso de depuración ha afectado a 301 inscripciones de ficheros.

3. 4.3. OTRO TIPO DE ACTIVIDADES

Entre las actividades del Registro General de Protección de Datos, se encuentra la de realizar análisis de la inscripción cuando lo requiere una situación concreta, como puede ser una petición de la Dirección, una petición de la Inspección u otra causa similar. Dentro de este tipo de actividades destacan, durante el año 1997, los siguientes requerimientos:

** Datos Especialmente Protegidos*

Durante el año 1997, se procedió a requerir, por segunda vez, a 138 responsables de ficheros que habiendo recibido el primer requerimiento durante 1996, no habían procedido a aclarar o a subsanar la declaración de datos especialmente protegidos de ideología, creencias o religión. Se recibieron 70 respuestas que comunicaban que se había cometido un error en la declaración inicial de sus ficheros ya que éstos no contenían ni habían contenido datos de esta naturaleza.

Se recibieron 14 respuestas justificando el uso de este tipo de datos por las siguientes causas:

Gestión fiscal. Los responsables de 12 ficheros de los sectores de asesorías fiscales y gestorías declaraban ficheros con el fin de realizar la declaración del Impuesto sobre la Renta de las Personas Físicas, y señalaban el dato de Religión debido a la opción que se debe reflejar en la declaración, relativa a la cuota destinada por el Estado a sufragar las necesidades de la Iglesia Católica.

Gestión de la afiliación sindical de empleados. Esta información se recoge y gestiona según lo dispuesto en el artículo 11 de la Ley Orgánica 11/1985 de 2 de agosto, de Libertad Sindical, con el consentimiento del afectado y con el fin específico de la recaudación de cuotas de los afiliados por pertenencia a un sindicato. Por lo tanto, los empresarios responsables de ficheros declaran el apartado de Ideología cuando en sus ficheros figuran datos relativos a la afiliación sindical de los empleados. Ese tipo de justificación afectó a un fichero.

Entidad Religiosa . Una entidad religiosa justifica la presencia de datos de religión en su fichero.

Para el resto de responsables que no contestaron a este requerimiento se procederá a dar traslado a la Inspección a los efectos oportunos.

** Clubes de Fútbol o Sociedades Deportivas*

Como continuación a los dos requerimientos a Clubes de Fútbol y Sociedades Deportivas realizados en 1996 se procedió a remitir a la Inspección de Datos, a los efectos oportunos, la relación de 15 entidades que no habían procedido a declarar sus ficheros a efectos de inscripción. Durante el trámite de los correspendientes expedientes, se recibió la notificación de diez clubes solicitando la inscripción de sus ficheros. Las cinco entidades que no habían procedido a inscribir sus ficheros durante el período de tramitación del expediente sancionador resultaron sancionadas por Resolución del Director de la Agencia.

** Federaciones Deportivas*

Como continuación a los dos requerimientos a Federaciones Deportivas realizados en 1996, en Enero de 1997 se procede a remitir a la Inspección de Datos, a los efectos oportunos, relación de las 12 entidades que no habían contestado a ninguno de los dos requerimientos enviados por el Registro General de Protección de Datos. Realizadas las correspondientes inspecciones todas las entidades requeridas procedieron a la inscripción de sus ficheros.

** Entidades Aseguradoras*

Como continuación a los dos requerimientos a Entidades Aseguradoras realizados en 1996, en Enero de 1997 se procede a remitir a la Inspección de Datos, a los efectos oportunos, relación de las entidades que no habían contestado a ninguno de los dos requerimientos enviados por el Registro General de Protección de Datos. Realizadas las correspondientes inspecciones se recibieron diez nuevas inscripciones y la comunicación de la Inspeción de Datos de que siete entidades no poseen ficheros automatizados de datos de carácter personal.

** Ficheros con Ubicación Física en el Extranjero*

Como continuación a los requerimientos realizados a responsables de ficheros que no declaraban Transferencias Internacionales y si declaraban la ubicación de sus ficheros en un país extranjero, se procedió a remitir a la Inspección de Datos, a los efectos oportunos, relación de responsables que no habían notificado al Registro la declaración de dicha Transferencia Internacional. Realizadas las correspondientes inspecciones, en Mayo de 1997 quedan resueltos todos los requerimientos, se recibieron solicitudes de autorización de Transferencia Internacional, dos responsables notifican, para su inscripción, el apartado de Transferencia, dado que el país de destino era del mismo nivel de protección al de la Ley Orgánica 5/1992, y un responsable notificó la supresión del fichero, dado que el mismo no contenía datos de carácter personal.

3. 5. 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 establece la definición de 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 al artículo 12 del Convenio 108 del Consejo de Europa, estableciendo así una regulación del concepto de "flujo transfronterizo de datos". La protección de la integridad de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituyen una auténtica necesidadde 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 autorización del Director de la Agencia cuando tal sistema no exista, 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, 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".

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.

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.

3. 5.1. PAÍSES QUE PROPORCIONAN UNA PROTECCIÓN DE DATOS EQUIPARABLE A LA ESPAÑOLA

El Ministerio de Justicia, previo informe del Director de la Agencia, aprobó la relación de países que, a efectos de lo dispuesto en el artículo 32 de la Ley, proporcionan un nivel de protección equiparable por Orden de 2 de febrero de 1995, publicado en Boletín Oficial del Estado de fecha 10 de febrero de 1995.

La primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos, integra varias relaciones parciales, especificando de forma separada los países que proporcionan un nivel de protección equiparable al español, según se trate de ficheros de titularidad pública o privada.

Por otra parte, tanto las legislaciones de los distintos países como los estudios que se llevan a cabo en España sobre su naturaleza y alcance, se encuentran en un proceso de evolución permanente; por esta razón la relación de países tiene un carácter abierto, que deberá ser continuada y completada, en paralelo con la evolución de las legislaciones extranjeras y de los estudios correspondientes.

En este sentido, se ha planteado al Ministerio de Justicia la necesidad de sugerir la conveniencia de una nueva Orden que complete la anterior en dos materias diferentes:

- La primera, efectuando un cambio en el título de la misma de manera que no se hable de países con protección de datos de carácter personal equiparable, sino de países que garanticen un nivel de protección adecuado respecto de los datos personales que sean objeto de tratamiento o que estén destinados a ser objeto de tratamiento con posterioridad a su transferencia, tal y como dispone el artículo 25.1 de la Directiva.

- La segunda, completando la lista de países. A tal fin, por un lado, en el grupo primero de la Orden de 2 de febrero de 1995, deberían incluirse Italia y Grecia, cuyas Leyes de Protección de Datos fueron aprobadas el 31 de diciembre de 1996 y 10 de abril de 1997, respectivamente. Y, por otro, debería añadirse en el apartado segundo, a Estonia, en cuanto garantiza, desde el 19 de julio de 1996, un nivel de protección suficiente tanto en ficheros de titularidad pública o privada y a Lituania ya que desde el 11 de junio de 1996 garantiza nivel de protección suficiente, si bien solamente en los ficheros de titularidad pública.

3. 5.2. 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 requiere la exigencia de una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia, ubicada legalmente en nuestro país. Dicha entidad, como responsable de los ficheros, deberá garantizar 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. Se requieren las garantías que se exponen a continuación:

* Toda la información de las circunstancias relacionadas con la transferencia, y en particular;

- la naturaleza de los datos,
- la finalidad,
- medidas de seguridad
- la duración del tratamiento,
- el país de destino final,
- normas sectoriales, o profesionales que pudieran existir.

* 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.

* Que la titularidad del fichero corresponde a una entidad domiciliada en territorio español y que dicha entidad, como responsable del fichero, garantizará todas las obligaciones y derechos establecidos, así como que se continuará facilitando desde España los derechos de acceso, rectificación y cancelación.

* 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.

* Deberán indicar la dirección completa de la empresa destinataria de la transferencia, la naturaleza de los datos que se van a transferir, las finalidades para las que se transfieren los datos, la duración del tratamiento, las medidas de seguridad adoptadas, el sector de actividad al que pertenece la empresa, la existencia de normas sectoriales o profesionales que pudieran existir, así como cualquier otra información que consideren oportuna.

3. 5.3. ANÁLISIS DEL APARTADO DE TRANSFERENCIAS INTERNACIONALES A EFECTOS DE INSCRIPCIÓN

El total de ficheros inscritos en el Registro, que contienen en su declaración transferencias internacionales de datos es de 919 de los cuales 48 corresponden a inscripciones de titularidad pública y 871 de titularidad privada.

A lo largo del año 1997, se analizaron 112 ficheros, tanto públicos como privados, inscritos en el Registro que habían declarado transferencias internacionales amparándose en supuestos legales relacionados con legislación dineraria.

Las entidades privadas que declaran este tipo de transferencias internacionales son, por lo general, bancos, cajas de ahorro, sociedades de inversión financiera y entidades de seguros. También hay otras entidades que las declaran con la finalidad de mantener relaciones comerciales con clientes o proveedores extranjeros.

En cuanto a los ficheros de titularidad pública, que consignaban este tipo de transferencias, se encuentran 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 del Organismo Parques Nacionales y de la Comunidad Autónoma de Navarra, y los ficheros relacionados con la gestión de los fondos FEDER inscritos por el Ministerio de Economía y Hacienda. Adicionalmente estas transferencias, excepto las del Banco de España, se encuentran amparadas en la existencia de Convenios con la Unión Europea.

Adicionalmente, en algunas de las inscripciones se declaran además alguno de los siguientes motivos:

Se ampara en tratado o convenio del que España forma parte	Se efectúa con destino a algún país con nivel de protección	Se efectúa con autorización del Director de la Agencia	TITULARIDAD PÚBLICA	TITULARIDAD PRIVADA
No	No	No	5	14
No	Si	No	1	60
No	Si	Si	0	2
Si	No	No	0	3
Si	Si	No	12	14

Los tratados o convenios en los que se amparan son:

TRATADO O CONVENIO
TITULARIDAD PRIVADA
LAS DERIVADAS DE LAS RELACIONES INTERBANCARIAS INTERNACIONALES CONFORME A SU LEGISLACION ESPECIFICA
REGIMEN JURIDICO DE CONTROL DE CAMBIOS LEY 40/79 DEL 10/12; REAL DECRETO 2402 DEL 10/10/80; LEY ORG. 10/83 DE 16/08 Y SIGUIENTES.
TODAS LAS QUE REGULAN EL COMERCIO INTERNACIONAL DE DIVERSO RANGO Y DISTINTAS FECHAS
TRATADO UNION EUROPEA

Los textos consignados en el subapartado de país destinatios son los siguientes:

PAIS DESTINATARIO	TITULARIDAD PUBLICA	TITULARIDAD PRIVADA
Alemania	-	6
Bélgica	3	6
Brasil	-	1
Colombia	-	1
Dinamarca	-	5
Estados Unidos	-	15
Filipinas	-	2
Finlandia	-	1
Francia	-	5
Holanda	-	3
Israel	-	1
Italia	-	3
Japón	-	7
Reino Unido	-	10
Suiza	-	25
Venezuela	-	1
Internacional	2	35
Unión Europea	11	7

Como resultado del análisis expuesto anteriormente se procedió a realizar dos grupos, identificados cada uno de ellos por las siguientes consideraciones:

- Ficheros que no pertenecían al sector financiero pero que habían declarado realizar este tipo de transferencia con la finalidad de gestión de clientes en terceros países.

- Ficheros pertenecientes a entidades financieras que realizan transferencias amparadas en su legislación específica en materia dineraria. Normalmente adherido al sistema SWIFT(Sistema internacional de intercambio de datos bancarios).

En el primer caso, se requirió a los responsables, para comunicarles que la declaración de la Transferencia Internacional, no estaba amparada por la legislación dineraria, ya que de la descripción o finalidad del fichero, se deducía que no se trataba de transferencias de este tipo.

En relación con el segundo grupo, se constató que era suficiente la declaración amparada en la legislación dineraria y adicionalmente se subsanó el error al declarar que se amparan en un Tratado Internacional.

Al cierre de este ejercicio queda pendiente la respuesta a los respectivos requerimientos, siendo previsible la respuesta de todos ellos en el primer trimestre del año.

3. 5.3.1. 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 772. A continuación con 53 inscripciones, se encuentran los ficheros que declaran transferencias dinerarias conforme a su legislación específica, casi todos ellos en relación con el sector financiero. Se declaran 17 ficheros que realizan las transferencias amparados en Tratados o Convenios en los que España forma parte. El número de transferencias internacionales amparadas en este supuesto, son un número 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. Siete ficheros realizan la transferencia de datos a otros países con objeto de intercambiar datos de carácter médico cuando así lo exige el tratamiento del afectado o una investigación epidemiológica.

3. 5.3.2. 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 44 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, 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 39. Por otra parte, 15 ficheros contienen transferencias de carácter dinerario, nueve ficheros declaran las transferencias internacionales a efectos de prestar auxilio judicial internacional y cinco ficheros tienen por objeto intercambiar datos de carácter médico.

Expedientes de autorización de Transferencia Internacional

La petición de autorización de transferencias internacionales de datos, efectuada al amparo del artículo 32 de la Ley, requiere la exigencia de una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia y que se encuentra domiciliada en nuestro país. Dicha entidad, como responsable de los ficheros, deberá garantizar 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. Una vez dictada la autorización por el Director de la Agencia, en virtud de las competencias que tiene establecidas por el artículo 36.l) de la Ley, será objeto de inscripción en el Registro General de Protección de Datos, según determina el artículo 38. c).

Durante el año 1997, se han solicitado 25 expedientes de autorización. Resolviéndose en el año, 24 de ellos. Además se han resuelto seis, iniciados en el año 1996. Por lo tanto, se han autorizado e inscrito en el Registro General 30, quedando pendiente de resolución un expediente para el ejercicio siguiente. En la tramitación de estas autorizaciones se han visto afectados 33 ficheros, siendo Estados Unidos el país que más autorizaciones recibe, debido a que un gran porcentaje de las multinacionales tienen su empresa matriz en dicho país. Por otra parte, también se solicitan autorizaciones para los múltiples países en los que una empresa tiene ubicadas delegaciones, debido a que en un mismo expediente se pueden autorizar diferentes países como destinatarios de las transferencias internacionales. En estos casos, se normaliza la inscripción, inscribiendo como países de destino la denominación "internacional".

En cuanto a las cifras totales de expedientes autorizados, se han tramitado 81 expedientes de autorización de transferencia internacional de datos, de los cuales 15 se han iniciado en el año 1995, 41 en el año 1996 y 25 en el año 1997. En total se han visto afectados por expedientes de autorización de transferencias internacionales 128 inscripciones de ficheros. El principal país destinatario de los datos ha sido Estados Unidos con un 78,13% de los ficheros autorizados seguido a mucha distancia por las transferencias autorizadas a un número determinable de países coincidentes con las sedes de una empresa.

3. 5.4. ANÁLISIS DE LAS CIRCUNSTANCIAS DEL MOVIMIENTO INTERNACIONAL DE DATOS

Las solicitudes presentadas por responsables de ficheros en las que se solicita autorización para realizar una transferencia internacional se han basado fundamentalmente en las siguientes razones:

- Razones de 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 crédito, seguros, química y fabricantes de bienes informáticos.

- Razones de mejor servicio al cliente. Se encuentra en diferentes sectores y para fines muy diferentes,

* 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 poder atender al cliente cuando éste se encuentre desplazado en el país destinatario de la transferencia. Siempre se realiza ante la solicitud del interesado.

- Razones que implican necesariamente la transmisión de los ficheros para satisfacer la petición del cliente.

* Las alegan empresas responsables de los sistemas de distribución mundial. La generalización de reserva, emisión de billetes y otros servicios del transporte a nivel internacional de los sistemas mundiales de distribución 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 están 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 por medio de terminales u ordenadores personales 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 se produce ante una relación contractual de la que el interesado forma parte con el fin de obtener servicios en otros países.

3. 5.5. PROBLEMAS PRÁCTICOS

Los problemas que se ha ido encontrando la Agencia de Protección de Datos en la tramitación de las autorizaciones de Transferencias Internacionales pueden resumirse de la siguiente forma:

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 empresa ubicada en el territorio español es una de las delegaciones que la compañía matriz (ubicada fuera del extracomunitario de la Unión Europea) tiene en distintos países para realizar una cobertura mundial a 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.

Se exige un certificado de la entidad que garantice que los datos de sus clientes se van a tratar a nivel mundial de conformidad con la Ley Española.

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 firmado de la empresa en relación a las normas de seguridad de acceso a la información a nivel mundial.

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 exigió al responsable del fichero establecido fuera del territorio de la Unión, la obligación de determinar otra persona física o jurídica residente en España que será el nuevo responsable del tratamiento y de la Transferencia Internacional.

A su vez se exigió a la empresa ubicada en España la obligación de comunicar la extinción del contrato a la Agencia de Protección de Datos.

En estos casos se exige a las dos empresas medidas contractuales en las que figure las actuaciones expuestas anteriormente.

3. La Transferencia Internacional se realiza por una empresa española ubicada en territorio nacional, que no tiene delegaciones comerciales fuera del territorio español.

La empresa se dedica al sector de actividad 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 conforman el informe comercial, el responsable del tratamiento deberá informar y tener el consentimiento del interesado, antes de realizar la Transferencia, la identidad del destinatario de los datos y el país en el que está establecido.

4. La Transferencia Internacional para tratamiento de datos con finalidad de realizar la gestión de recursos humanos de una forma global de un grupo de empresas con sede en diversos países cuya central estaba establecida en un tercer país.

El problema residía 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 y el consentimiento informado para realizar la transferencia a países terceros.

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 esta 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 en el caso que la empresa no fuera española.

6. Empresas que no pertenecen al sector Bancario y su objeto es transferir dinero a terceros países a los familiares de las personas titulares de los datos.

Se consideró que la finalidad era la misma que la transferencia dineraria y por tanto, no es exigible la autorización.

7. 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 video club, a los efectos estrictamente estadísticos y prestación de servicios de tratamiento informático con consentimiento del interesado a estos efectos.

Se justifica la necesidad de la Transferencia Internacional, ante 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.

8. La Transferencia Internacional a un tercer país por una empresa española cuya actividad es el establecimiento de un directorio 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, y 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 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.

3. 5.6. LA DIRECTIVA EUROPEA Y LA TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

La Directiva Europea sobre Protección de Datos considera que el establecimiento y funcionamiento del mercado interior en el que está garantizada la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria junto con la protección de los derechos fundamentales de las personas la libre circulación de datos personales de un Estado miembro a otro. Por otra parte se reconoce que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social, que el avance de las tecnologías de la información facilita considerablemente el tratamiento e intercambio de los datos y con el paso del tiempo, que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un gran desarrollo. En este sentido, se puede realizar un paralelismo con las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario europeo, están destinadas a colaborar e intercambiar datos personales a fin de cumplir sus funciones, en el marco del espacio sin fronteras que conforma el mercado interior.

La Directiva no sólo regula el tratamiento de datos personales dentro de la UE, sino que **también incluye disposiciones sobre transferencia de datos a países terceros** (artículos 25 y 26), considerando que el hecho de que el responsable de un fichero o tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas y que en estos casos deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la legislación del Estado miembro. El principio básico es que los Estados miembros únicamente deberían permitir dichas transferencias cuando se garantice un nivel de protección de datos adecuado. Existe claramente la posibilidad de que se den casos donde no se garantice una protección adecuada, y siempre que

no se aplique ninguna de las exenciones previstas, las transferencias se verán bloqueadas.

Un giro tal de los acontecimientos podría causar trastornos considerables a los flujos mundiales de datos personales, y en consecuencia, al comercio internacional. Si bien el artículo XIV del GATTS (Acuerdo General sobre el Comercio de Servicios) permitiría el bloqueo de las transferencias de datos personales, sería no obstante preferible evitar esta situación. La solución óptima sería que aquellos paises terceros a los que se transfieren datos regularmente elevaran su nivel de protección hasta un nivel considerado satisfactorio.

La UE está negociando acuerdos generales que proporcionen un marco común para las **relaciones comerciales y de cooperación** con terceros países. Estos acuerdos suelen cubrir una amplia gama de aspectos, desde la política exterior y de seguridad hasta aspectos comerciales y de desarrollo económico. Desde que se adoptó la Directiva sobre protección de datos, los servicios de la Comisión persiguen incluir en dichos acuerdos, directa o indirectamente, la protección de datos y de la vida privada, con ocasión de la negociación de los mismos.

Algunos países pueden resultar *paraísos de dato* para los operadores económicos que busquen menores costes de tratamiento de datos. El objetivo de los acuerdos entre la Comunidad y estos países ha sido simplemente un intercambio de información junto con una recomendación de que el pais en cuestión considere cómo puede garantizar una protección adecuada a las transferencias de datos procedentes de países de la CE. La protección de datos se ha planteado de esta forma con Méjico y Paquistán, no obstante, la lista de países está en constante crecimiento.

En Japón, ya existe una ley de protección de datos que cubre el sector público, si bien cuenta con amplias excepciones. Las autoridades japonesas están considerando la forma de desarrollar normas de protección de la vida privada para el sector privado.

El acuerdo marco con Canadá firmado en diciembre de 1996 prevé el mismo tipo de debates entre las autoridades europeas y canadienses sobre la intimidad en la vida privada.

Además de todas estas reuniones, la solución lógica a largo plazo para los problemas de flujo internacional de datos personales sería un acuerdo multilateral sobre un conjunto de normas obligatorias relativas a la protección de datos.

Aparte de estas acciones específicas, la Comisión está desarrollando una política coherente con vistas a la aplicación de las disposiciones sobre transferencia de datos de la Directiva a países terceros. Se encargó al "Centre de Recherche Informatique et Droit de la Universidad de Namur, en Bélgica, un estudio sobre la metodología para la evaluación de dichas transferencias de datos. Este trabajo ha servido como base para la discusión de estos temas en el Grupo de Trabajo del artículo 29 de la Directiva.

3. 6. 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 1997, el número de ficheros inscritos en el Registro General era de 229.804, de los cuales 27.969 correspondían a inscripciones de titularidad pública y 201.835 a inscripciones de titularidad privada.

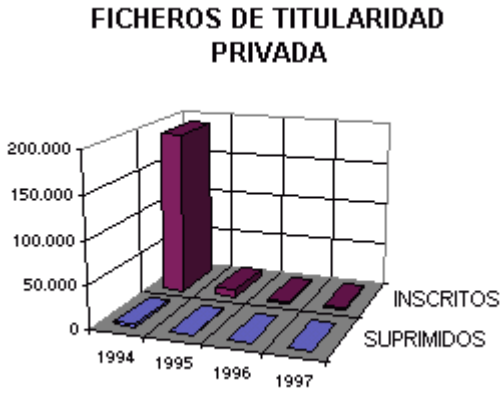
RESUMEN DETALLADO SEGUN LA TITULARIDAD, ESTADO DEL FICHERO Y AÑO DE INSCRIPCION

Se recoge en esta tabla el estado de los ficheros a 31 de Diciembre de 1997, en función de la titularidad, estado y año en que se ha realizado la inscripción de los mismos.

ESTADO	**INSCRITOS**				**SUPRIMIDOS**			
AÑO INSCRIPCION	**1994**	**1995**	**1996**	**1997**	**1994**	**1995**	**1996**	**1997**
TITULARIDAD PUBLICA	19.845	4.783	1.819	1.522	1.207	46	38	1
T O T A L	27.969				1.292			
TITULARIDAD PRIVADA	189.937	7.945	2.193	1.760	3.541	297	215	29
T O T A L	201.835				4.082			
TOTAL AÑO	209.782	12.728	4.012	3.282	4.748	343	253	30
	229.804				5.374			

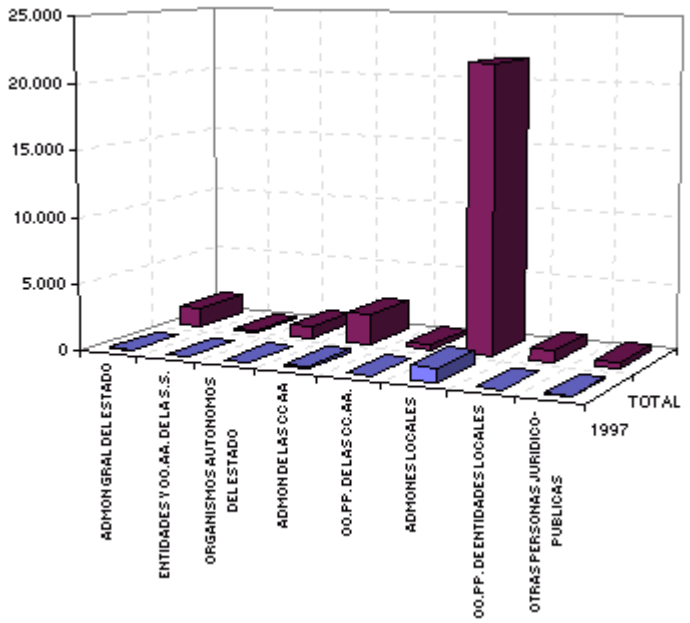
(*) Las cifras que aparecen en esta tabla correspondientes a los años 1994, 1995 y 1996 no coinciden con las publi-

cadas en memorias anteriores, debido a que durante el año 1997 se han realizado operaciones de supresión sobre ellos.



DISTRIBUCIÓN DE FICHEROS PÚBLICOS INSCRITOS SEGÚN EL TIPO DE ADMINISTRACIÓN AL QUE PERTENECEN

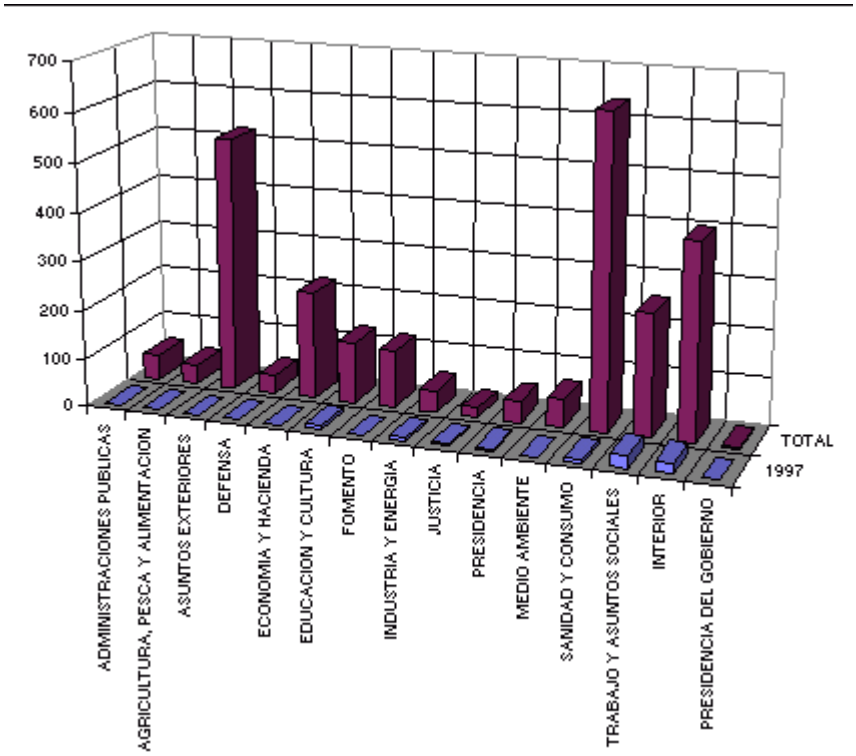
	1997	TOTAL
ADMON GRAL DEL ESTADO	39	1.523
ENTIDADES Y OO.AA. DE LA S.S.	13	106
ORGANISMOS AUTONOMOS DEL ESTADO	26	939
ADMON DE LAS CC AA	206	2.235
OO.PP. DE LAS CC.AA.	29	345
ADMONES LOCALES	1081	21.577
OO.PP. DE ENTIDADES LOCALES	34	793
OTRAS PERSONAS JURIDICO-PUBLICAS	94	451
TOTAL	1.522	27.969



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 General del Estado, Entidades y Organismos de la Seguridad Social y Organismos Autónomos del Estado, integrando a éstos dentro del Ministerio al que están adscritos.

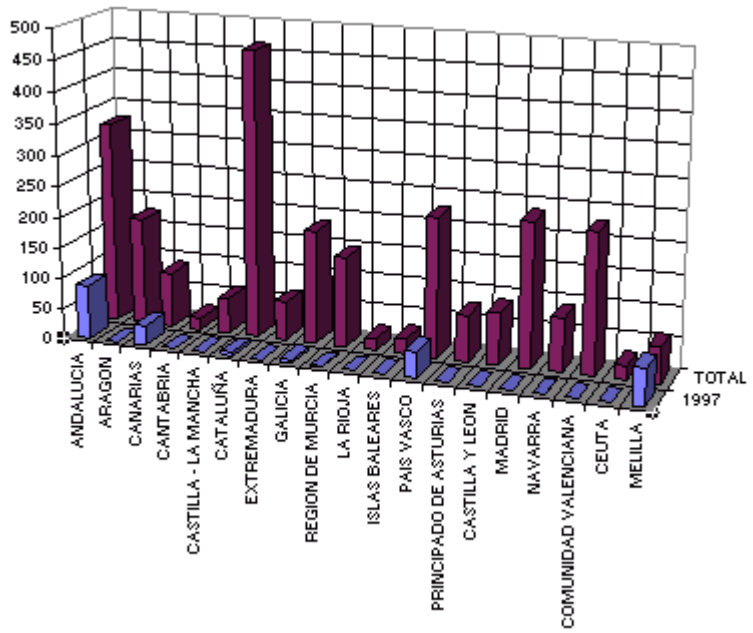
	1997	TOTAL
MINISTERIO DE ADMINISTRACIONES PUBLICAS	0	51
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACION	1	39
MINISTERIO DE ASUNTOS EXTERIORES	0	522
MINISTERIO DE DEFENSA	0	37
MINISTERIO DE ECONOMIA Y HACIENDA	0	220
MINISTERIO DE EDUCACION Y CULTURA	8	125
MINISTERIO DE FOMENTO	0	119
MINISTERIO DE INDUSTRIA Y ENERGIA	6	45
MINISTERIO DE JUSTICIA	4	19
MINISTERIO DE LA PRESIDENCIA	5	42
MINISTERIO DE MEDIO AMBIENTE	0	58
MINISTERIO DE SANIDAD Y CONSUMO	7	635
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	25	252
MINISTERIO DEL INTERIOR	22	400
PRESIDENCIA DEL GOBIERNO	0	4
TOTAL	78	2.568



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	1997	TOTAL
ANDALUCIA	86	327
ARAGON	0	174
CANARIAS	32	89
CANTABRIA	0	20
CASTILLA - LA MANCHA	1	57
CATALUÑA	6	463
EXTREMADURA	0	62
GALICIA	6	184
REGION DE MURCIA	1	146
LA RIOJA	0	19
ISLAS BALEARES	0	25
PAIS VASCO	43	225
PRINCIPADO DE ASTURIAS	0	74
CASTILLA Y LEON	0	84
MADRID	0	234
NAVARRA	1	88
COMUNIDAD VALENCIANA	0	227
CEUTA	0	23
MELILLA	59	59
TOTAL	235	2.580



DISTRIBUCIÓN DE FICHEROS PUBLICOS DE OTRAS PERSONAS JURIDICO-PUBLICAS

	1997	TOTAL
CAMARAS DE COMERCIO, INDUSTRIA Y NAVEGACION	0	187
UNIVERSIDADES	92	225
OTROS	0	39
T O T A L	92	451

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	
	1997	TOTAL	1997	TOTAL
ANDALUCIA	**29**	**653**	**109**	**5.284**
ALMERIA	2	104	2	950
CADIZ	4	40	23	261
CORDOBA	7	54	11	221
GRANADA	5	168	12	1.182
HUELVA	1	85	3	1.150
JAEN	3	76	28	432
MALAGA	4	36	13	365
SEVILLA	3	90	17	723
ARAGON	**3**	**413**	**7**	**1.890**
HUESCA	3	143	7	486
TERUEL	0	37	0	128
ZARAGOZA	0	233	0	1.276
ASTURIAS	**15**	**44**	**71**	**268**
ILLES BALEARS	**1**	**61**	**12**	**602**
CANARIAS	**9**	**52**	**44**	**309**
PALMAS, LAS	5	22	29	156
SANTA CRUZ DE TENERIFE	4	30	15	153
CANTABRIA	**7**	**38**	**30**	**168**
CASTILLA-LA MANCHA	**6**	**335**	**24**	**1.817**
ALBACETE	1	72	4	347
CIUDAD REAL	1	107	2	557
CUENCA	1	81	7	549
GUADALAJARA	1	10	2	56
TOLEDO	2	65	9	308
CASTILLA Y LEON	**15**	**495**	**62**	**2.171**
AVILA	1	5	2	15
BURGOS	2	91	7	318
LEON	0	163	0	801
PALENCIA	1	18	4	76
SALAMANCA	9	80	39	338
SEGOVIA	0	14	0	103
SORIA	1	8	5	27
VALLADOLID	0	81	0	336
ZAMORA	1	35	5	157

CATALUÑA	**29**	**410**	**331**	**2.360**
BARCELONA	19	172	281	1.221
GIRONA	4	53	26	335
LLEIDA	4	103	16	388
TARRAGONA	2	82	8	416
COMUNIDAD VALENCIANA	**17**	**305**	**79**	**2.133**
ALICANTE	3	136	15	1.182
CASTELLON DE LA PLANA	0	35	0	225
VALENCIA	14	134	64	726
EXTREMADURA	**4**	**183**	**23**	**1.536**
BADAJOZ	0	154	0	1.381
CACERES	4	29	23	155
GALICIA	**14**	**208**	**59**	**839**
A CORUÑA	6	80	34	402
LUGO	3	35	8	142
OURENSE	4	33	15	124
PONTEVEDRA	1	60	2	171
RIOJA, LA	**3**	**30**	**19**	**131**
MADRID	**9**	**48**	**118**	**628**
MURCIA	**2**	**34**	**18**	**382**
NAVARRA	**1**	**78**	**7**	**432**
PAIS VASCO	**16**	**176**	**102**	**1.420**
ALAVA	2	39	15	181
GUIPUZCOA	6	65	37	724
VIZCAYA	8	72	50	515
CEUTA	**0**	**0**	**0**	**0**
MELILLA	**0**	**0**	**0**	**0**

FICHEROS PRIVADOS INSCRITOS DISTRIBUIDOS POR COMUNIDADES AUTÓNOMAS Y PROVINCIAS

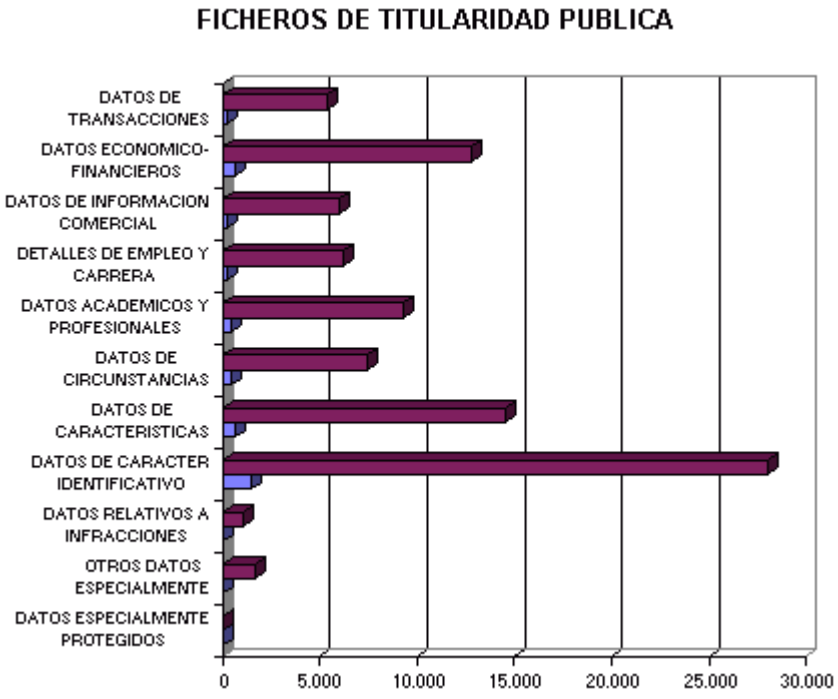
	EMPRESAS		FICHEROS	
	1997	TOTAL	1997	TOTAL
ANDALUCIA	**50**	**8.967**	**91**	**16.891**
ALMERIA	1	409	1	803
CADIZ	10	1.624	39	2.539
CORDOBA	6	1.074	7	2.413
GRANADA	4	725	4	1.386
HUELVA	1	616	1	998
JAEN	1	820	1	1.739
MALAGA	12	1.993	13	3.377
SEVILLA	16	1.713	25	3.726
ARAGON	**45**	**7.962**	**64**	**12.988**
HUESCA	1	1.800	1	2.509
TERUEL	2	572	2	892
ZARAGOZA	42	5.595	61	9.587
ASTURIAS	**19**	**1.921**	**19**	**3.551**
ILLES BALEARS	**8**	**1.205**	**12**	**2.865**
CANARIAS	**12**	**1.202**	**16**	**2.212**
PALMAS, LAS	8	692	9	1.279
SANTA CRUZ DE TENERIFE	4	513	7	933
CANTABRIA	**7**	**556**	**14**	**1.221**
CASTILLA-LA MANCHA	**5**	**2.952**	**24**	**5.156**
ALBACETE	2	909	7	1.404
CIUDAD REAL	0	611	0	1.093
CUENCA	0	521	0	874
GUADALAJARA	2	223	16	525
TOLEDO	1	688	1	1.260
CASTILLA Y LEON	**13**	**4.496**	**16**	**8.311**
AVILA	1	195	1	348
BURGOS	2	1.261	3	2.030
LEON	1	638	5	1.210
PALENCIA	0	232	0	452
SALAMANCA	1	530	2	1.256
SEGOVIA	1	280	1	485
SORIA	0	240	0	389
VALLADOLID	4	891	4	1.597
ZAMORA	0	235	0	544
CATALUÑA	**196**	**30.017**	**410**	**54.990**

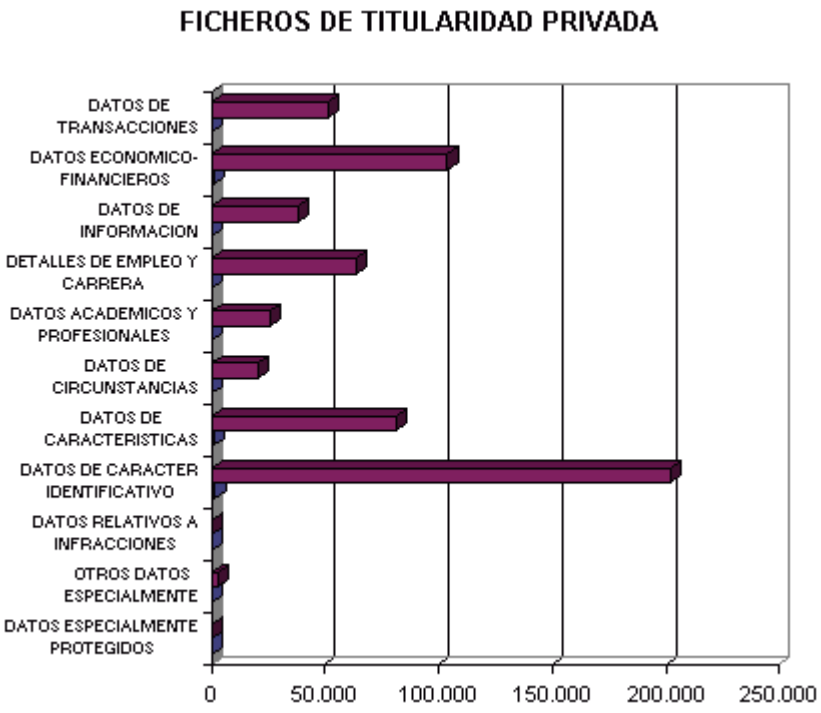
	EMPRESAS		FICHEROS	
	1997	TOTAL	1997	TOTAL
COMUNIDAD VALENCIANA	**50**	**14.271**	**70**	**23.586**
ALICANTE	19	5.630	32	8.998
CASTELLON DE LA PLANA	4	2.358	5	4.026
VALENCIA	27	6.289	33	10.564
EXTREMADURA	**69**	**1.991**	**90**	**3.375**
BADAJOZ	65	1.552	67	2.450
CACERES	4	440	23	925
GALICIA	**16**	**6.398**	**66**	**11.537**
A CORUÑA	8	3.336	32	5.888
LUGO	1	856	1	1.334
OURENSE	2	561	3	1.057
PONTEVEDRA	5	1.649	30	3.258
RIOJA, LA	**2**	**1.667**	**2**	**3.079**
MADRID	**348**	**16.126**	**763**	**36.817**
MURCIA	**11**	**2.748**	**11**	**4.524**
NAVARRA	**9**	**1.693**	**15**	**3.185**
PAIS VASCO	**40**	**3.643**	**73**	**7.289**
ALAVA	3	525	29	1.075
GUIPUZCOA	8	1.828	12	3.621
VIZCAYA	29	1.297	32	2.593
CEUTA	**1**	**52**	**4**	**115**
MELILLA	**0**	**35**	**0**	**53**

DISTRIBUCIÓN DE FICHEROS SEGÚN LA TIPOLOGÍA DE DATOS QUE CONTIENEN

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1997	TOTAL	1997	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	5	58	3	308
OTROS DATOS ESPECIALMENTE PROTEGIDOS	82	1.671	113	3.414
DATOS RELATIVOS A INFRACCIONES	76	1.107	---	---
DATOS DE CARACTER IDENTIFICATIVO	1.522	27.969	1.760	201.835
DATOS DE CARACTERISTICAS PERSONALES	709	14.500	880	81.030
DATOS DE CIRCUNSTANCIAS SOCIALES	425	7.444	353	20.744
DATOS ACADEMICOS Y PROFESIONALES	463	9.250	310	25.694
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIV/	297	6.235	573	64.069
DATOS DE INFORMACION COMERCIAL	273	6.046	293	38.280
DATOS ECONOMICO-FINANCIEROS	630	12.835	911	103.903
DATOS DE TRANSACCIONES	237	5.407	461	51.790

--- No aplicable a esta titularidad





FICHEROS INSCRITOS CON DATOS SENSIBLES

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1997	TOTAL	1997	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	**5**	**58**	**3**	**308**
Ideología	5	38	2	121
Creencias	1	19	0	38
Religión	1	13	1	174
OTROS DATOS ESPECIALMENTE PROTEGIDO	**82**	**1.671**	**113**	**3.436**
Origen Racial	9	75	0	147
Salud	79	1.648	113	3.249
Vida Sexual	7	342	0	132
DATOS RELATIVOS A INFRACCIONES	**76**	**1.107**	---	---
Infracciones Penales	37	693	---	---
Infracciones Administrativas	72	783	---	---

--- No aplicable a esta titularidad

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

DISTRIBUCIÓN DE FICHEROS PÚBLICOS SEGÚN SU FINALIDAD

	1997	TOTAL
GESTION TRIBUTARIA Y DE RECAUDACION	378	6.323
PROCEDIMIENTOS ADMINISTRATIVOS	334	7.926
GESTION DE ESTADISTICAS INTERNAS	291	7.584
GESTION ECONOMICA CON TERCEROS	250	5.680
PADRON	206	4.122
GESTION DE PERSONAL	193	3.994
OTRAS FINALIDADES	151	4.032
FUNCION ESTADISTICA PUBLICA	143	4.982
CONCESION Y GESTION DE PERMISOS Y LICENCIAS	117	3.104
GESTION DEUDA PUBLICA Y TESORERIA	87	2.339
PRESTACIONES DE ASISTENCIA SOCIAL	78	1.506
OTRAS ENSEÑANZAS, BECAS Y AYUDAS A ESTUDIANTES	76	929
RELACIONES LABORALES Y CONDICIONES DE TRABAJO	74	1.294
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD	73	1.760
FORMACION DE PERSONAL	68	1.316
GESTION DE CATASTROS INMOBILIARIOS RUSTICOS Y URBANOS	67	1.770
EDUCACION UNIVERSITARIA	67	425
SERVICIO MILITAR	62	2.080
SEGURIDAD Y CONTROL INTERNO	62	1.899
GESTION SANCIONADORA	61	2.182
PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONOMICAS	61	1.817
SERVICIOS SOCIALES DE LA TERCERA EDAD	60	710
OTROS SERVICIOS SOCIALES	58	1.075
ACTUACIONES POLICIALES	53	2.003
GESTION Y CONTROL SANITARIO	53	1.125
PROMOCION Y GESTION DE EMPLEO	52	734
INVESTIGACIONES CIENTIFICAS O MEDICAS Y ACTIVIDADES ANALOGA	48	924
PUBLICACIONES	48	537
PROCEDIMIENTOS JUDICIALES	47	795
EDUCACION INFANTIL Y PRIMARIA	42	701
FORMACION PROFESIONAL	40	1.013
DEPORTES	37	843
SERVICIOS SOCIALES A MINUSVALIDOS	35	1.013
AYUDAS ACCESO A VIVIENDA	35	997
EDUCACION SECUNDARIA	35	610
CONTROL DE INCOMPATIBILIDADES	33	581
NACIONALIDAD	32	924
EDUCACION ESPECIAL	30	337
FOMENTO Y APOYO A ACTIVIDADES ARTISTICAS Y CULTURALES	30	294
PROTECCION DEL MENOR	28	590
FORMACION PROFESIONAL Y ESCUELA OFICIAL DE IDIOMAS	27	632
PRESTACIONES A LOS DESEMPLEADOS	26	940

	1997	TOTAL
HISTORIAL CLINICO	25	589
PRESTACIONES DE GARANTIA SALARIAL	22	239
PROMOCION Y SERVICIOS A LA JUVENTUD	21	623
ACCION SOCIAL EN FAVOR DEL PERSONAL DE ADMONES. PUBLICAS	18	760
ENCUESTAS SOCIOLOGICAS Y DE OPINION	14	132
SEGURIDAD VIAL	13	1.287
PRESTACION SOCIAL SUSTITUTORIA	13	820
PROMOCION Y SERVICIOS A LA MUJER	13	560
ACCION EN FAVOR DE MIGRANTES	13	376
PROTECCION CIVIL	11	1.617
INSPECCION Y CONTROL DE SEGURIDAD Y PROTECCION SOCIAL	11	647
PROTECCION A LOS CONSUMIDORES	9	179
RELACIONES COMERCIALES CON EL EXTERIOR	8	391
CONTROL DE PATRIMONIO DE ALTOS CARGOS PUBLICOS	5	216
GESTION Y CONTROL DE CENTROS E INSTITUCIONES PENITENCIARIAS	4	315
PROTECCION PATRIMONIO HISTORICO ARTISTICO	3	91
TRABAJOS PENITENCIARIOS	2	269
INDULTOS	1	261
DEFENSA DE LA COMPETENCIA	1	20
REGULACION DE MERCADOS FINANCIEROS	0	28

DISTRIBUCIÓN DE FICHEROS PRIVADOS SEGÚN SU FINALIDAD

	1997	TOTAL
GESTION DE CLIENTES	640	63.824
GESTION CONTABLE, FISCAL Y ADMINISTRATIVA	636	133.123
OBTENCION DE ESTADISTICAS DIVERSAS	608	54.287
GESTION DE COBROS Y PAGOS	575	87.758
PUBLICIDAD PROPIA	456	19.117
HISTORICOS DE RELACIONES COMERCIALES	292	31.847
GESTION DE PERSONAL	287	52.862
SEGURIDAD Y CONTROL INTERNO	218	9.944
PROSPECCIONES DE MERCADO	208	6.731
INFORMACION SOBRE LA SOLVENCIA PATRIMONIAL Y CREDIT	172	3.444
OTRAS FINALIDADES	168	8.403
ENCUESTAS DE OPINION	147	2.787
PUBLICIDAD PARA TERCEROS	124	2.612
AUDITORIAS, ASESORIAS Y SERVICIOS RELACIONADOS	105	13.365
SEGUROS DE VIDA Y SALUD	88	5.375
OTRO TIPO DE SEGUROS	78	5.492
SELECCION DE PERSONAL	75	3.432
GESTION ADMINISTRATIVA DE LOS INTEGRANTES DE CLUBES	70	2.035
GESTION DE TARJETAS DE CREDITO Y SIMILARES	66	1.620
CUENTA DE CREDITO	63	4.279
PRESTACIONES SOCIALES	62	13.659
CUENTA DE DEPOSITO	57	2.332
GESTION Y CONTROL SANITARIO	51	1.653
OTROS SERVICIOS FINANCIEROS	50	3.974
INVESTIGACIONES CIENTIFICAS Y MEDICAS	45	676
HISTORIAL CLINICO	44	1.845
FORMACION PROFESIONAL	42	1.430
OTRAS ENSEÑANZAS	36	1.346
SERVICIOS DE TELECOMUNICACION	36	1.051
INVESTIGACION	33	433
REGISTRO DE ACCIONES Y OBLIGACIONES	29	2.107
GESTION DE PATRIMONIOS	29	2.008
SEGURIDAD	29	639
GESTION DE FONDOS DE PENSIONES Y SIMILARES	27	2.201
MEDIOS DE COMUNICACION SOCIAL	22	434
EDUCACION UNIVERSITARIA	13	720
EDUCACION SECUNDARIA	13	518
EDUCACION INFANTIL PRIMARIA	11	453
RESERVA Y EMISION DE BILLETES	9	304
EDUCACION ESPECIAL	7	283
INVESTIGACIONES PRIVADAS A PERSONAS	5	81

DISTRIBUCIÓN DE EMPRESAS INSCRITAS SEGÚN LA CLASIFICACIÓN NACIONAL DE ACTIVIDADES ECONÓMICAS DE PERTENENCIA

	C N A E	1997	TOTAL
1	AGRICULTURA, GANADERIA, CAZA Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	11	2.022
2	SELVICULTURA, EXPLOTACION FORESTAL Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	0	98
5	PESCA, ACUICULTURA Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	0	251
10	EXTRACCION Y AGLOMERACION DE ANTRACITA, HULLA, LIGNITO Y TURBA	1	88
11	EXTRACCION DE CRUDOS DE PETROLEO Y GAS NATURAL; ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS EXPLOTACIONES PETROLIFERAS Y DE GAS, EXCEPTO ACTIVIDADES DE PROSPECCION	1	115
12	EXTRACCION DE MINERALES DE URANIO Y TORIO	0	30
13	EXTRACCION DE MINERALES METALICOS	0	38
14	EXTRACCION DE MINERALES NO METALICOS NI ENERGETICOS	0	310
15	INDUSTRIA DE PRODUCTOS ALIMENTICIOS Y BEBIDAS	20	2.831
16	INDUSTRIA DEL TABACO	3	45
17	INDUSTRIA TEXTIL	3	1.232
18	INDUSTRIA DE LA CONFECCION Y DE LA PELETERIA	3	679
19	PREPARACION, CURTIDO Y ACABADO DEL CUERO; FABRICACION DE ARTICULOS DE MARROQUINERIA Y VIAJE; ARTICULOS DE GUARNICIONERIA, TALABARTERIA Y ZAPATERI	1	757
20	INDUSTRIA DE LA MADERA Y DEL CORCHO, EXCEPTO MUEBLES; CESTERIA Y ESPARTER	0	857
21	INDUSTRIA DEL PAPEL	2	438
22	EDICION, ARTES GRAFICAS Y REPRODUCCION DE SOPORTES GRABADOS	38	1.512
23	COQUERIAS, REFINO DE PETROLEO TRATAMIENTO DE COMBUSTIBLES NUCLEARES	1	62
24	INDUSTRIA QUIMICA	18	1.087
25	FABRICACION DE PRODUCTOS DE CAUCHO Y MATERIAS PLASTICAS	6	949
26	FABRICACION DE OTROS PRODUCTOS MINERALES NO METALICOS	5	1.048
27	METALURGIA	9	462
28	FABRICACION DE PRODUCTOS METALICOS, EXCEPTO MAQUINARIA Y EQUIPO	4	1.537
29	INDUSTRIA DE LA CONSTRUCCION DE MAQUINARIA Y EQUIPO MECANICO	3	931
30	FABRICACION DE MAQUINAS DE OFICINA Y EQUIPOS INFORMATICOS	1	77
31	FABRICACION DE MAQUINARIA Y MATERIAL ELECTRICO	5	781
32	FABRICACION DE MATERIAL ELECTRONICO; FABRICACION DE EQUIPO Y APARATOS DE RADIO, TELEVISION Y COMUNICACIONES	1	323
33	FABRICACION DE EQUIPO E INSTRUMENTOS MEDICO-QUIRURGICOS, DE PRECISION, OPTICOS Y RELOJERIA	2	174
34	FABRICACION DE VEHICULOS DE MOTOR, REMOLQUES Y SEMIRREMOLQUES	3	331
35	FABRICACION DE OTRO MATERIAL DE TRANSPORTE	0	130
36	FABRICACION DE MUEBLES; OTRAS INDUSTRIAS MANUFACTURERAS	5	1.423
37	RECICLAJE	0	73

	C N A E	1997	TOTAL
40	PRODUCION Y DISTRIBUCION DE ENERGIA ELECTRICA, GAS, VAPOR Y AGUA CALIENTE	5	189
41	CAPTACION, DEPURACION Y DISTRIBUCION DE AGUA	8	233
45	CONSTRUCCION	29	6.364
50	VENTA, MANTENIMIENTO Y REPARACION DE VEHICULOS DE MOTOR, MOTOCICLETAS Y CICLOMOTORES; VENTA AL POR MENOR DE COMBUSTIBLE PARA VEHICULOS DE MOTOR	32	6.062
51	COMERCIO AL POR MAYOR E INTERMEDIARIOS DEL COMERCIO, EXCEPTO DE VEHICULOS DE MOTOR Y MOTOCICLETAS	47	11.858
52	COMERCIO AL POR MENOR, EXCEPTO EL COMERCIO DE VEHICULOS DE MOTOR, MOTOCICLETAS Y CICLOMOTORES; REPARACION DE EFECTOS PERSONALES Y ENSERES DOMESTICOS	69	8.918
55	HOSTELERIA	17	3.685
60	TRANSPORTE TERRESTRE; TRANSPORTE POR TUBERIAS	8	1.870
61	TRANSPORTE MARITIMO, DE CABOTAJE Y POR VIAS DE NAVEGACION INTERIORES	9	1.749
62	TRANSPORTE AEREO Y ESPACIAL	5	96
63	ACTIVIDADES ANEXAS A LOS TRANSPORTES; ACTIVIDADES DE AGENCIAS DE VIAJES	12	1.194
64	CORREOS Y TELECOMUNICACIONES	14	866
65	INTERMEDIACION FINANCIERA, EXCEPTO SEGUROS Y PLANES DE PENSIONES	62	556
66	SEGUROS Y PLANES DE PENSIONES, EXCEPTO SEGURIDAD SOCIAL OBLIGATORIA	40	1.112
67	ACTIVIDADES AUXILIARES A LA INTERMEDIACION FINANCIERA	21	2.426
70	ACTIVIDADES INMOBILIARIAS	43	4.125
71	ALQUILER DE MAQUINARIA Y EQUIPO SIN OPERARIO, DE EFECTOS PERSONALES Y ENSERES DOMESTICOS	5	466
72	ACTIVIDADES INFORMATICAS	31	1.690
73	INVESTIGACION Y DESARROLLO	4	211
74	OTRAS ACTIVIDADES EMPRESARIALES	115	9.651
75	ADMINISTRACION PUBLICA, DEFENSA Y SEGURIDAD SOCIAL OBLIGATORIA	1	29
80	EDUCACION	12	1.364
85	ACTIVIDADES SANITARIAS Y VETERINARIAS, SERVICIO SOCIAL	25	
90	ACTIVIDADES DE SANEAMIENTO PUBLICO	0	124
91	ACTIVIDADES ASOCIATIVAS	58	2.244
92	ACTIVIDADES RECREATIVAS, CULTURALES Y DEPORTIVAS	71	1.777
93	ACTIVIDADES DIVERSAS DE SERVICIOS PERSONALES	12	1.521
95	HOGARES QUE EMPLEAN PERSONAL DOMESTICO	0	0
99	ORGANISMOS EXTRATERRITORIALES	0	0
	OTROS	0	24.998

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

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
SOPORTE	**1.997**	**TOTAL**	**1.997**	**TOTAL**
SOPORTE PAPEL	1.433	26.622	1.475	163.659
SOPORTE INFORMATICO/MAGNETICO	465	10.970	450	28.379
VIA TELEMATICA	40	2.967	196	5.096
OTROS SOPORTES	37	3.027	207	33.586
PROCEDENCIA DE LOS DATOS	**1.997**	**TOTAL**	**1.997**	**TOTAL**
ENTIDAD PRIVADA	111	3.011	245	25.615
ADMINISTRACIONES PUBLICAS	482	10.285	170	2.511
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	1.397	26.266	1.463	181.467
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	94	3.849	115	4.068
FUENTES ACCESIBLES AL PUBLICO	65	2.719	245	8.777
PROCEDIMIENTO DE RECOGIDA	**1.997**	**TOTAL**	**1.997**	**TOTAL**
ENCUESTAS O ENTREVISTAS	150	3.708	478	43.680
DECLARACIONES O FORMULARIOS	1.266	24.144	901	84.938
REGISTROS PUBLICOS	243	6.425	129	3.778
TRANSMISION ELECTRONICA DE DATOS	93	4.467	181	3.510
DIRECTORIOS TELEFONICOS, COMERCIALES, CATALOGOS, MEMORIA	27	1.815	165	9.022
OTROS PROCEDIMIENTOS DE RECOGIDA	129	2.686	367	68.924

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

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1997	**TOTAL**	**1997**	**TOTAL**
EXISTE CONSENTIMIENTO DE LOS AFECTADOS	221	6.439	302	16.953
EXISTE UNA RELACION JURIDICA CUYO DESARROLLO, CONTROL Y CUMPLIMIENTO IMPLICA NECESARIAMENTE LA CONEXION DEL FICHERO CON FICHEROS DE TERCEROS	164	3.678	155	12.720
EXISTE UNA NORMA REGULADORA QUE LAS AUTORIZA	732	9.610	218	19.603
SE TRATA DE DATOS RECOGIDOS DE FUENTES ACCESIBLES AL PUBLICO	67	4.669	38	2.294
CORRESPONDEN A COMPETENCIAS IDENTICAS O QUE VERSAN SOBRE LAS MISMAS MATERIAS, EJERCIDAS POR OTRAS ADMINISTRACIONES PUBLICAS	345	10.000	---	---
SON DATOS OBTENIDOS O ELABORADOS CON DESTINO A OTRA ADMINISTRACION PUBLICA	269	8.878	---	---
TOTAL FICHEROS INSCRITOS CON CESIONES	**811**	**16.368**	**467**	**34.436**

--- No aplicable a esta titularidad

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.

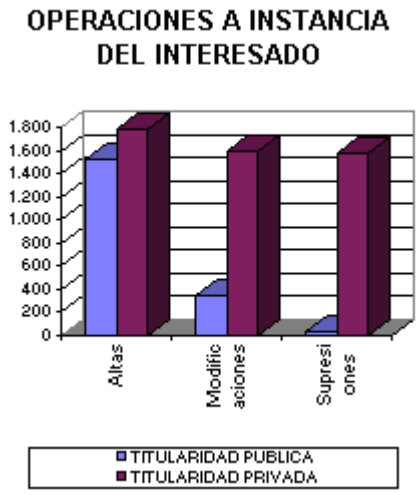
SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LOS FICHEROS QUE DECLARAN TRANSFERENCIAS INTERNACIONALES DE DATOS

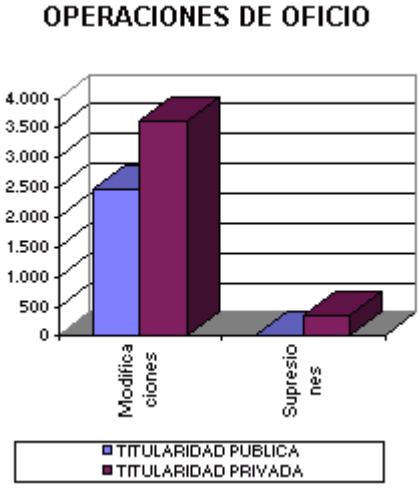
	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1997	TOTAL	1997	TOTAL
SE AMPARA EN TRATADO O CONVENIO DEL QUE ESPAÑA FORMA PARTE	4	39	0	17
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	1	9	0	0
TIENE POR OBJETO INTERCAMBIAR DATOS DE CARACTER MEDICO Y AS LO EXIGE EL TRATAMIENTO DEL AFECTADO O LA INVESTIGACION EPIDEMIOLOGICA	2	5	1	7
SE REFIERE A TRANSFERENCIAS DINERARIAS	1	15	1	53
SE EFECTUA CON DESTINO A ALGUN PAIS DE LOS CITADOS EN EL REGLAMENTO CON NIVEL DE PROTECCION EQUIPARABLE	5	44	100	772
SE EFECTUA CON AUTORIZACION DEL DIRECTOR DE LA AGENCIA	0	0	33	128
TOTAL FICHEROS CON TRANSFERENCIAS INTERNACIONALES	**6**	**48**	**111**	**871**

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.

RESUMEN DE OPERACIONES REALIZADAS DURANTE EL AÑO 1997 SOBRE FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS SEGÚN LA TITULARIDAD Y TIPO DE OPERACIÓN

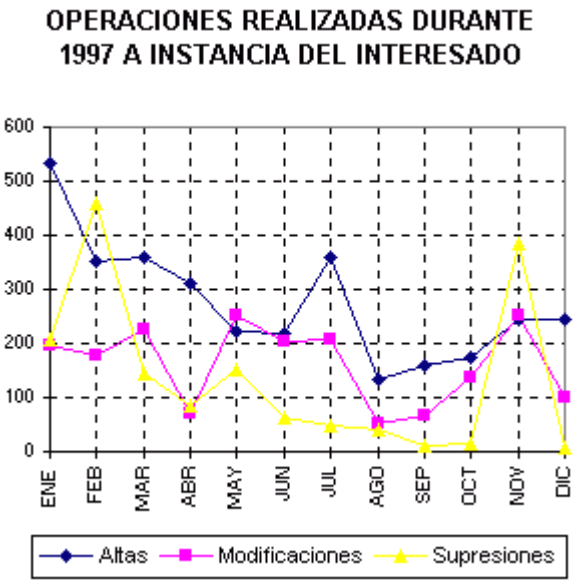
	TITULARIDAD PUBLICA	TITULARIDAD PRIVADA	TOTAL
OPERACIONES A INSTANCIA DEL RESPONSAB			
Altas	1.523	1.789	3.312
Modificaciones	344	1.597	1.941
Supresiones	39	1.571	1.610
T O T A L	1.906	4.957	6.863
OPERACIONES REALIZADAS DE OFICIO			
Altas	0	0	0
Modificaciones	2.457	3.625	6.082
Supresiones	11	350	361
T O T A L	2.468	3.975	6.443
TOTALES	**4.374**	**8.932**	**13.306**

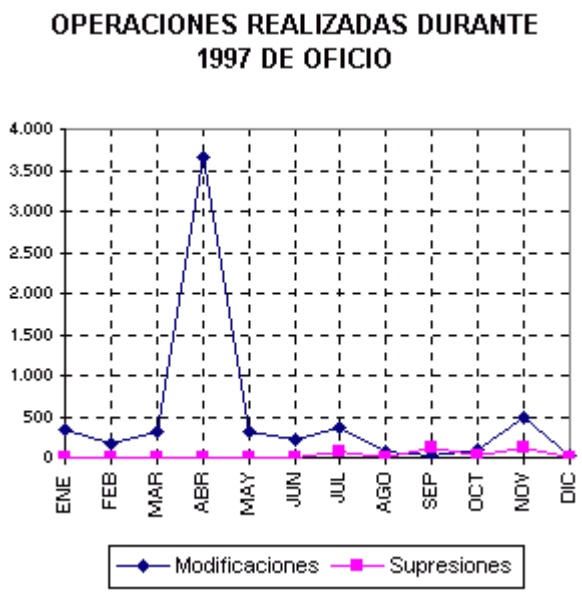




RESUMEN DE OPERACIONES REALIZADAS DURANTE EL AÑO 1997 SOBRE FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS POR MESES

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
OPERACIONES A INSTANCIA DEL INTERESADO													
Altas	533	351	360	310	222	218	361	134	158	173	246	246	3.312
Modificaciones	196	179	227	71	252	203	207	52	66	136	251	101	1.941
Supresiones	207	458	143	84	151	62	48	40	10	13	385	9	1.610
T O T A L	936	988	730	465	625	483	616	226	234	322	882	356	6.863
OPERACIONES DE OFICIO													
Altas	0	0	0	0	0	0	0	0	0	0	0	0	0
Modificaciones	332	166	307	3.667	307	227	363	71	29	95	483	35	6.082
Supresiones	2	0	0	7	1	1	71	12	121	22	116	8	361
T O T A L	334	166	307	3.674	308	228	434	83	150	117	599	43	6.443
T O T A L E S	**1.270**	**1.154**	**1.037**	**4.139**	**933**	**711**	**1.050**	**309**	**384**	**439**	**1.481**	**399**	**13.306**





4. LA INSPECCIÓN DE DATOS.

4. 1. INTRODUCCIÓN

La Ley Orgánica 5/1992, en su artículo 39, dota a la Agencia de Protección de Datos de la Potestad de Inspección. Por su parte, el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, en su artículo 27 establece que la Inspección de Datos es el órgano de la Agencia al cual competen las funciones inherentes al ejercicio de la Potestad de Inspección que el artículo 39 de la Ley Orgánica 5/1992, atribuye a la Agencia.

Asimismo se estatuye que los funcionarios que ejerzan funciones inspectoras tendrán la consideración de autoridad pública en el desempeño de sus funciones y 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, detallándose a continuación, en los artículos 28 y 29 las funciones inspectoras e instructoras de la Inspección de Datos, que se pueden resumir de la siguiente forma:

- Efectuar inspecciones, periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera ficheros, de titularidad pública o privada, en los locales en los que se hallen los ficheros y los equipos informáticos correspondientes.

- Examinar los soportes de información que contengan los datos personales, los equipos físicos y los sistemas de transmisión y acceso a los datos y requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto.

- Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992.

- Requerir la exhibición de cualesquiera documentos pertinentes y el envío de toda información precisa para el ejercicio de las funciones inspectoras.

- El ejercicio de los actos de instrucción relativos a la adopción de las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora de la Agencia con relación a los responsables de los ficheros privados en el marco de un Procedimiento Sancionador.

Además, se dispone que el responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario actuante de la autorización expedida por el Director de la Agencia.

Es, por lo tanto, la Inspección de Datos, un elemento fundamental en el régimen de garantías establecido por la Ley Orgánica 5/1992 para la defensa de la privacidad de los ciudadanos, puesto que a ella corresponde comprobar in situ si los tratamientos realizados por los responsables de ficheros respetan lo establecido en la ley, ostentando, para ello,

amplias competencias para la revisión de los equipos y sistemas informáticos; con el lógico contrapeso de un estricto deber de secreto de los funcionarios que la componen respecto de la información que pudieran conocer en el curso de sus actuaciones.

Por lo que se refiere a la información de carácter general relativa a la actividad de la Inspección, a lo largo del año 1997 se iniciaron, por parte de la misma, 682 Expedientes de Investigación con objeto de determinar tanto si se habían producido infracciones a lo establecido en la Ley Orgánica 5/1992 como para tutelar a aquellos ciudadanos que consideraban que se les había impedido ejercer los derechos de acceso, rectificación o cancelación que la ley les otorga.

De los 682 expedientes arriba mencionados, 134 correspondieron a actuaciones de oficio y 548 fueron motivados por la recepción de escritos de denuncia o reclamaciones de tutelas de derechos.

En los Gráficos I, II y III podemos apreciar de forma detallada, tanto la distribución geográfica como por sectores de acti - vidad de los expedientes iniciados.

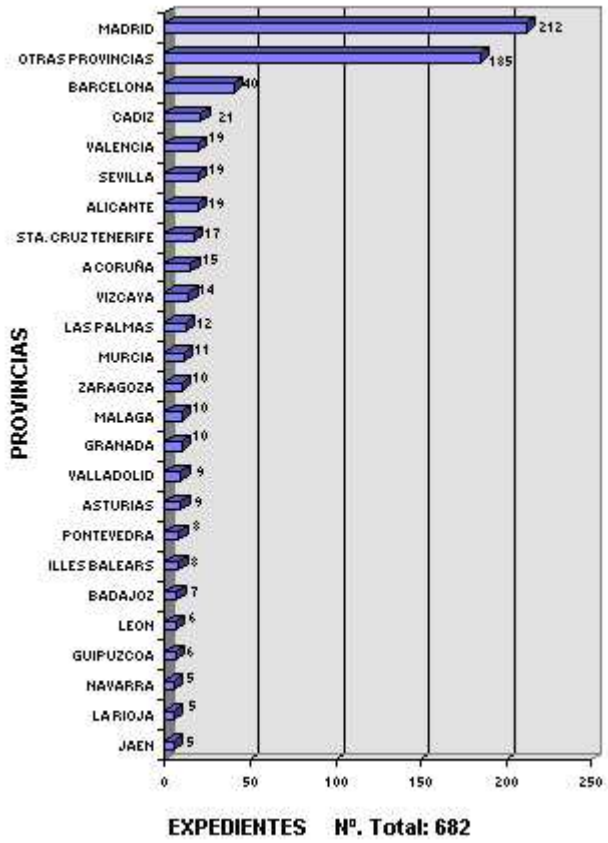


GRÁFICO I. EXPEDIENTES INICIADOS POR PROVINCIA DEL DENUNCIANTE.

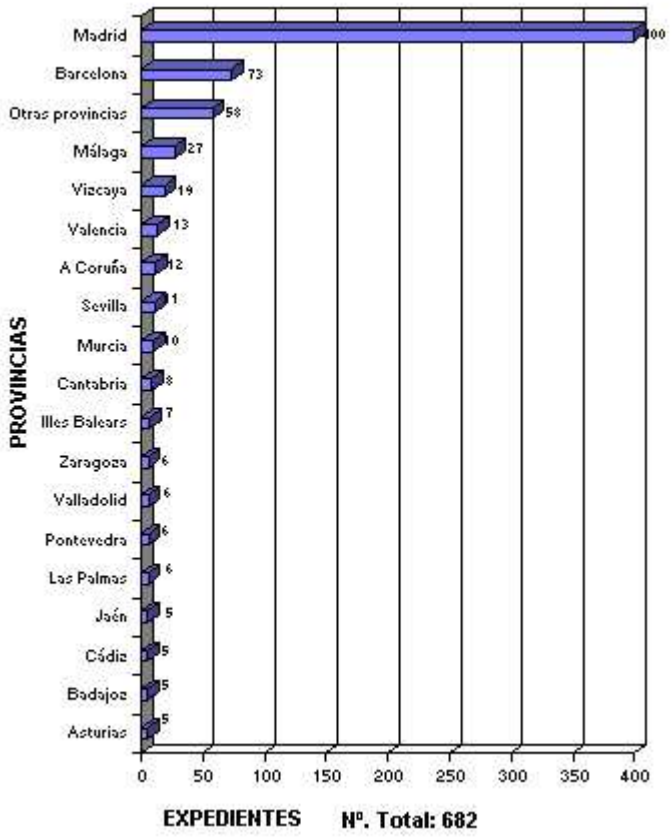


GRÁFICO II. EXPEDIENTES INICIADOS POR PROVINCIA DEL DENUNCIADO.

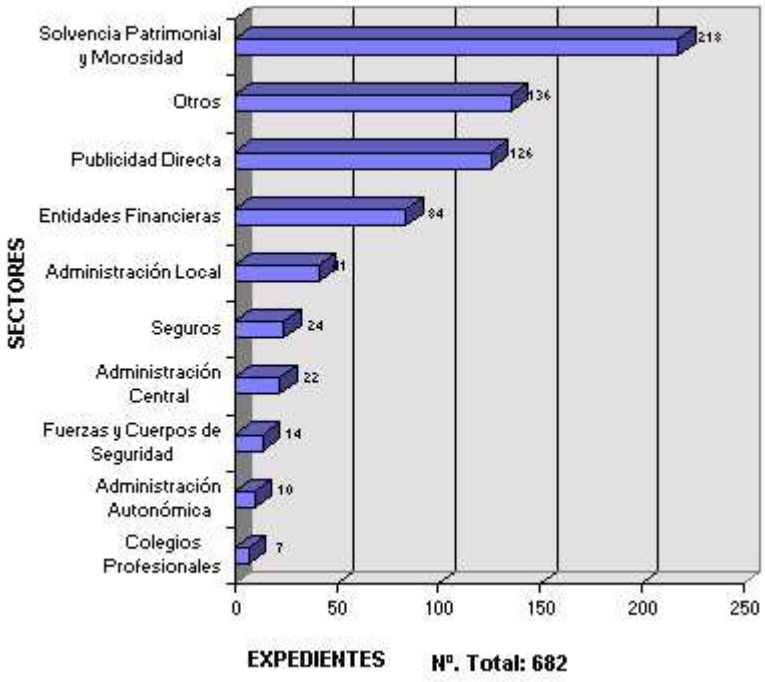


GRÁFICO III. EXPEDIENTES INICIADOS POR SECTORES.

Si establecemos una comparación con las cifras del año anterior, podremos observar que, aparentemente el número de expedientes abiertos ha disminuido (682 frente a 922), pero si tenemos en cuenta que, como ya se especificó en la Memoria de 1996, de los 922, 429 correspondieron a un Ejercicio del Derecho de Acceso ejercitado en bloque por los miembros de una Cooperativa que por su carácter de derecho personal requirió la apertura de un expediente por cada afectado, tenemos que, si consideramos los 429 expedientes antes mencionados como uno, realmente se ha pasado de 494 a 682 expedientes iniciados, lo que supone un incremento de casi un 40% respecto a 1996, siendo oportuno mencionar en este punto que los efectivos de la Inspección en 1997 fueron los mismos que en 1996, debiendo asumir, por lo tanto, un fuerte aumento en la carga de trabajo.

Respecto a la distribución geográfica de los expedientes iniciados, que se muestra en los Gráficos I y II, poco hay que decir que no se haya dicho ya en anteriores Memorias. Continúa existiendo un gran desequilibrio entre Madrid y el resto de provincias, persistiendo los factores que mencionábamos en 1996: el efecto de potenciación del conocimiento de la Agencia por razón de su sede y, en el caso de la distribución geográfica de los responsables de ficheros denunciados, constatar de nuevo que las empresas pertenecientes a aquellos sectores que provocan más denuncias ante la Agencia, tienen, mayoritariamente, su sede en Madrid.

Hecha esta salvedad, un estudio del Gráfico III confirma las tendencias ya observadas en años anteriores respecto de las preocupaciones fundamentales de los ciudadanos en relación con la protección de sus datos personales: los relativos a morosidad (a los que cabría unir una gran parte de los referidos a entidades financieras, ya que la mayor parte de ellos también se refieren a esta materia) y, a mucha distancia, en segundo lugar, la recepción de publicidad no deseada. También se confirma, como en años anteriores, el escaso número de denuncias recibidas relativas a datos especialmente protegidos, como los que pudieran contener ficheros con datos de sanidad, seguros o ficheros policiales.

En lo que respecta a la realización de inspecciones in situ, en el año 1997 se realizaron 375 frente a las 245 de 1996. Ello supone un incremento del 53% respecto al año anterior. Una vez más, no hay cambios respecto a los años precedentes: los ficheros sobre incumplimiento de obligaciones dinerarias y solvencia patrimonial y los dedicados a publicidad directa siguen recibiendo el mayor número de inspecciones en lógica correspondencia con la distribución sectorial de las denuncias.

En los Gráficos IV y V se puede apreciar de una forma más pormenorizada la distribución de inspecciones geográficamente y por sectores.

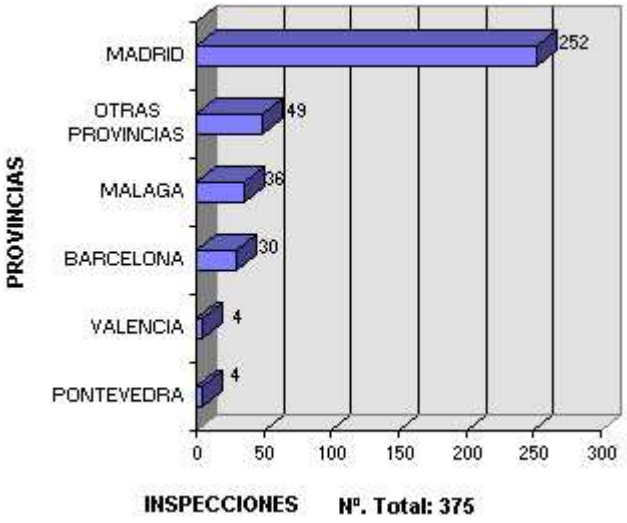


GRÁFICO IV. INSPECCIONES REALIZADAS POR PROVINCIAS.

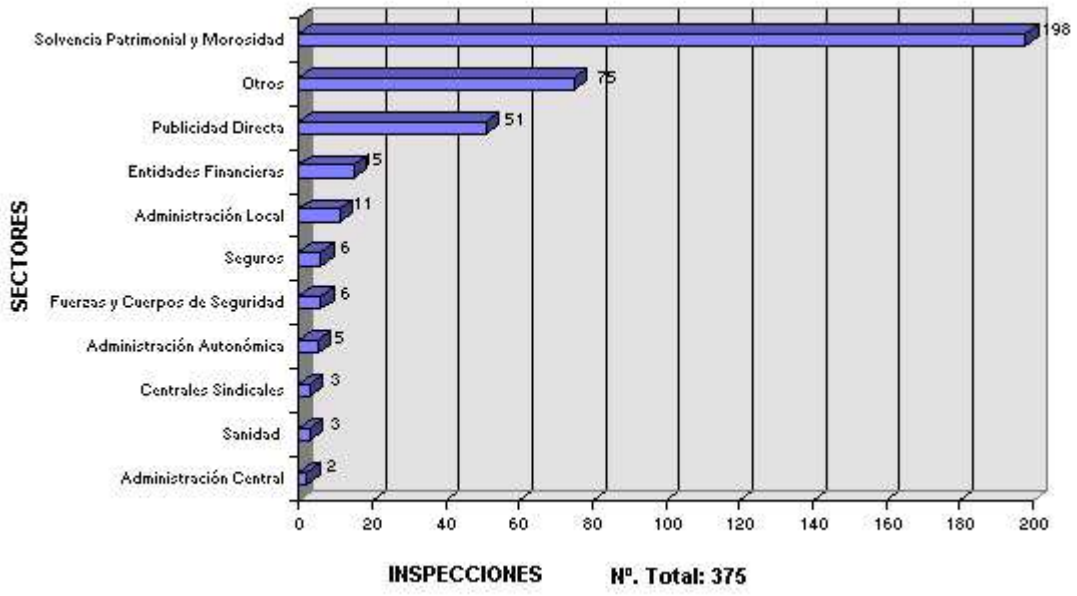


GRÁFICO V. INSPECCIONES REALIZADAS POR SECTORES.

Por lo que respecta a los Planes de Inspección sectoriales realizados de oficio por la Agencia en aras de un mejor conocimiento de los tratamientos realizados y los datos almacenados en determinados tipos de ficheros, el más importante llevado a cabo en 1997 se correspondió con la continuación del Plan de Inspección de ficheros policiales, en el marco del cual se procedió a revisar los archivos automatizados de doce Policías Locales: Barcelona, Benidorm, Bilbao, Ibiza, Lloret de Mar, Marbella, Madrid, Murcia, Sevilla, Valladolid, Vigo y Zaragoza.

Como consecuencia de las actividades de la Inspección, se procedió a la apertura de 202 Procedimientos Sancionadores frente a los 90 de 1996, casi un 125% más, así como a 6 Procedimientos de Infracción de Administraciones Públicas, uno más que en 1996.

Una vez más y a fuer de ser reiterativos, hemos de incidir en la polarización de los Procedimientos Sancionadores en torno a los sectores de solvencia patrimonial y morosidad y de publicidad directa y, geográficamente, en torno a Madrid y, a una gran distancia, Barcelona.

Por lo que se refiere a procedimientos sancionadores resueltos a lo largo de 1997, se produjeron 223 resoluciones, de las que 135 fueron sancionadoras (13 muy graves, 77 graves y 45 leves) y en 88 se declaró la no responsabilidad.

GRÁFICO VI. PROCEDIMIENTOS SANCIONADORES INICIADOS POR PROVINCIAS.

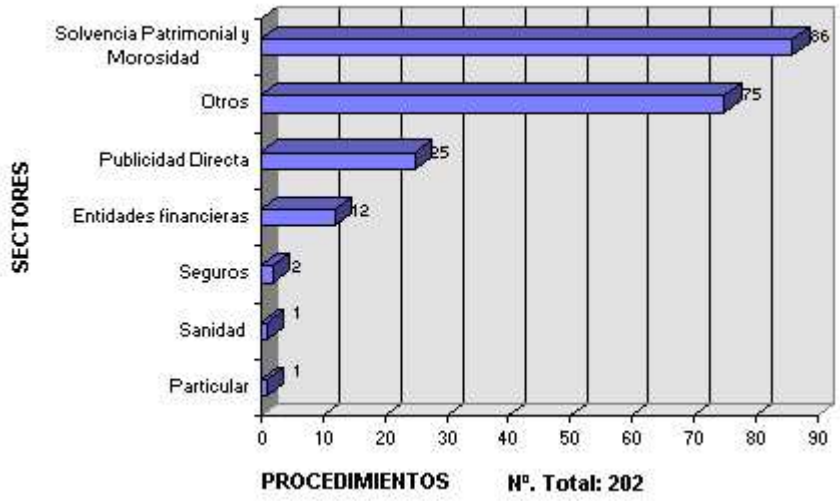


GRÁFICO VII. PROCEDIMIENTOS SANCIONADORES INICIADOS POR SECTORES.

También se procedió a la apertura de 113 Procedimientos de Tutela de Derechos derivados de las reclamaciones de los ciudadanos, de los que el 27% corresponden al ejercicio del derecho de acceso, el 8% al de rectificación y el 65% al de cancelación.

En los gráficos VIII y IX se plasman la distribución de los mismos por sectores y por provincias, no apartándose ninguna de ellas de lo mencionado hasta ahora.

GRÁFICO VIII. PROCEDIMIENTO DE TUTELA DE DERECHOS INICIADOS POR SECTORES.

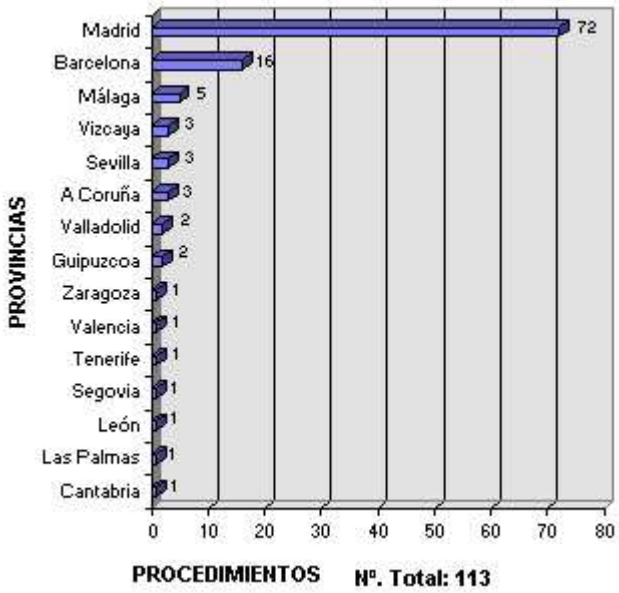


GRÁFICO IX. PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR PROVINCIAS.

4. 2. ANÁLISIS POR SECTORES DE ACTIVIDAD

Como en Memorias de años anteriores, una vez presentado el panorama general de lo que ha sido la actuación de la Inspección de Datos en 1997, pasaremos a analizar todos aquellos aspectos de relevancia que se han puesto de manifiesto en distintos sectores de actividad públicos y privados.

4. 2.1. ADMINISTRACIÓN GENERAL DEL ESTADO.

En primer lugar, debemos destacar que algunas de las organizaciones pertenecientes a este sector, disponen de los mayores ficheros automatizados que incluyen datos de carácter personal de ámbito nacional, no solamente respecto a su volumen, información concerniente a millones de españoles, sino también con respecto a la riqueza de su contenido y a los recursos tanto físicos como humanos necesarios para su tratamiento.

Durante 1997 se ha procedido a la apertura de 22 Expedientes de Investigación en este sector, lo que supone un aumento del 100% con respecto a los 11 del periodo anterior. La mayor parte de los expedientes han sido iniciados a instancias de los afectados, siendo tramitados dos de ellos por el procedimiento de Tutela de los Derechos. Sin embargo, en tres de ellos las reclamaciones han sido formuladas por organizaciones sindicales y una a iniciativa de la propia Agencia ante noticias aparecidas en los medios de comunicación.

No obstante, sigue siendo un número sorprendentemente bajo con respecto al número total de actuaciones llevadas a cabo por la Inspección de Datos de esta Agencia y en relación con el número de Organismos incluidos en este sector y al volumen de información que necesitan manejar para cumplir las funciones que tienen encomendadas.

Los organismos sobre los que se han centrado la mayor parte de las actuaciones han sido la Agencia Estatal de Administración Tributaria y la Tesorería General de la Seguridad Social, posiblemente las dos organizaciones públicas que disponen de mayor información acerca de los ciudadanos. Asimismo, otras administraciones objeto de investigación han sido:

* Ministerio de Educación y Cultura y Escuela Oficial de Idiomas.

* Cámaras Oficiales de Comercio, Industria y Navegación.

* Ministerio de Justicia.

* Ministerio de Asuntos Exteriores: Agencia Española de Cooperación Internacional.

* Ministerio de Economía y Hacienda: Parque Móvil Ministerial.

A continuación procederemos a analizar los casos objeto de investigación fijándonos en su naturaleza desde el punto de vista de protección de datos:

4.2.1.1. Cesión de datos.

Uno de los aspectos más comúnmente reflejados en los escritos presentados por los ciudadanos ante esta Agencia, ha sido la posible vulneración de la Ley Orgánica 5/1992, por parte de diversas instituciones debido a la cesión de datos personales incluidos en los ficheros de los que son responsables, sin el consentimiento de los afectados.

En primer lugar debemos hacer mención, entre otros, a lo establecido en el artículo 11.1 de la Ley Orgánica 5/1992, 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.

Las conclusiones obtenidas de las actuaciones previas efectuadas por la Inspección y relacionadas con el principio de cesión de datos las podemos agrupar, en función de los destinatarios de la cesión, en los siguientes apartados:

- **Jueces o Tribunales.** Esta es una de las excepciones al principio general del consentimiento previo del afectado, de acuerdo con el artículo 11.2 d) de la Ley Orgánica 5/1992, por lo que la cesión era acorde con la citada norma.

- **Cámaras de Comercio, Industria y Navegación.** En este caso la cesión se enmarcaba en lo dispuesto en el artículo 11.2 a) de la Ley Orgánica, que establece que, el consentimiento para la cesión de los datos personales no será preciso cuando una Ley prevea otra cosa.
Las Cámaras son corporaciones de derecho público con personalidad jurídica y plena capacidad de obrar para el cumplimiento de sus fines. Para la financiación de sus actividades las Cámaras dispondrán, entre otros, de los ingresos del denominado recurso cameral permanente. El artículo 17.1 de la Ley 3/1993, de Cámaras Oficiales de Comercio, Industria y Navegación, especifica que, las Administraciones Tributarias estarán obligadas a facilitar a las Cámaras, a su solicitud, los datos con transcendencia tributaria referidos a ejercicios anteriores que resulten imprescindibles para la gestión del recurso cameral.
De conformidad con este precepto se podrían ceder los datos tributarios imprescindibles a las citadas corporaciones y la referida información sólo podrá ser utilizada para el fin previsto en la Ley 3/1993,.

- **Empresas privadas.** Por parte de varias Cámaras de Comercio, Industria y Navegación se facilitaban datos personales a empresas privadas con objeto de la prestación de servicios de tratamiento automatizado. En todos los casos analizados se pudo constatar que los ficheros automatizados que incluían datos de carácter personal y que fueron objeto de cesión a empresas privadas, lo fueron en el marco del artículo 27 de la Ley Orgánica 5/1992 que regula la prestación de servicios de tratamiento automatizado de datos de carácter personal.

- **Entidades bancarias.** Cabe señalar en esta sección el escrito recibido en la Agencia en el que se ponía de manifiesto la posible vulneración, por parte del Ministerio de Educación y Cultura, de los principios de la Ley Orgánica 5/1992. El hecho objeto de la denuncia fue la posible ilegalidad en la cesión de los datos identificativos y económicos de los empleados a entidades bancarias con la finalidad del pago de las correspondientes nóminas. Los citados hechos podrían, de nuevo, enmarcarse en lo establecido en el artículo 27 de la citada norma.

Asimismo, debemos mencionar que en los convenios suscritos por las entidades implicadas se especifica que, el citado servicio deberá realizarse de acuerdo con la normativa por la que se dispone el pago de haberes y retribuciones, al personal en activo de la Administración del Estado y de los Organismos Autónomos, a través de establecimientos bancarios o Cajas de Ahorro.

4.2.1.2. Deber de secreto.

Cabe señalar con respecto a este principio lo que establece el artículo 10 de la Ley Orgánica 5/1992, 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 aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

En relación con este principio han sido formuladas seis reclamaciones por ciudadanos que manifestaban que, funcionarios o personal laboral pertenecientes a diversas Administraciones (Tesorería General de la Seguridad Social, Agencia Estatal de Administración Tributaria, Instituto Nacional de Empleo y la Escuela Oficial de Idiomas de Zaragoza) habían desvelado datos personales incluidos en los ficheros automatizados cuyos responsables son las citadas Administraciones. Aunque en algún caso aún no ha finalizado la tramitación de los expedientes, en la mayor parte de los incidentes se han podido constatar los hechos objeto de reclamación, no estando justificadas las consultas realizadas por el desempeño de las funciones asignadas al personal que las había efectuado.

Dada la trascendencia de las posibles infracciones cometidas, las Administraciones implicadas habían procedido a incoar expediente disciplinario a las personas implicadas. Asimismo, ante la gravedad de algunos hechos y, habida cuenta de que los mismos podrían encajar en los tipos delictivos contemplados en los artículos 417 y 418 del Código Penal, las instituciones responsables de los ficheros habían procedido a dar traslado al Ministerio Fiscal.

4. 2.1.3. Derechos de las personas.

Debemos señalar en esta sección los hechos manifestados en un escrito presentado ante esta Agencia, en el que se

especificaba la denegación del derecho de acceso por parte del Ministerio de Justicia al informe incluido en un expediente de la citada Institución. Una vez realizadas las actuaciones por parte de la Inspección se constató que el citado informe se encontraba clasificado en la categoría de secreto al amparo del Acuerdo del Consejo de Ministros de 28 de noviembre de 1996. Por ello, los citados hechos se podrían enmarcar en lo establecido en el artículo 2.3 b) de la Ley Orgánica 5/1992, que dispone que se regirán por sus disposiciones específicas los ficheros sometidos a la normativa sobre protección de materias clasificadas.

4. 2.2. AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA.

Entre las actuaciones más significativas llevadas a cabo por la Inspección de Datos en el ámbito de la Administración General del Estado, debemos hacer especial mención a las investigaciones realizadas a instancia de la denuncia formulada por una organización sindical, en la que ponía de manifiesto la posible vulneración de la Ley Orgánica 5/1992, por parte de la Agencia Estatal de Administración Tributaria (AEAT). La denuncia hacía referencia a la adjudicación a empresas privadas de determinados concursos relacionados con la campaña del Impuesto sobre la Renta de las Personas Físicas (IRPF) de 1996 y se centraba en el acceso que dichas empresas tendrían a los datos tributarios de los contribuyentes.

Se realizaron sendas inspecciones al Departamento de Informática Tributaria (unidad que se encarga de prestar los servicios informáticos a la AEAT) y a la Unión Temporal de Empresas (UTE) adjudicataria del concurso. Los objetivos de las inspecciones se pueden resumir en los siguientes puntos:

* Verificar las actividades encomendadas a la UTE por parte de la AEAT y relacionadas con la campaña del IRPF de 1996.

* Identificar los ficheros automatizados que incluyen datos de carácter personal y que son objeto de tratamiento por parte de la UTE.

* Comprobar las medidas técnicas y organizativas establecidas por parte de la AEAT y de la UTE con objeto de garantizar la confidencialidad de la información de los contribuyentes.

De las conclusiones obtenidas de las actuaciones previas realizadas podemos destacar los siguientes aspectos:

Las actividades contratadas a la empresa adjudicataria fueron:

* Servicio Telefónico de Información Tributaria Básica. Se realizaba de una forma totalmente anónima, accediéndose exclusivamente a un fichero automatizado que incluye Preguntas y Respuestas Tributarias (INFORMA). Este fichero también está disponible en Internet. Por todo ello, estas actividades se encuentran fuera del ámbito de aplicación de la Ley Orgánica 5/1992 por no referirse a tratamiento de datos personales.

* Servicio de Cita Previa por Teléfono. Con objeto de atender este servicio, el operador accedía a un fichero automatizado que incluye exclusivamente los datos identificativos del contribuyente. Estos datos estaban completamente separados del resto de datos fiscales y para acceder a los mismos el operador debía, obligatoriamente, identificarse al sistema.

* Servicio de Atención Telefónica para la Confección de Declaraciones del IRPF. De forma voluntaria y totalmente anónima el contribuyente que lo deseaba comunicaba al operador sus datos económicos tributarios y éste le notifica su resultado. En el caso de que el ciudadano deseara que se le remitiera la documentación, debía indicar una dirección, que, una vez impresa, no se almacenaba.

Los datos personales de los contribuyentes a los que tiene acceso y, en su caso, los que figuraban en los equipos informáticos de la entidad adjudicataria del concurso son los necesarios para cumplir las funciones especificadas en el contrato.

Por otra parte, en todos los locales donde se prestaba el servicio, había, permanentemente, funcionarios de la AEAT realizando funciones de control, supervisión y apoyo técnico.

Además, el personal de la empresa adjudicataria había recibido diversos cursos de formación en temas tributarios (impartidos por la AEAT) y en técnicas de atención al público. Asimismo, la empresa adjudicataria les había informado de la legislación vigente en materia de protección de datos y confidencialidad de la información que manejaban. Además, la cláusula quinta del contrato firmado entre la UTE y el trabajador hacía referencia a la confidencialidad de los datos del Cliente.

También la cláusula XI del pliego administrativo del concurso de adjudicación especificaba que la información o especificaciones facilitadas por la Agencia al contratista deberán ser consideradas por éste como confidenciales. Asimismo, en las ofertas que resultaron adjudicatarias, se hacía referencia expresa a la confidencialidad de la información manejada.

Los ficheros automatizados utilizados por la UTE y cuyo responsable es la Agencia Estatal de Administración Tributaria se encuentran inscritos en el Registro General de Protección de Datos.

Como resultado de las investigaciones previas realizadas, hay que señalar que, no se ha detectado la existencia de

actuaciones, por parte de la Agencia Estatal de Administración Tributaria y por parte de la UTE, que pudieran constituir vulneración a lo establecido por la Ley Orgánica 5/1992. Las mencionadas contrataciones se podrían enmarcar en la prestación de servicios de tratamiento automatizado de datos de carácter personal regulado en el artículo 27 de la citada norma.

Finalmente, la AEAT ha remitido en 1998 el documento de destrucción de los ficheros informatizados que incluían los datos relativos al Servicio de Atención Telefónica para la Confección de Declaraciones del IRPF

4. 2.3. ADMINISTRACIÓN AUTONÓMICA

El número de expedientes que se tramitaron relativos a ficheros gestionados por las Administraciones Autonómicas fue de 10, dos fueron iniciados de oficio y el resto lo fueron a raíz de reclamaciones recibidas en esta Agencia, correspondiendo tres de ellos a Tutelas de Derechos. De entre todos estos expedientes dos merecen ser destacados, el primero de ellos como muestra de colaboración entre esta Agencia y los órganos de las Comunidades Autónomas que ejercen las funciones que el artículo 40 de la Ley Orgánica 5/1992 les otorga y el segundo por la significación de la Resolución dictada por el Director de la Agencia.

El primer expediente se inició para obtener información en relación con un estudio que había contratado el Consorcio Regional de Transportes de la Comunidad de Madrid a una empresa externa. Dado que este Consorcio es un organismo de titularidad pública encuadrado dentro de la Comunidad de Madrid y que, durante la tramitación del expediente se creó la Agencia de dicha Comunidad, comenzando por tanto a ejercer las competencias que la Ley le atribuye, se dio traslado a la misma de lo actuado por la Agencia en cumplimiento de lo establecido en el artículo 40 de la Ley Orgánica 5/1992.

El segundo expediente estuvo relacionado con la Consejería de Hacienda y Economía de la Comunidad Autónoma de La Rioja y concluyó con Resolución sancionadora del Director de la Agencia. En la tramitación de dicho expediente se acreditó que la Dirección General de Economía y Presupuestos, dependiente de la Consejería de Hacienda y Economía y órgano de gobierno de esa Comunidad depositaria del secreto estadístico, y que disponía del fichero del Censo Electoral proporcionados por el Instituto Nacional de Estadística en el marco de lo que establece la Ley 12/1989 1, cedió dicho fichero a la Dirección General de Bienestar Social, que no figuraba como órgano de gobierno de La Rioja que tuviera competencias en materia estadística. Por tanto, esta cesión de datos censales sin el consentimiento de los afectados suponía una infracción de carácter muy grave del artículo 11.1 de la Ley Orgánica 5/1992, en relación con el artículo 15.1.a) de la Ley 12/1989, que establece que la comunicación a efectos estadísticos entre las Administraciones y organismos públicos de los datos personales protegidos por el secreto estadístico sólo será posible si los servicios que reciban los datos desarrollan funciones fundamentalmente estadísticas y han sido regulados como tales antes de que hayan sido cedidos.

4. 2.4. ADMINISTRACIÓN LOCAL

El número de expedientes que se tramitaron relativos a ficheros gestionados por la Administración Local fue de 41. De éstos, 26 fueron iniciados de oficio, refiriéndose 24 de ellos a la no inscripción de sus ficheros automatizados en el Registro General de Protección de Datos de esta Agencia. El resto de los expedientes fueron iniciados a raíz de reclamaciones recibidas, correspondiendo uno de ellos a una Tutela del Derecho de Acceso. De entre estos expedientes tres de ellos han finalizado con Resolución sancionadora del Director de la Agencia.

4.2.4.1. Resoluciones sancionadoras

Entre las Resoluciones sancionadoras cabe destacar las que se dictaron en los procedimientos abiertos contra el Ayuntamiento de Mediona (Barcelona) y el Ayuntamiento de Vinalesa (Castellón) y en las que se acreditó que estos Ayuntamientos habían cedido datos del Padrón Municipal de Habitantes, sin que mediara el consentimiento previo de los afectados.

En el primer caso, se había producido la entrega de un listado conteniendo los datos de 123 habitantes de la localidad a un colegio ubicado en el término municipal de Mediona.

Asimismo, en el segundo caso, se hizo entrega de un listado del Padrón a la sucursal de una entidad bancaria para ofertar sus servicios a los habitantes del municipio.

Por lo tanto, en ambos casos, la Agencia entendió que se había producido una infracción de carácter muy grave del artículo 11.1 de la Ley Orgánica 5/1992.

En estas Resoluciones se tuvo especialmente en cuenta lo dispuesto en el apartado tercero del artículo 16 modificado de la Ley 4/1996 2 respecto de las cesiones de los datos del Padrón Municipal, que determina que los datos de dicho Padrón se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado, solamente 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; también se establece que estos datos pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989; por último, prescribe que fuera de estos supuestos los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992 y en la Ley 30/1992 3.

4. 2.4.2. No inscripción en el Registro General de Protección de Datos

En el año 1997 siguieron realizándose actuaciones de oficio por parte de la Inspección relativas a la no inscripción de ficheros en el Registro General de Protección de Datos por parte de un gran número de municipios.

De estas Entidades Locales existe todavía un gran número de ellas que no han procedido a realizar tal inscripción, aunque se encuentran realizando las gestiones oportunas para llevarla a cabo. Como dato digno de mención, hemos de destacar que el Ayuntamiento de Ourense aun no ha procedido a inscribir sus ficheros, siendo la única capital de provincia en esta situación a finales de 1997.

4.2.5. FICHEROS DE FUERZAS Y CUERPOS DE SEGURIDAD

Al igual que en el año 1996, en el año 1997 se ha recibido un número bajo de entrada de reclamaciones en el sector de los ficheros de las Fuerzas y Cuerpos de Seguridad, en concreto sólo dos. El resto de las actuaciones se realizaron de oficio.

Ya es conocido el criterio de esta Agencia de que los ficheros policiales de las Fuerzas y Cuerpos de Seguridad deben ser tenidos especialmente en cuenta en los planes de inspecciones de oficio que se llevan a cabo, dado el régimen especial que les otorga la Ley Orgánica 5/1992. Por tanto, dado que en años anteriores se habían inspeccionado los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y de la Ertzaintza, este año se planificó la realización de inspecciones de oficio a los ficheros policiales de las Policías Locales, llevándose a cabo inspecciones en los cuerpos de Policía Local de los Ayuntamientos de Barcelona, Benidorm, Bilbao, Ibiza, Lloret de Mar, Marbella, Madrid, Murcia, Sevilla, Valladolid, Vigo y Zaragoza.

Asimismo, durante el año 1997, han continuado las reuniones del grupo de trabajo compuesto por personal de esta Agencia y del Departamento de Interior del Gobierno Vasco y formado a raíz de la inspección realizada a los ficheros policiales de la Ertzaintza, siendo previsible que a lo largo del año 1998 el trabajo realizado se plasme en una norma reguladora, dictada por ese Departamento para sus ficheros policiales, y que concrete algunos de los conceptos jurídicos indeterminados que aparecen en la regulación de los ficheros de las Fuerzas y Cuerpos de Seguridad en la Ley Orgánica 5/1992.

4. 2.5.1. Expedientes de reclamación tramitados

Como ya se ha indicado, dos han sido las reclamaciones tramitadas. La primera de ellas interpuesta por la Asociación Pro Derechos Humanos de España y en la que se manifestaba que se estaba elaborando un censo de inmigrantes subsaharianos en la ciudad de Melilla por parte de la Comisaría Provincial de Policía de esa ciudad, utilizándose datos sanitarios provenientes del INSALUD. Realizadas las inspecciones pertinentes, se comprobó que dicha Comisaría Provincial mantenía un fichero automatizado que recogía los datos de carácter personal de los inmigrantes subsaharianos que se encontraban en esa ciudad, siendo estos datos recabados principalmente de la información proporcionada por los propios afectados y no encontrándose evidencias que demostraran que se estaban utilizando datos provenientes del INSALUD. Por ello, se procedió al archivo de las actuaciones.

La segunda reclamación tramitada proviene de una comunicación recibida de la Fiscalía del Tribunal Superior de Justicia de Cataluña, en la que se solicitaba la realización de una inspección al fichero informático de la Policía Local del Ayuntamiento de Gavá (Barcelona), con el fin de que se dictaminara si el mencionado fichero se ajustaba a la legalidad vigente. Por ello se realizó inspección en los locales de la Policía de ese Ayuntamiento, comprobándose que el fichero del Padrón de Habitantes de esa localidad había sido incorporado a sus ficheros policiales, así como que no se acreditó suficientemente, tal y como exige el artículo 20.2 de la Ley Orgánica 5/1992, la existencia de un supuesto de peligro real para la seguridad pública o para la represión de infracciones penales, respecto de los datos policiales que habían sido recabados sin el consentimiento de los afectados. Por tanto, se procedió a la apertura de Procedimiento de Infracción de Administraciones Públicas, según lo previsto en el artículo 45 de la Ley Orgánica 5/1992. La Resolución que puso fin a este procedimiento, concluyó que ese Ayuntamiento había infringido lo dispuesto en el artículo 4.2 de la Ley Orgánica 5/1992, por haber incorporado de forma masiva a sus ficheros de finalidad policial los datos del Padrón Municipal, y lo dispuesto en su artículo 20.2 por haberse registrado datos de carácter personal fuera de los casos permitidos en el citado artículo; ambas infracciones están tipificadas como de carácter grave en el artículo 43.3d) de esta Ley.

Debe resaltarse que, de acuerdo con los principios de la Ley Orgánica 5/1992, no habría inconveniente para que en el ejercicio de las funciones específicas de la Policía Municipal, se utilicen los datos del Padrón municipal siempre que se asegure que se utilizan únicamente aquellos datos que son adecuados, pertinentes y no excesivos, se realice en el marco de expedientes concretos y con necesidades debidamente justificadas y se garanticen la confidencialidad y seguridad de los datos personales.

4.2.5.2. Inspección de oficio de los ficheros de las Policías Locales

Esta inspección iniciada de oficio pretendía conocer el estado general de los ficheros automatizados con finalidad policial de las Policías Locales, prestando especial interés a aquellos que puedan contener datos especialmente protegidos. Los ficheros de tipo administrativo no se revisaron, ya que éstos, tal y como se recoge en el artículo 20 apartado 1 de la Ley Orgánica 5/1992, están sometidos al régimen general de la Ley, y por ello, quedaron fuera de los objetivos de las inspecciones que se realizaron.

Los objetivos del Plan de Inspección fueron los siguientes:

- Verificar que se habían inscrito en el Registro General de Protección de Datos todos los ficheros automatizados de la Policía Local o que se habían iniciado los trámites pertinentes para ello.

- Constatar el tipo de datos especialmente protegidos residentes en los ficheros y la justificación de la existencia de los mismos en cumplimiento de la Ley Orgánica 5/1992 (necesidad para los fines de una investigación concreta).

- Determinar la existencia de un procedimiento de obligado cumplimiento en el que se definiera la forma de cancelar la información contenida en los ficheros, en los términos que indica la Ley Orgánica 5/1992 en su artículo 20 apartado 4.

- Confirmar la existencia de una clasificación por categorías de los ficheros en función de su grado de fiabilidad, en cumplimiento del artículo 20 apartado 2 de la Ley Orgánica 5/1992.

- Precisar las cesiones de datos de los ficheros: en qué casos se producían, a qué organismos y de qué forma; también determinar a qué ficheros tenían acceso las Policías Locales, prestando especial atención al acceso que tuvieran habilitado a los ficheros del propio Ayuntamiento y a los de otras Fuerzas y Cuerpos de Seguridad.

- Averiguar la existencia de procedimientos documentados de obligado cumplimiento que determinaran las medidas de seguridad asociadas a cada uno de los ficheros.

Fueron seleccionados los municipios de las principales capitales de provincia atendiendo a su población y los de las principales áreas turísticas, tratando de que todas ellos pertenecieran a Comunidades Autónomas diferentes. Por ello, fueron seleccionados los Ayuntamientos de las siguientes grandes ciudades: Madrid, Barcelona, Sevilla, Zaragoza, Bilbao, Murcia, Valladolid y Vigo; también fueron seleccionados los siguientes municipios de áreas turísticas: Marbella (Málaga), Benidorm (Alicante), Ibiza (Baleares) y Lloret de Mar (Gerona).

Las inspecciones se realizaron durante los meses de mayo y junio, y de éstas se desprendieron las siguientes conclusiones:

- **Inscripción en el Registro General de Protección de Datos:** se detectaron numerosos ficheros pertenecientes a las Policías Locales que no habían sido inscritos en la Agencia, hecho del que se dio traslado al Registro General de Protección de Datos a los efectos oportunos.

- **Existencia de ficheros policiales:** se encontró que sólo algunas de las Policías Locales inspeccionadas disponían de ficheros en los que se recogían los datos de personas de interés policial (personas detenidas, personas sometidas a investigación, requisitorias de personas por la comisión de delitos, etc.), ya que las tareas estrictamente policiales son desempeñadas en la mayoría de los municipios por otras Fuerzas y Cuerpos de Seguridad. También se detectó en algunos municipios la existencia de programas informáticos estándar, que, de una forma integrada, automatizaban todas las tareas que desempeñaban las Policías Locales, desde aquellas de tipo administrativo hasta las de carácter policial.

- **Existencia de datos especialmente protegidos:** se comprobó que el origen racial es el principal dato especialmente protegido que se recogía en los ficheros de tipo policial, recabándose en los casos en los que las personas eran detenidas.

- **Cancelación de datos:** en ninguna de las Policías Locales inspeccionadas existía una normativa que regulara la cancelación de oficio de los datos con finalidad policial, en el sentido expuesto en el artículo 20.4 de la Ley Orgánica 5/1992. Los datos más antiguos de personas detenidas eran del año 1986, aunque en la gran mayoría de las Policías Locales estos datos correspondían a datos de detenciones realizadas con posterioridad a 1990.

- **Ejercicio de los derechos de acceso, cancelación y rectificación:** aunque en ninguna Policía Local constaba que ningún ciudadano hubiera ejercido estos derechos, se confirmó que no existía una normativa que documentara qué pasos debían seguirse ante la recepción de una petición de este tipo. Simplemente, si se hubieran producido, se habrían canalizado a través de los Registros de Entrada de los Ayuntamientos.

- **Clasificación por categorías:** en ningún caso se encontró una categorización de los ficheros policiales en función de su grado de fiabilidad. No obstante, la información recogida en los ficheros policiales inspeccionados era, en general, de alta fiabilidad.

- **Cesiones de datos realizadas por las Policías Locales:** en general, las Policías Locales sólo realizan cesiones de datos de sus ficheros a las instituciones judiciales, no habiéndose detectado ninguna irregularidad a este respecto.

- **Acceso a otros ficheros por parte de las Policías Locales:** Se comprobó que, con carácter general, las Policías Locales podían realizar consultas a los ficheros de las Fuerzas y Cuerpos de Seguridad que resultaban relevantes para el ejercicio de sus funciones y que están recogidas en las normas de creación de dichos ficheros.

Por tanto, dado que las deficiencias detectadas no eran determinantes para la apertura de Procedimientos de Infracción de Administraciones Públicas y que estas inspecciones se enmarcaban dentro de otras similares realizadas en otros Ayuntamientos, llevadas a cabo con el fin de conocer el estado de los ficheros policiales de las Policías Locales, no se consideró la posibilidad de proceder a la apertura de Procedimientos de Infracción de Administraciones Públicas. Sí se

consideró que era necesario establecer recomendaciones a escala supramunicipal, que permitirían obtener una solución global a las deficiencias detectadas en los Ayuntamientos inspeccionados, y a las que pudieran existir en otros Ayuntamientos que no lo fueron. Por ello, durante el año 1998 se iniciarán los contactos oportunos con la Federación Española de Municipios y Provincias, con el fin de adoptar unos criterios generales que puedan ser adoptados por todas las Policías Locales.

4. 2.6. SANIDAD

4. 2.6.1. Reclamaciones recibidas

Al igual que en años anteriores hay que destacar el escaso número de denuncias presentadas ante la Agencia que hicieran referencia a posibles infracciones en el tratamiento de datos sanitarios. A continuación se describen aquellos que por su relevancia se han juzgado más representativos.

4.2.6.1.1. *Donación de sangre*

Reclamación en la que el denunciante, tras una donación de sangre efectuada en un centro móvil de un organismo de una Comunidad Autónoma, recibió, meses después de la misma, una carta en la que le remitían los resultados del análisis efectuado a la sangre extraída y una tarjeta de donante. Al ser enviados dichos resultados por una empresa privada, el denunciante creyó vulnerada su intimidad por poseer esta empresa datos relativos a su salud.

Después de realizar las oportunas actuaciones de investigación, se pudo comprobar que la empresa que remitió el resultado de los análisis únicamente realizó la personalización y ensobrado de los envíos procedentes de la Comunidad Autónoma, en base a un contrato de servicios establecido entre ambas entidades. Los datos facilitados por la Comunidad fueron borrados de la empresa al finalizar las tareas contratadas.

Al ser éste un contrato de servicios contemplado en el artículo 27 de la Ley Orgánica 5/1992, se procedió al *Archivo* de las actuaciones.

2.6.1.2. *Estudio de Prevención de enfermedades cardiovasculares*

Habiendo tenido la Agencia conocimiento de la existencia de un proyecto para estudiar la posible prevención de enfermedades cardiovasculares en una determinada Comunidad Autónoma y dado que para el desarrollo de dicho proyecto estaba prevista, en una primera fase, la cesión de los datos clasificados por edad y sexo del Padrón Municipal del conjunto de la población de algunos Municipios, se abrió un expediente de investigación con el objetivo de comprobar la adecuación a lo que establece la Ley Orgánica 5/1992.

Tras la realización de las pertinentes actuaciones de investigación se obtuvo información en la que se declaraba que dicho proyecto por el momento y por decisión de los Distritos Sanitarios, está suspendido por no haberse podido solventar los problemas económicos y administrativos existentes, por lo que no ha llegado a requerirse ningún dato de carácter personal.

2.6.1.3. *Divulgación de datos de salud mental*

Un funcionario de un Ayuntamiento manifestó que datos relativos a su salud mental proporcionados a dicho Ayuntamiento en forma de informe médico, han sido divulgados sin su autorización, y que dicha información figura en las Actas de la sesión plenaria del Ayuntamiento. Sin embargo estos datos ni fueron ni iban a ser automatizados por lo que se procedió al *Archivo* del expediente.

2.6.1.4. *Denegación de acceso a resultados de pruebas médicas*

Reclamación en la que el denunciante manifiesta que después de habérsele realizado un reconocimiento médico en la empresa, solicitó el resultado de sus análisis, a lo que la misma respondió que sus pruebas no habían sido completadas, no facilitándosele ningún tipo de información. Esta reclamación dio lugar a la apertura de un procedimiento de Tutela de Derechos.

La empresa alegó no haber sido incorporados los datos relativos al reconocimiento médico en su Base de Datos, por no haber concluido todavía el proyecto de informatización previsto en una cláusula del Convenio Colectivo 1989-1990.

En las investigaciones realizadas se pudo comprobar que la empresa sí disponía de ficheros que contenían datos relativos a la salud de los empleados, y que en ellos se encontraban datos relativos al denunciante. La reclamación de acceso finalmente fue *estimada*.

2.6.1.5. *Datos de salud en los ficheros de una compañía aseguradora*

El denunciante pone en conocimiento de la Agencia la existencia de datos relativos a su *Salud* en una compañía aseguradora, sin consentimiento del mismo, en base a una solicitud de seguro realizada en 1990.

Como consecuencia de los hechos constatados en las investigaciones realizadas, se abre expediente sancionador a la compañía aseguradora por infracción al artículo 7.3 de la Ley Orgánica 5/1992, que establece que este tipo de datos

sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente".

2.6.1.6. *Revelación de datos de salud*

Reclamación en la que el denunciante expone el hecho de haber circulado los datos relativos a su salud por las distintas Unidades de su Dependencia, como consecuencia del expediente abierto por un procedimiento de cese en destino. Entre la documentación de dicho expediente se encontraban todas las bajas médicas del interesado durante su permanencia en la Unidad, por lo que denuncia la falta de confidencialidad con la que se ha tratado el mismo.

Después de realizar las oportunas actuaciones de investigación, se comprobó que los datos relativos a la salud del denunciante, fueron obtenidos a partir de su Ficha Personal y de Antecedentes, siendo necesarios para tramitar su expediente de cese en destino debido a que existe una Orden General en la que en su artículo 5º se establece que la pérdida de condiciones psicofísicas que han de reunir quienes integren Unidades similares a la cual pertenece el denunciante, dará lugar a la baja de la misma una vez reconocida esa pérdida en el oportuno expediente.

Por otra parte, los datos relativos a la salud del denunciante no se encuentran en ficheros automatizados, excediendo por tanto el ámbito de la Ley Orgánica 5/1992.

4.2.6.2. Plan de inspección en hospitales públicos (Acuerdo con INSALUD)

El sector sanitario tiene un especial interés respecto a los derechos de los ciudadanos en relación con la protección de sus datos personales, dado que los datos relativos a la salud de las personas están considerados como especialmente protegidos en el artículo 7 de la Ley Orgánica 5/1992.

Independientemente de las denuncias presentadas relativas a este sector y con el objetivo de conocer la panorámica del mismo en relación a la protección de datos, la Agencia contempló la posibilidad de iniciar un estudio que afectaba a todas las entidades públicas o privadas así como profesionales autónomos que pudieran tratar datos relativos a la salud.

Como inicio de este estudio se definió en 1995 un Plan de Inspección de oficio en el sector hospitalario, que continuó en 1996, con el objetivo principal de conocer la situación actual hospitalaria respecto a la forma en la que son tratados los datos en cuanto a Seguridad, Privacidad y Confidencialidad, así como estudiar la medida en la que se garantizan los derechos de los afectados. En relación con el mencionado plan de inspección se realizaron inspecciones en varios hospitales dependientes del INSALUD.

Estas inspecciones se dieron por finalizadas en el año 1996, elaborándose un informe de conclusiones relativos a los aspectos más relevantes respecto a protección de datos detectados en las inspecciones realizadas.

Dicho informe fue remitido al INSALUD, con el propósito de poner de manifiesto la situación de los centros inspeccionados en relación con la protección de datos y solicitar una respuesta a las deficiencias observadas.

Las principales conclusiones plasmadas en el mencionado informe se resumen a continuación:

- No existe el necesario conocimiento e implicación por parte de los órganos directivos de los centros, en lo que a protección de datos se refiere, así como tampoco una mentalización adecuada respecto de los problemas de seguridad.

- No existen definiciones de nivel de confidencialidad de los datos que se utilizan desde los distintos puntos de tratamiento de los centros.

- No están definidos ni documentados los procedimientos en materia de cesión de datos médicos ni los requisitos legales necesarios para su cesión a otros centros.

- No existen procedimientos sobre los tipos de datos que pueden transferirse internacionalmente así como los posibles destinatarios.

- No existe control de salida de datos de los centros.

- No se informa a los afectados de los puntos indicados en el artículo 5 de la Ley Orgánica 5/1992.

- No existen procedimientos para ofrecer información a los afectados ante el ejercicio de su derecho de acceso.

- No están correctamente declarados los ficheros existentes.

- No existe, generalmente, un Plan de Seguridad ni conciencia respecto de los riesgos asociados a una seguridad deficiente.

Como consecuencia de este informe, en septiembre de 1997, el INSALUD ha distribuido una Circular a los Servicios Centrales, Direcciones Provinciales, Gerencias y Centros Asistenciales, en la que se indica que para dar cumplimiento a las recomendaciones de la Agencia, y adecuar de forma gradual y precisa los sistemas de información a las obligaciones que establece la Ley 5/1992, la Presidencia Ejecutiva, con el informe favorable de la Asesoría Jurídica, dicta

instrucciones relativas a:

- Ámbito de aplicación.

- Controles en el acceso a la información.

- Administración de Seguridad.

- Utilización de la información.

- Controles en los soportes de datos.

- Seguridad en las comunicaciones.

- Controles de acceso a locales.

- Declaración de ficheros automatizados.

- Derecho de información del paciente.

- Cesión y transferencia internacional de datos.

- Relaciones con empresas externas.

- Desarrollo de un Plan de Seguridad.

Estas instrucciones, aunque no resuelven totalmente los problemas detectados al ser extremadamente difícil abordarlos de una forma conjunta y completa, sí pueden considerarse como un intento importante dirigido a mejorar aspectos substanciales de la protección de datos personales en los hospitales dependientes del INSALUD.

En un futuro próximo, se pretende abordar un trabajo similar con las redes sanitarias dependientes de las distintas Comunidades Autónomas con competencias transferidas en materia de sanidad.

Por otra parte, será necesario completar el estudio comenzado en el sector sanitario incluyendo inspecciones en hospitales privados, así como iniciar una nueva fase que contemple la situación en relación con la protección de datos de todas aquellas personas que realicen su actividad profesional como autónomas o cualquier otra entidad, pública o privada, que trate datos relativos a la salud.

4.2.7. FICHEROS DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Al igual que en años anteriores, el sector de prestación de servicios de información sobre solvencia patrimonial y crédito ha sido el que ha ocasionado, durante 1997, un mayor número de reclamaciones de tutela de los derechos de acceso, rectificación o cancelación de datos personales garantizados por la Ley Orgánica 5/1992, y de denuncias de presuntas infracciones de la misma. La gran mayoría de las reclamaciones y denuncias recibidas en relación con este sector (más del 90%) hacían referencia a 4 ficheros solamente.

Este hecho reafirma la experiencia de años anteriores y permite concluir, sin lugar a dudas, que la información tratada en los ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, es la que continúa despertando una mayor inquietud entre los ciudadanos.

En cuanto a las actuaciones practicadas, los inspectores de la Agencia levantaron 198 actas en relación con ficheros de esta naturaleza de las 375 realizadas; es decir, más del 50% del total. Como ya se ha anticipado, la mayor parte de estas actas, 177, hacían referencia a 4 ficheros solamente, lo que muestra el alto grado de concentración del sector.

Por su parte, de los 202 procedimientos sancionadores y 113 procedimientos de tutelas de derechos tramitados por la Agencia, 86 procedimientos sancionadores y 27 procedimientos de tutelas de derechos hacían referencia al tratamiento de datos contenidos en ficheros de esta naturaleza.

La actividad desarrollada ha permitido incrementar el conocimiento del sector confirmando la tendencia de concentración y de la intención de ampliar los servicios con información sobre cumplimiento de obligaciones dinerarias y, en general, de la denominada solvencia positiva. Asimismo, este conocimiento ha sido utilizado en la elaboración de la instrucción 1/1998, de la Agencia, y servirá de base para la elaboración de una instrucción dedicada exclusivamente a los ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992.

Además, al margen de ciertas discrepancias existentes entre las interpretaciones de la Agencia y las de los responsables de ficheros de esta naturaleza, se ha constatado un interés notable de estos últimos por adaptar los tratamientos a las exigencias legales.

4. 2.7.1. Naturaleza de las actuaciones que han motivado la apertura de expedientes sancionadores

Se ha constatado un notable descenso de procedimientos relacionados con algunos aspectos como el ejercicio del derecho de acceso, y se han iniciado procedimientos por nuevos tipos de infracción como, por ejemplo, no remitir los informes de las auditorías de seguridad exigidas por la Instrucción 1/1995, de la Agencia. Sin embargo, y a pesar de las modificaciones introducidas por los responsables de ficheros, la naturaleza de las infracciones detectadas no difiere en exceso de las de ejercicios anteriores.

4.2.7.1.1. *No atender al ejercicio de los derechos de rectificación y cancelación*

El problema más importante de los detectados consiste en que el responsable de un fichero común sobre incumplimiento de obligaciones dinerarias, ante las solicitudes de los afectados, en lugar de atenderlas y tramitarlas para hacerlas efectivas en el plazo de cinco días, contesta al afectado informando de los datos relativos a su persona que figuran en el fichero y comunicándole que se dirija a la entidad que consta como informante de sus datos. En la actualidad los procedimientos empleados por los responsables de ficheros de esta naturaleza ya ha corregido tal conducta. Los procedimientos abiertos se deben a hechos producidos con anterioridad a esta adecuación.

También se ha comprobado que alguna entidad ante el ejercicio de un derecho de acceso, rectificación o cancelación sobre información contenida en un fichero de esta naturaleza no procedió a contestar al afectado en el plazo previsto por la normativa vigente.

4.2.7.1.2. *Inclusión de datos erróneos por causas no imputables al afectado (Calidad de datos)*

Algunos procedimientos sancionadores se han iniciado como consecuencia de la inclusión en un fichero de incumplimiento de obligaciones dinerarias a causa del tratamiento de las entidades que han gestionado la tramitación del pago, motivada por errores tales como la no comunicación del número de cuenta o la comunicación de un importe de cobro erróneo. Este tipo de sucesos se produce con mayor asiduidad entre entidades que comunican impagos producidos al fichero común inmediatamente después de que se produzca. El número de errores se reduciría si, en lugar de enviar datos inmediatamente, se informara al afectado que se va a comunicar el impago al fichero de solvencia patrimonial y crédito, dándole la oportunidad de aclarar la situación.

En algunos ficheros donde se recoge información proveniente de diversas fuentes, los datos relativos a un afectado han sido enriquecidos con información que no hacía referencia a su persona. La causa principal suele ser que la identificación del afectado, en algunos casos, se realiza únicamente por coincidencia de nombre y apellidos.

4.2.7.1.3. *No reflejar la situación real del afectado (Calidad de datos)*

La infracción que más se ha producido es consecuencia de que los datos almacenados en el fichero no recogían sucesos ocurridos con posterioridad a la inclusión de los mismos.

En ficheros que tratan datos de cumplimiento e incumplimiento de obligaciones dinerarias suministrados por el acreedor o por quien actúa por su cuenta o interés, se ha comprobado que es frecuente que la actualización de los datos referentes a los pagos efectuados por los afectados no son comunicados al responsable del fichero en los plazos previstos en la normativa vigente. Este hecho se produce tanto en la información que la entidad actualiza de oficio, como la que se produce como consecuencia del ejercicio de los derechos de rectificación o cancelación de los afectados.

En ficheros conteniendo datos de fuentes accesibles al público, el problema resulta mucho más difícil de resolver, ya que en la mayor parte de los casos no se publican las sentencias, desistimientos y otras muchas incidencias de procedimientos judiciales o reclamaciones de organismos públicos, que sí han sido publicadas en alguna de las fases de la tramitación.

4.2.7.1.4. *Inconsistencia en ficheros de múltiples copias (Calidad de datos)*

Existen responsables de ficheros que distribuyen información contenida en el fichero común a entidades con quienes tienen contratado el servicio y, en algunos casos, estas entidades deben encargarse de la actualización de la copia que mantienen en sus equipos con la información recibida.

Con motivo de algunas denuncias recibidas se ha constatado que la información contenida en las copias ubicadas en los equipos informáticos de las entidades que tienen contratado el servicio, no coincide con la información contenida en el fichero del que ésta procede, con la consiguiente vulneración del principio de calidad de datos por parte de la entidad que recibe la información.

4.2.7.1.5. *No notificar la inclusión en un fichero de solvencia patrimonial y crédito*

Aunque en la actualidad casi todos los responsables de ficheros, tanto de incumplimiento de obligaciones dinerarias como de solvencia patrimonial, han habilitado procedimientos para efectuar las preceptivas notificaciones a los afectados de su inclusión en el fichero, todavía se han detectado algunos casos en que los responsables de ficheros no pueden acreditar el envío de la notificación.

Resulta significativo que en un porcentaje elevado de las reclamaciones recibidas, la denuncia se ciñe a que no se ha producido la notificación de inclusión en el fichero, con independencia de que los datos que aparecen en él se ajusten

o no a la situación real del afectado.

4.2.7.1.6. *Utilizar datos obtenidos de un modo ilegítimo*

Durante este ejercicio no se han tramitado procedimientos sancionadores por la obtención ilícita de datos incorporados en ficheros de esta naturaleza. No obstante, cabe recordar que en el caso de que un afectado ejerza su derecho de acceso, el responsable del fichero debe comunicarle la procedencia de la información.

4.2.7.1.7. *Mantener datos con una antigüedad superior a seis años*

También este año se ha constatado el mantenimiento de información adversa con una antigüedad superior a los seis años desde que se produjo el impago o la reclamación.

Aunque en el caso de los ficheros en los que la información la suministra el acreedor o quién actúe por su cuenta o interés, la responsabilidad de la existencia de información con una antigüedad superior a seis años corresponde a la entidad informante, debe recordarse que se evitarían la mayor parte de denuncias en este sentido si el responsable del fichero común efectuara controles periódicos sobre los datos tratados en el fichero.

4.2.7.1.8. *Accesos no autorizados*

La Agencia ha tenido reclamaciones manifestando que empleados de una entidad con acceso a un fichero con fines de información sobre solvencia patrimonial y crédito ha desvelado a una tercera persona no autorizada datos contenidos en el mismo. A pesar de la dificultad que entraña probar este tipo de conductas, en algunos casos se han encontrado evidencias suficientes.

En otro orden de cosas, también se han instruido procedimientos sancionadores al comprobarse, durante la tramitación de algunos expedientes, que empresas que no aportan información a un fichero de incumplimiento de obligaciones dinerarias han tenido acceso a los datos contenidos en el mismo. Los denunciantes han descubierto estas prácticas principalmente por dos vías: la primera, por recibir escritos informándole que figuraban datos referentes a su persona en un fichero de esta naturaleza y ofreciéndose a tramitar su cancelación en el mismo; la segunda, la aparición en algún informe comercial de información procedente de ficheros de incumplimiento de obligaciones dinerarias.

Durante este ejercicio, la Agencia ha vuelto a conseguir soportes magnéticos que contenían una copia parcial de uno de los ficheros más importantes de incumplimiento de obligaciones dinerarias. Sirva este hecho para recordar la necesidad de un reglamento de medidas de seguridad que permita a la Agencia atajar este fenómeno.

4.2.8. PUBLICIDAD DIRECTA

Durante este año se han recibido en la Agencia un total de 126 denuncias relacionadas directamente con el envío postal de publicidad, que han originado el inicio de otros tantos expedientes de investigación, lo que supone un incremento de aproximadamente el 25% con respecto a los iniciados en el año anterior. Al igual que en 1996, la mayor parte de los ciudadanos denunciaba la obtención de datos no ajustada a lo que establece el artículo 29 de la Ley Orgánica 5/1992 "*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*" .

Considerando el número de Procedimientos Sancionadores que han finalizado en 1997 con una resolución estimatoria, se observa que más del 30% de ellos versaban sobre actividades relacionadas con el envío postal de publicidad, siendo reseñable que de las 9 resoluciones con que se sancionaba una falta muy grave, 7 de ellas se refieren a hechos relacionados con este tipo de actividad. De éstas últimas, cabe destacar las sanciones impuestas a tres entidades por la cesión de datos relativos a sus propios clientes a otras entidades con fines de marketing, sin que los afectados hubiesen otorgado previamente su consentimiento.

También en este año se han obtenido evidencias de la disponibilidad, por parte de las empresas inspeccionadas, de ficheros que contienen datos procedentes del Censo Electoral y que habitualmente son utilizados para el envío postal de publicidad. Por estos motivos han sido sancionadas 11 entidades, en 5 de las cuales, dedicadas principalmente al marketing directo, ya había recaído una sanción en años anteriores por hechos similares.

En ausencia de una información más fiable o adaptada al producto o servicio que se pretende vender, los repertorios de abonados a los servicios telefónicos (en soporte de papel o electrónico) siguen siendo, hoy por hoy, una de las principales fuentes de obtención de datos relativos a los potenciales clientes, como destinatarios de diversos envíos publicitarios. Sin embargo, en el desarrollo de las inspecciones realizadas ha podido comprobarse que aún hoy, cinco años después de la entrada en vigor de la Ley, un número considerable de empresas disponen de ficheros que contienen datos recabados con anterioridad, por lo que en algunos casos su tratamiento en la actualidad podría considerarse no adecuado a la legalidad.

Aparte de la proliferación de las denominadas tarjetas de fidelización, este año han visto la luz dos iniciativas privadas, importadas de otros países europeos, con el objetivo de configurar una base de datos personales suficientemente extensa, tanto cuantitativa como cualitativamente, que pudiese ser utilizada para la realización de publicidad directa.

Para ello, ofreciendo el sorteo de premios, se distribuyó un elevado número de copias de sendos formularios de encuesta, de cuya cumplimentación se podrían deducir personalizadamente los hábitos de vida y consumo de un amplio sector de la población de nuestro país.

Con objeto de determinar su adecuación a los requisitos previstos en la Ley Orgánica 5/1992 se iniciaron los correspondientes Procedimientos Sancionadores, que, a 31 de diciembre de 1997, aún no habían sido resueltos. Sin embargo, estos hechos sí han puesto de manifiesto la necesidad, no contemplada en el articulado actual de la Ley, de que la propia Agencia pudiera intervenir con carácter previo o preventivo en este tipo de iniciativas, con el fin de establecer las necesarias garantías con que debieran realizarse para adaptarse a la normativa vigente.

Por último, cabe destacar la cada vez mayor implantación que está teniendo en nuestro país el desarrollo de conocidas técnicas de mercadotecnia a través del canal electrónico que proporcionan las redes telemáticas. En este sentido, a pesar de las importantes iniciativas que están surgiendo para dotar a Internet de un mayor nivel de seguridad, siguen existiendo hoy en día importantes riesgos sobre la confidencialidad de los datos personales aportados por el propio interesado y los que pueden deducirse indirectamente por su conexión a Internet, por lo que sería deseable una mayor concienciación al respecto por parte del ciudadano, objetivo al que la Agencia ha pretendido contribuir mediante la publicación de unas Recomendaciones a Usuarios, que son comentadas en otro apartado de esta edición.

4.2.8.1. UTILIZACIÓN DE DATOS PERSONALES DE ABONADOS A SERVICIOS TELEFÓNICOS

En relación con la utilización de los datos de los clientes de Telefónica de España, S.A. (en adelante Telefónica) para la realización de campañas de publicidad directa, ya en 1996 se procedió a la apertura de un primer procedimiento sancionador a Telefónica y a Telefónica Publicidad e Información, S.A.U. (en adelante TPI), ésta última filial de la primera. Dicho procedimiento sancionador tuvo su origen en las cesiones de datos personales que Telefónica realizaba a TPI sin disponer del consentimiento de los afectados. Por otro lado, TPI, y a partir de los datos que recibía de Telefónica, en conjunción con otros datos procedentes de diversas fuentes, realizaba una clasificación de los abonados a la telefonía fija en base a criterios socioeconómicos y geográficos con el fin de alquilar dichos datos a terceros. Telefónica realizaba el tratamiento automatizado de los datos y las cesiones a terceros sin disponer del consentimiento de los afectados. A mediados de 1997, el Director de la Agencia consideró probados los hechos expuestos y resolvió el procedimiento sancionando a ambas compañías.

Con el fin de recabar el consentimiento de los abonados para realizar las cesiones arriba mencionadas, Telefónica remitió a los abonados al servicio telefónico un encarte, a finales de 1996, con el siguiente texto:

"Estimado Cliente:
Con la finalidad de proporcionarle los mejores servicios, le participamos que los datos que de usted disponemos están incorporados en fichero informatizado titularidad de esta Empresa.
Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y en su caso, revocación del consentimiento para la cesión de sus datos, en los términos previstos en la Ley 5/1992, y demás normas que la desarrollan, a través de nuestros Servicios Comerciales.
Para una atención más completa y personalizada, le comunicamos que dichos datos podrán ser intercambiados entre Telefónica de España, S.A. y las correspondientes filiales y participadas del Grupo Telefónica para la oferta de productos o servicios que puedan ser de su interés a partir del 31 de Enero de 1997, salvo instrucciones expresas en contrario por su parte."

Al objeto de informar a los abonados sobre la primera cesión, los cesionarios y los datos cedidos (artículo 25 de la Ley Orgánica 5/1992), Telefónica les remitió un segundo encarte cuyo texto figura a continuación al que se adjuntaba una relación de empresas del grupo que serían las cesionarias de los datos, entre las que se encontraba TPI:

"Como continuación a nuestra anterior comunicación y en cumplimiento de lo dispuesto en el art. 25.1 e la L.O. 5/92 de 29 de octubre, le comunicamos que los datos relativos a su identificación, productos y servicios contratados, han sido cedidos o podrán serlo, a las empresas filiales y participadas del ***Grupo Telefónica,*** *y a las que en el futuro se incorporen al mismo como filiales o participadas, todo ello al objeto de que Vd. disponga de la mejor información y, en su caso, posibilitarle el acceso a nuestros más avanzados servicios y productos en el área de las telecomunicaciones."*

Ambos encartes dieron lugar a un segundo procedimiento sancionador contra Telefónica por dos motivos:

La primera notificación realizada no cumplía los requisitos mínimos exigidos por el artículo 11 de la Ley Orgánica 5/1992.

La segunda notificación, ni satisfacía las carencias de la primera, puesto que tiene su fundamento en el artículo 25 de la Ley Orgánica 5/1992, ni podría tratarse de la comunicación del artículo 25, ya que la cesión carecería del requisito previo del consentimiento del afectado.

En el procedimiento anterior también se añadió una imputación adicional al margen de los encartes enviados y relativa al incumplimiento de lo preceptuado en el artículo 5 de la Ley Orgánica 5/1992, que establece los requisitos sobre la información que se debe de facilitar a las personas de las que se van a recaban datos personales para su posterior automatización. La información que Telefónica facilitaba a sus abonados era siempre información a posteriori respecto de la recogida de los datos cuando según la Ley debe ser a priori.

En este sentido, Telefónica no informaba a los afectados, de los que recaba datos personales, ni de la existencia de diferentes repertorios de abonados con diferente información cada uno de ellos, ni se informaba de las consecuencias de la obtención de los datos, ni se ofrecía la posibilidad de seleccionar en que repertorios no se deseaba aparecer. Telefónica consideraba que todos los repertorios de abonados eran iguales, y no permitía una exclusión selectiva, cuando la realidad es que eran distintos, puesto que distinta era la información y la forma de acceso que ofrecía cada uno de ellos.

Con el fin de solventar las deficiencias de las dos notificaciones anteriores, Telefónica remitió, a finales de 1997, un nuevo encarte a todos los abonados a la telefonía fija, junto al nuevo texto que a continuación se reproduce, se adjuntaba, de nuevo, una relación de las empresas filiales y participadas del grupo:

"En cumplimiento de la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, le comunicamos que Vd. tiene derecho a acceder, rectificar o cancelar los datos relativos a su contratación con "Telefónica de España, S.A.". Asimismo, le informamos que dichos datos podrán ser entregados a las empresas filiales y participadas actuales del ***Grupo Telefónica*** *para su cesión a terceros con fines de publicidad y marketing directo a partir del 01-01-1998, salvo instrucciones expresas en contrario".*

La circular remitida por Telefónica a sus abonados adolecía, en principio, de falta de información respecto de los siguientes aspectos:

La circular no especificaba que datos personales de los abonados iban a ser cedidos.

No quedaban determinados los cesionarios de la información que se iba a ceder. Si, por un lado, se relacionaban doce empresas del grupo a las que se iban a ceder datos, por otro lado se afirmaba que se iban a ceder también a terceros, pero sin especificar a quienes.

La circular tampoco incluía un dato tan básico como la referencia de a donde debía dirigirse el abonado para expresar su rechazo a la cesión de sus datos.

Con motivo de esta última circular la Agencia volvió a abrir un nuevo Procedimiento Sancionador por los motivos anteriormente expuestos. Por otro lado, diversos medios de comunicación se hicieron amplio eco y seguimiento de la política de Telefónica respecto de los datos personales de sus abonados publicando, prácticamente a diario, artículos criticando la política de la compañía en este terreno.

Finalmente, a finales de 1997, Telefónica decidió cambiar la política de la compañía respecto de la utilización de los datos personales de sus clientes. En este sentido tomó las siguientes decisiones:

Acordó paralizar las cesiones de datos personales de los abonados a terceros. En este sentido, se remitió una circular firmada por el Presidente de la compañía a todos los abonados comunicando tal decisión.

De forma coherente con la decisión anterior, se dio orden a TPI para que desmantelase la línea de negocio del producto CODITEL (suministro de datos personales a terceros para fines publicitarios), solicitando la mencionada empresa la supresión de la anotación relativa a los ficheros inscritos en el Registro General de Protección de Datos de la Agencia puesto que había procedido a la destrucción de los mismos.

Finalizado el ejercicio de 1997 permanecen aún pendientes de resolución los dos últimos procedimientos sancionadores abiertos contra Telefónica cuyas resoluciones finales recaerán en la primera mitad de 1998 y que por lo tanto escapan del alcance de esta memoria. No obstante, y tras exponer lo que ha sido la secuencia de hechos acontecidos a lo largo de 1997 respecto de la comercialización de los datos de los abonados a servicios de telecomunicación, cabe realizar dos reflexiones, que se desprenden de la lectura del apartado segundo de la exposición de motivos de la propia Ley Orgánica 5/1992 y del punto 7.4 del Anexo a la Recomendación nº R(95) 4 *sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicaciones especialmente en lo que se refiere a los servicios telefónicos* (adoptada por el Comité de Ministros del Consejo de Europa el 7 de febrero de 1995). Esperemos que sus contenidos sean tenidos en cuenta de cara al futuro por las empresas que prestan servicios de telecomunicaciones:

Del preámbulo de la Ley Orgánica 5/1992: *" (...) Para la adecuada configuración, que esta Ley se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley contempla el principio del consentimiento, exigiendo que, al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona -artículo 8.2- y del Convenio 108 del Consejo de Europa -artículo 9.2-, que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla".*

Del Anexo a la Recomendación nº R(95) 4: *" (...) El cruce de datos contenidos en una guía telefónica con otros datos u*

otros ficheros deberá estar prohibido, salvo que el derecho interno lo permita o si es necesario para los operadores de red o para los proveedores de servicios con fines operativos".

4. 2.9. SEGUROS PRIVADOS

4.2.9.1. Ficheros de prevención del fraude

En el mes de mayo, se resolvió el Procedimiento Sancionador iniciado en 1996 en relación con el fichero común creado, por una determinada agrupación de interés económico que se había constituido a partir de un importante grupo de entidades aseguradoras, con objeto de prevenir el fraude en la selección de riesgos y en la liquidación de siniestros.

En la Resolución se admitía la creación del fichero al amparo de lo dispuesto en el artículo 24 de la Ley 30/1995 4, por lo que se entendía que no era posible imputar a cada una de las entidades aseguradoras la cesión de datos de los asegurados sin el consentimiento de éstos, ya que al transmitir los datos al que se considera responsable de un fichero común le correspondería a éste la obligación de notificar la inclusión en el fichero en los términos que se desprenden del artículo 28 de la Ley Orgánica 5/1992 o bien, en su caso, recabar el citado consentimiento.

En este sentido, se consideró que la propia agrupación de interés económico, como responsable del fichero común, sí había incumplido lo dispuesto en el artículo 6.1 y 28 de la Ley Orgánica 5/1992, en relación con el artículo 24 de la Ley 30/1995, por lo que había incurrido en la infracción tipificada en el artículo 43.3 d) de la Ley Orgánica 5/1992, al no haberse ni notificado a los afectados su inclusión en el fichero automatizado ni haberse obtenido su consentimiento, con anterioridad al tratamiento automatizado de sus datos personales.

4.2.9.2. Automatización ilegítima de datos de salud

En este apartado, cabe reseñar la Resolución del Procedimiento Sancionador iniciado a una compañía aseguradora, a partir de la denuncia presentada por uno de sus clientes, que declaró no haber recibido satisfacción al ejercicio de su derecho de acceso con respecto al fichero de la entidad. Como consecuencia de las actuaciones practicadas, pudo obtenerse evidencia de que la entidad había procedido a automatizar los datos relativos a las enfermedades del solicitante de la póliza en octubre de 1995, no teniéndose constancia de que se hubiese recabado previamente su consentimiento expreso.

La mencionada Resolución recuerda que el artículo 7.3 de la Ley 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*". Esta norma supone un régimen especial para un determinado tipo de datos que la Ley considera especialmente protegidos. No son, por tanto, aplicables a los mismos las disposiciones del artículo 6 de la Ley Orgánica 5/1992, que prevé que no es necesario el consentimiento del afectado en determinados supuestos entre los que se encuentra el que se refiera 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 el caso de los datos de salud es necesario que el afectado consienta expresamente (lo que en este caso, tal y como se desprendía de los hechos probados, no había sucedido) o bien que por razones de interés general así lo disponga una Ley. Es aquí, donde es necesario tener en cuenta lo que dispone la Ley 50/1980 5. El artículo 10 de dicha Ley dispone que el tomador del seguro tiene el deber, antes de la conclusión de contrato, de declarar al asegurador, de acuerdo con el cuestionario que éste le someta, todas las circunstancias por él conocidas que puedan influir en la valoración del riesgo. Si bien este precepto, puede llevar a concluir que el tomador tiene la obligación de facilitar a la compañía aseguradora los datos de salud que puedan influir en la valoración del riesgo, sin embargo, no autoriza a la automatización de los datos de salud relativos al asegurado sin el consentimiento expreso y menos aún, cuando el asegurado no coincide con el tomador.

Lo expuesto es independiente del hecho de que los datos sólo se utilicen con la finalidad propia del contrato de seguro. Hay que tener en cuenta, que en cualquier caso, y de acuerdo con lo establecido en el artículo 4, en su párrafo segundo, "*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*", principio que además queda reforzado en relación con los datos de salud, al ponerlo en relación con lo dispuesto en el artículo 7 de la Ley Orgánica 5/1992.

4. 2.10. COLEGIOS PROFESIONALES.

Al igual que en el periodo precedente, durante 1997 se han tramitado un número reducido (siete) de procedimientos en el ámbito de colegios y asociaciones profesionales. Todos ellos fueron iniciados a instancias de los afectados. Los citados procedimientos han dado lugar a la apertura de tres Tutela de Derechos y el resto a la apertura de investigaciones por parte de la Inspección de Datos.

En este sector podemos destacar el expediente, iniciado a instancias de diversos miembros de una asociación profesional de ámbito nacional perteneciente al ámbito sanitario, por una posible cesión de datos personales de sus socios residentes en una determinada Comunidad Autónoma, sin el consentimiento de los mismos, para ser utilizados en las elecciones del Colegio Profesional correspondiente.

Como consecuencia de los citados hechos se procedió a la apertura de Procedimiento Sancionador a la asociación

profesional, tramitación que no ha finalizado en el momento actual.

4.2.11. TARJETAS PARA ESTUDIANTES UNIVERSITARIOS

En 1997 se han recibido en la Agencia dos reclamaciones relativas a las posibles cesiones de datos realizadas por distintas Universidades a entidades bancarias para la confección de tarjetas identificativas de los alumnos de las mismas y que al mismo tiempo servirían como tarjetas de crédito o débito de dichas entidades.

Concretamente, una de ellas se hizo en base a un acuerdo existente entre la Universidad y la Entidad Bancaria, por el que dicha entidad se encargaría de hacer la Tarjeta/Carnet Universitario, consiguiendo así solicitudes de tarjeta con la doble finalidad de carnet y financiera.

Con tal motivo se abre un expediente de investigación con el objetivo de comprobar la posible existencia de infracciones a la Ley Orgánica 5/1992, en el transcurso del cual y pese a no haber finalizado todavía las actuaciones, se han puesto de manifiesto los siguientes hechos.

La Universidad ha facilitado a la entidad bancaria, quien firma un compromiso de confidencialidad, datos relativos a una parte de los estudiantes, en base a un convenio de colaboración suscrito entre ambas entidades. Aunque se tiene previsto informar a los afectados en el momento de la solicitud de matrícula, en la fase experimental no se ha informado a los afectados ni solicitado consentimiento de los mismos.

En base a este convenio se crea la tarjeta-carnet que puede tener una doble funcionalidad. Por una parte es carnet universitario como documento de identificación y acceso a los terminales de información dentro de la Universidad y por otra parte, y para aquellas personas que expresamente lo soliciten, puede tener las funcionalidades financieras de tarjeta de crédito y monedero electrónico. La parte universitaria es obligatoria y la parte financiera es optativa.

El colectivo al que se dirige la Tarjeta es a alumnos, profesores y personal de administración y servicios de la Universidad.

Para el almacenamiento de datos la tarjeta cuenta con microchip y banda magnética, para guardar información relativa a temas académicos o financieros. Esta información podrá ser actualizada desde los distintos terminales dispuestos al efecto.

Por otra parte los ficheros inscritos en el Registro General de Protección de Datos por la Universidad, no consta cesión alguna a la entidad bancaria implicada.

4.2.12. SALAS DE BINGOS

Con motivo de una denuncia presentada en la Agencia relativa al uso de los datos de carácter personal realizado por los Bingos, en 1997 se abrió un expediente de oficio, que continúa en 1998, con el objetivo de estudiar dicho sector en cuanto al cumplimiento de la Ley Orgánica 5/1992, y concretamente de la Instrucción 2/1996, de 1 de marzo, de la Agencia, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

Las inspecciones comenzaron a realizarse en 1997, teniendo como objetivo:

- Comprobar la tipología de los datos recogidos.

- Período de conservación de los mismos.

- Cumplimiento de los derechos de los afectados.

- Utilización de los datos.

- Cesiones.

- Inscripción de ficheros.

Aunque todavía no ha finalizado el Plan de Inspección, sí se pueden avanzar algunas conclusiones:

Normalmente la tipología de los datos recabados se corresponde con la indicada en el documento de identificación (DNI, Pasaporte), siendo la información respecto a lo que especifica el artículo 5 de Ley Orgánica 5/1992, en general, deficiente.

Además se ha podido constatar que los datos son únicamente utilizados con la finalidad de controlar el acceso al Bingo y que existe un gran celo por preservar la confidencialidad de los datos recabados.

Respecto al período de conservación de los datos existe en general una discrepancia entre la Instrucción 2/1996, de 1 de marzo y las legislaciones autonómicas respectivas, ya que las competencias en materia de Bingos están transferidas a las distintas Comunidades Autónomas.

También se ha comprobado que existe un gran desconocimiento por parte del sector respecto a la obligatoriedad de inscribir los ficheros con datos de carácter personal en el Registro General de Protección de Datos .

4. 2.13. SECRETO PROFESIONAL.

Tres de las Resoluciones sancionadoras emitidas en 1997 por la Agencia relativas a ficheros privados, inciden sobre la vulneración del artículo 10 de la Ley Orgánica 5/1992, que establece 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*". Por otra parte, el artículo 43.3.g) de la Ley Orgánica 5/1992 establece como falta grave "*la vulneración del deber de guardar secreto, cuando no constituya infracción muy grave*".

Concurre además la circunstancia de que en los tres casos citados la sanción recayó sobre entidades bancarias que suministraron información relativa a uno de sus clientes a otras personas no autorizadas a acceder a esos datos. Estos hechos suponían, de por sí, facilitar información sobre datos personales a terceras personas ajenas al afectado, independientemente de su parentesco o proximidad, y dado que esos datos habían sido automatizados en algún momento, entraban dentro del ámbito de protección de la Ley. Teniendo en cuenta que el secreto profesional supone, en palabras del Tribunal Constitucional (Sentencia de 26-11-84), *el deber de secreto que se impone a determinadas personas de lo que conocieren por razón de su profesión, reconocido expresamente en el artículo 24.2 de la Constitución,* y que el secreto bancario, según recoge la misma sentencia, *no puede tener otro fundamento que el derecho a la intimidad del cliente, reconocido en el propio articulo 18 de la Carta Magna*, resultaba evidente que la actuación llevada a cabo por las tres entidades vulneraba lo dispuesto en la Ley.

Por otra parte, conviene señalar que, aunque en alguno de los casos la información revelada consistía en un saldo deudor en una cuenta corriente, ésta constituiría no sólo un mero dato contable, sino también un dato de carácter personal. Ello se debe a que si bien el dato bancario, aisladamente considerado, es decir, como mero conjunto de números o anotaciones contables, no supone dato personal alguno, se convierte en tal cuando se asocia a otros datos marcadamente personales, como nombre, apellidos, domicilio,..., pues de lo contrario, carecería de todo valor, incluso para la propia entidad bancaria, a la que no le aportaría ningún tipo de información o utilidad.

5. SECRETARIA GENERAL

Las principales actividades realizadas por la Secretaría General durante 1997 han ido dirigidas a facilitar el funcionamiento, en sus aspectos materiales, técnicos y de recursos humanos así como de atención al ciudadano de la Agencia de Protección de Datos, para lo que 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 :

5. 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 Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia, en los siguientes órganos:

-El Director de la Agencia, asistido por su Secretaría Particular y el jefe del Gabinete Jurídico.
-El Consejo Consultivo
-El Registro General de Protección de Datos integrado por 11 funcionarios.
-La Inspección de Datos constituida por 17 puestos de trabajo de funcionarios, de los que 2 se encuentran vacantes.
-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.

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.

- 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 46 puestos de trabajo que se proveen por funcionarios y 3 ordenanzas con vínculo laboral . Al finalizar el año 1997 se encontraba cubierta en un 94% 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 1997, así como Aprobación del Proyecto de Plan de Acción Social del Ente Público para 1998, siguiendo las recomendaciones previstas en el Acuerdo de Administración - Sindicatos para el periodo 1995-1997 sobre condiciones de trabajo en la Función Pública.

5.2. 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 expiraba el 31 de diciembre de 1997. La aproximación de la fecha de vencimiento del contrato evidenció la conveniencia de iniciar actuaciones dirigidas a la asignación a la Agencia de un edificio que le permita desarrollar las competencias que la ley le encomienda con la estabilidad que el desempeño de sus funciones exige, teniendo en cuenta además la previsión de crecimiento de su actividad y de sus recursos humanos. Sin embargo las gestiones realizadas ante la Dirección General del Patrimonio del Estado dirigidas a obtener un edificio adecuado para el ejercicio de las funciones de la Agencia de Protección de Datos no culminaron en 1997 con la asignación de un edificio para este Ente Público. En consecuencia, se negoció, en condiciones favorables para la Administración Pública, la prórroga del actual contrato de arrendamiento hasta el 31 de diciembre del año 2000. Asimismo se mantiene el contrato de arrendamiento de un pequeño local destinado a almacén y archivo del Ente Público.

5. 3. OTRAS FUNCIONES Y TAREAS

- Se ha organizado una **Conferencia en la Universidad de Verano Menéndez Pelayo** con el título **:" La protección de datos en España: situación y perspectivas de futuro",** orientada a favorecer un encuentro entre expertos e interesados en esta materia que permitiera proporcionar una aportación al necesario proceso de difusión de la regulación legal y reglamentaria en materia de intimidad y datos personales automatizados. El contenido y desarrollo de la Conferencia se aborda con más detenimiento en otro apartado de la memoria

- Se ha organizado **una Conferencia Eurolberoamericana sobre Protección de Datos Personales** a la que han asistido Autoridades de Protección de Datos Europeas y representantes de países Iberoamericanos. La Conferencia ha tenido como objetivo primordial el promover un encuentro entre profesionales que aportara un intercambio de opiniones, ideas y experiencias en relación con el proceso de elaboración de disposiciones legales y reglamentarias en esta materia que debe desarrollarse en los países latinoamericanos, y al propio tiempo contribuir con la experiencia europea en relación con la protección de datos personales. Las conclusiones y desarrollo de esta Conferencia se tratan expresamente en otro apartado de la Memoria.

- Se ha convocado la **PRIMERA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES",** con una dotación de un millón de 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 "Utilización y control de Datos Laborales Automatizados" de cuyo contenido se trata mas adelante en otro capítulo.

- 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 1996.

5.4. 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:

5.4.1. 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 la Agencia entre los ciudadanos se ha realizado una campaña de información en medios de comunicación. La operación ha ido dirigida a concienciar a los ciudadanos de sus derechos frente a una posible invasión de su intimidad por el uso de la informática. La campaña institucional ha tenido como destinatarios a los ciudadanos en general y su núcleo ha consistido en la inserción de anuncios divulgativos en prensa escrita 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 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, quejas, reclamaciones o denuncias.

5.4.2. CAMPAÑA INFORMATIVA MEDIANTE TRÍPTICOS Y MANUALES

Además de la campaña de comunicación en periódicos, se ha continuado con la difusión de cuatro dípticos divulgativos con información general que permita conocer al público los objetivos de la campaña. Su contenido versa sobre información general de la Agencia, ejercicio de los derechos, ficheros de morosidad y marketing directo. En estos folletos se trata de convertir en accesible la información difícil de asimilar por su complejidad y falta de difusión de la protección de datos personales automatizados, utilizando los ejemplos prácticos y la imagen para convertir el contenido en más atractivo. Para su difusión se ha contado 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 facilitan a los ciudadanos que se dirigen a la Agencia en demanda de información.

Con el fin de ampliar y complementar el contenido del tríptico 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.

Asimismo se ha procedido a la edición y distribución de un Manual sobre Recomendaciones a Usuarios de Internet elaborado por la Agencia. La distribución se ha efectuado fundamentalmente a través del Congreso Expo Internet 97, las Omic y otras Organizaciones y Asociaciones de Consumidores, habiéndose hecho también entrega del mismo a los ciudadanos que lo han solicitado.

5. 5. CONSEJO CONSULTIVO

* El Consejo Consultivo, previsto en el articulo 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.

* En su composición, está integrada por los siguientes miembros:
- Presidente:
  D. Juan José Martin-Casallo López, Director de la Agencia de Protección de Datos.
- Vocales:
  D. Carlos Navarrete Merino, Diputado propuesto por Congreso de los Diputados
  Dª. Rosa Vindel López, Senadora propuesta por el Senado
  D. José Antonio India Gotor, 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. Eduardo Vilariño Pintos, Vocal propuesto por el Consejo de Universidades .
  D. Adolfo Varela Cea, 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 Cámara de Comercio, Industria y Navegación.
  D. José Ramón Recalde Díez, Representante de la Administración Central, designado por el Gobierno.
- Secretaria:
  Dª. Sofía Perea Muñoz, Secretaria General de la Agencia de Protección de Datos .

* Un estricto cumplimiento de los artículos antes referenciados exigiría la designación de los Vocales que seguidamente se relacionan:

* Un 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:

- Planes de actuación de la Inspección de Datos y del Registro General de Protección de Datos a lo largo de 1997.

- Convocatoria de la primera edición del Premio Protección de Datos Personales, así como fallo del mismo.

- Reunión en España de Autoridades de Protección de Datos Europeas con representantes de los países Iberoamericanos en el marco de la Conferencia de Ministros de Justicia de los Países Hispano-Luso-Americanos.

- Reuniones con la Consejería de Interior del Gobierno Vasco en relación con los ficheros de la Ertzaina.

- Posible reforma legislativa de la Ley Orgánica 5/1985 de Régimen Electoral general, sobre uso y utilización del censo electoral, en relación con la Ley 7/1996 de Ordenación del Comercio Minorista.

- Designación de la Agencia de Protección de Datos española como organizadora de la XX Conferencia Internacional de Autoridades de Protección de Datos que se celebrará en Santiago de Compostela en septiembre de 1998.

- Elaboración por la Agencia de un Manual de Recomendaciones a usuarios de Internet.

- Próxima expiración del mandato de la mayoría de los miembros del consejo Consultivo y del Director de la Agencia.

5. 6. EL ÁREA DE ATENCIÓN AL CIUDADANO

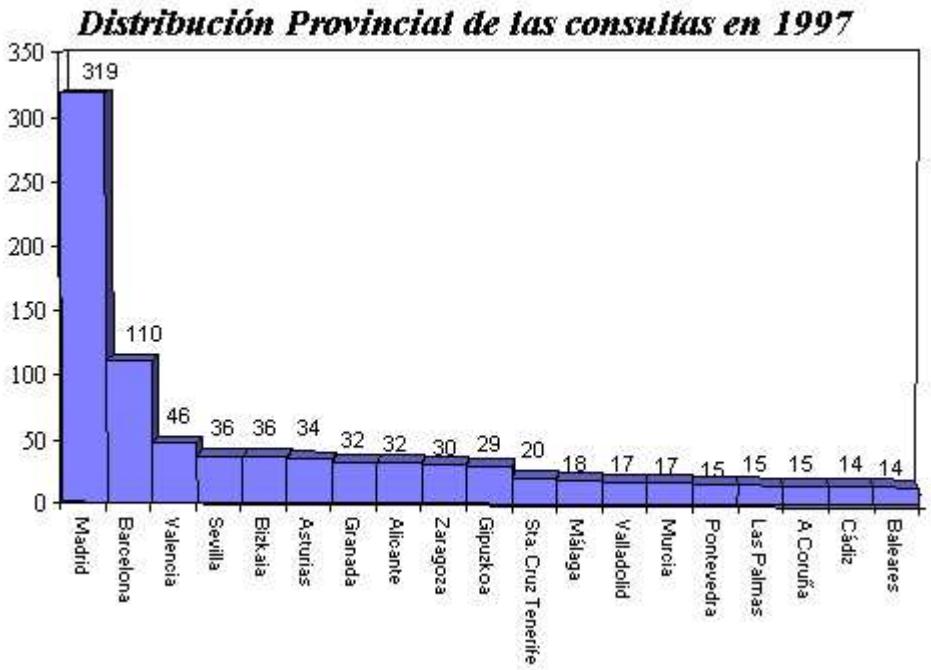
El Área de Atención al Ciudadano ha recibido a lo largo de 1997 más de 10.000 consultas telefónicas en relación con la protección de datos, más de 1300 consultas presenciales y 1009 consultas por escrito. Dado el interés que este tipo de cuestiones pueden plantear a las personas interesadas o destinatarias de las interpretaciones de las normas realizadas por la Agencia, 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.

Resulta particularmente destacable en este año la creación de una página web informativa en Internet, que contiene una guía informativa, modelos para ejercer los derechos, así como el catálogo actualizado de ficheros inscritos en la Agencia. El incremento de consultas por escrito se ha debido en parte a la existencia de un buzón de Correo Electrónico para las consultas, puesto a disposición del público en Internet.

Se clasifican las consultas en función de los sectores de actividad a los que afectan. En primer lugar, se plantean las cuestiones generales planteadas por el ciudadano. En segundo lugar los ficheros sobre solvencia patrimonial y crédito y publicidad directa; dentro de éste último se trata la publicidad a través de Internet. A continuación se tratan las cesiones a particulares de datos de naturaleza tributaria, de la Seguridad Social, el Padrón Municipal, el fichero de vehículos de la Dirección General de Tráfico y los ficheros policiales. Por último, un tercer sector, que hemos considerado mixto, dada la especial naturaleza de las actividades a que se refiere. Incluimos en este sector: la Sanidad, las Relaciones laborales y el Desempleo, la investigación científica, que pueden llevarse a cabo tanto por el sector público como privado; se incluyen en este apartado las Corporaciones de Derecho Público, igualmente los Colegios Profesionales, ya que, por su peculiar naturaleza, ejercen tanto potestades públicas como privadas.

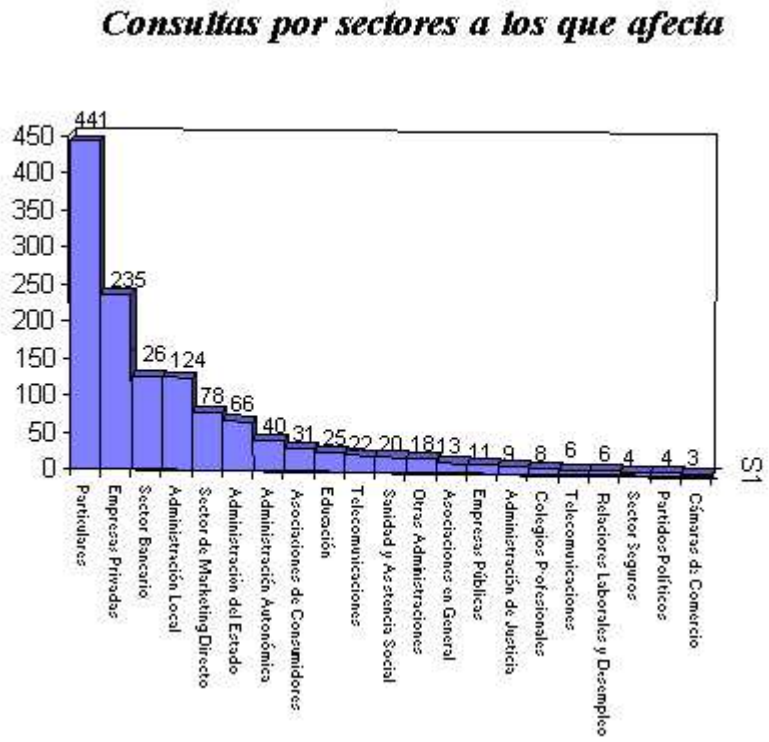
En ocasiones, cuando se produce una intersección entre más de un sector, se ha tomado como criterio para su clasificación, además del sector implicado, la naturaleza de los datos solicitados (datos fiscales, datos de salud) o su finalidad (p.e. control del fraude fiscal), dependiendo del aspecto que se considere más importante en cada caso, con el fin de evitar repeticiones.

La información relativa a las consultas se clasifica por los sectores a los que afecta, los temas sobre los que trata y su distribución por provincias. Tanto en el gráfico sobre sectores, como en el gráfico sobre temas la cifra no coincide con el número de consultas efectuadas o las cifras por provincias, porque con frecuencia en cada consulta se tratan varios temas o porque una consulta afecta a más de un sector.



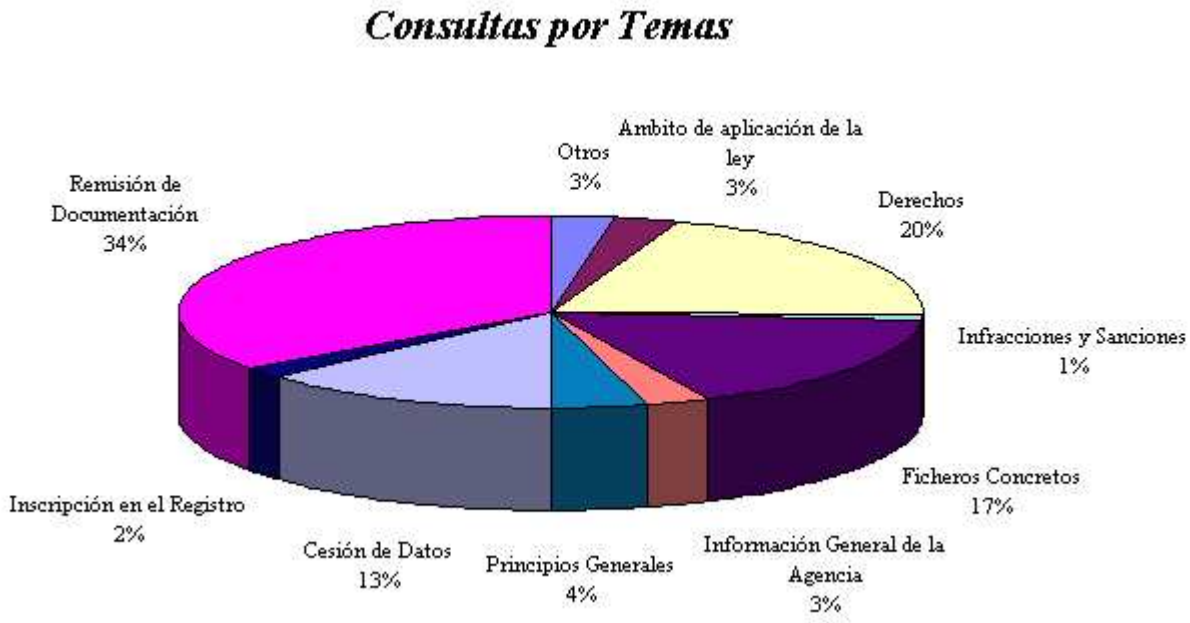
Distribución Provincial de las consultas en 1997

En este gráfico se recogen las consultas realizadas por provincias a lo largo de 1997. Resultan especialmente significativas las consultas de Madrid con 319, y Barcelona con 110. No se han incluido las provincias desde las que se han realizado menos de 14 consultas para evitar una dispersión excesiva de la información.



Consultas a los sectores a los que afectan.

Se clasifican las consultas en virtud de los sectores a los que afecta. Cada consulta puede afectar a dos o más sectores. Se ha dividido el sector privado en sector bancario, marketing directo, seguros, telecomunicaciones y empresas privadas en general que no pertenecen a estos sectores específicos. También se han excluido consultas de empresas que tienen relación con la educación, sanidad y relaciones laborales, por considerar que se encuentran mejor ubicadas en estos sectores.



Consultas por temas.

La distribución de las consultas muestra tres grupos principales: el ejercicio de los derechos previstos en la Ley Orgánica, la cesión de datos y la consulta sobre ficheros concretos, que comprende un grupo de ficheros de especial trascendencia en este ámbito y que se desglosa en el último gráfico.

TIPOS DE CONSULTAS SOBRE CESIÓN DE DATOS.

En este gráfico, se analizan las cuestiones relacionadas con las cesiones, que en su mayoría tienen que ver con cesiones entre Administraciones Públicas que, con frecuencia se encuentran previstas por las leyes.

CONSULTAS SOBRE FICHEROS CONCRETOS.

En este gráfico se puede observar cómo las consultas de los ciudadanos versan en su mayoría sobre ficheros de morosidad y marketing directo. Dentro de los ficheros públicos destaca el Padrón Municipal, los ficheros de las Administraciones Tributarias, y los ficheros policiales, que incluyen también las consultas relacionadas con las policias locales.

5. 6. 1. CUESTIONES GENERALES

5. 6. 1. 1. INFORMACIÓN EN LA RECOGIDA DE LOS DATOS

Con mucha frecuencia se plantean ante la Agencia consultas acerca de los requisitos que deben cumplirse cuando un ciudadano entrega sus datos personales para ser incluidos en un fichero automatizado. Para la recogida y tratamiento automatizado de los datos de carácter personal es indispensable el consentimiento del afectado. Este consentimiento debe ser un consentimiento informado, recabado con los requisitos del artículo 5 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos que dice:

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.

5. 6. 1. 2. INFORMACIÓN SOBRE EJERCICIO DEL DERECHO DE ACCESO.

Los ciudadanos a la Agencia, consultando en qué bases de datos se encuentran incluidos. En estos supuestos, hay que señalar 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. La función de la Agencia a este respecto, consiste en faci-

litar la información relativa a la descripción de los mismos, finalidad, servicios o unidades ante los que se pueden ejercer los derechos de acceso, rectificación y cancelación, los responsables del fichero, etc. Esta información es la contenida en el Registro General de Protección de Datos.

La Agencia puede suministrar la dirección de la oficina designada por el titular del fichero para ejercer los derechos de acceso, rectificación y cancelación, de aquellas entidades o personas de las que se 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 el ciudadano se dirija directamente a cada una de las empresas, solicitando le informen qué datos tienen, cómo los han obtenido y, en su caso, la cancelación de los datos en sus ficheros.

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 afectado 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. 6. 1. 3. INFORMACIÓN SOBRE EJERCICIO DEL DERECHO DE RECTIFICACIÓN Y CANCELACIÓN.

En numerosas ocasiones los ciudadanos se dirigen a la Agencia solicitando información acerca del modo de ejercicio de sus derechos de rectificación y cancelación de datos personales incluidos en ficheros automatizados. Los derechos de rectificación y cancelación son personales, y deben, por tanto, ser ejercidos directamente por los interesados ante los responsables/titulares de los ficheros automatizados. Esto es, debe el ciudadano dirigirse directamente al responsable del fichero , y no a la Agencia de Protección de Datos.

Si los datos de carácter personal incluidos en el fichero resultan inexactos o incompletos deben ser rectificados o cancelados en su caso en el plazo de 5 días desde la solicitud.

Si transcurrido el plazo previsto, de cinco días para los derechos de rectificación y de cancelación, desde la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, podrá dirigirse el ciudadano a la Agencia con copia de la solicitud cursada, para que ésta a su vez se dirija a la oficina designada con el objeto de hacer efectivo el ejercicio de sus derechos.

5. 6. 2 FICHEROS SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Las cuestiones relativas a los ficheros sobre solvencia patrimonial y crédito representan el 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.

La prestación de servicios de información de solvencia patrimonial y crédito ha experimentado una expansión importante debido a la utilización generalizada de los sistemas de tratamiento automatizado, junto con el incremento de la morosidad. La necesidad de mejorar el tráfico mercantil basado en el crédito personal en su sentido más amplio, junto con las consecuencias negativas de esta situación, parecen justificar la existencia de este tipo de ficheros. Ahora bien, la Ley Orgánica, sin desconocer estas circunstancias y la legalidad de este tipo de ficheros, establece en el artículo 28 una serie de limitaciones que garantizan los derechos de los afectados.

La inclusión en un fichero de morosos o impagados tiene una importancia considerable en la vida financiera de las personas, dado que como consecuencia de esta inclusión se produce la privación de todos los resortes del sistema crediticio, lo que abarca desde la tarjeta de un supermercado hasta un crédito hipotecario, pasando por todas las modalidades de tarjetas de crédito y créditos personales.

A menudo se han recibido consultas como consecuencia de la inclusión de personas jurídicas en estos ficheros. La Agencia de Protección de Datos carece de competencia para actuar, dado que la Ley Orgánica limita su ámbito de actuación a las personas físicas identificadas o identificables.

5. 6. 2. 1. INFORMACIÓN SOBRE EL ALCANCE DEL DEBER DE COMUNICACIÓN DEL ARTÍCULO 28.

En este tipo de ficheros quiebra el principio general de la Ley en sus artículos 6 y 11, que exigen el consentimiento para el tratamiento y la cesión. Se sustituye la necesidad del consentimiento previo informado por la 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; y dar al ciudadano la posibilidad de rectificar y cancelar dichos datos en el caso de que sean erróneos.

* 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.

* 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 inscripción 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. 6. 2. 2. EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN EN RELACIÓN CON LOS FICHEROS DE IMPAGADOS

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. 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.

No obstante, el derecho de acceso puede además ejercerse ante todas aquellas personas o entidades bancarias o de financiación que tienen acceso o conocimiento de datos relativos a solvencia de patrimonial y crédito, que tendrían 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 para solicitar la dirección del responsable del fichero para 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 serán rectificados o cancelados en su caso.

Para solicitar la rectificación o la cancelación, habrá que dirigirse en primer lugar al acreedor que ha facilitado los datos. Si no se ha producido la morosidad ni el impago, y existe un principio de prueba suficiente que contradiga esta inclusión, la cancelación deberá hacerse efectiva en el plazo de cinco días desde la solicitud, por parte del responsable del fichero de impagados.Transcurrido este plazo sin que la solicitiud haya sido atendida adecuadamente, podrá dirigirse a la Agencia, con copia de la solicitud cursada, que intervendrá del modo legalmente previsto.

Si los datos son simplemente inexactos, es decir, se ha producido la morosidad o el impago, pero ya se ha satisfecho, el procedimiento a seguir y los plazos serán los mismos, pero el responsable del fichero de morosos podrá mantener el dato rectificado y desfavorable hasta un máximo de séis años contados a partir de la inclusión en le fichero de morosos, o, en todo caso caso, a partir del cuarto mes del vencimiento de la obligación incumplida.

Otro problema que se plantea con cierta frecuencia, es la existencia de números del Documento Nacional de Identidad repetidos y casos de personas cuyos nombres y apellidos son completamente coincidentes o sustancialmente coincidentes con el de otras personas. En estos supuestos, resulta conveniente ejercer el derecho de cancelación ante el responsable del fichero, y, en su caso, interponer la reclamación correspondiente ante la Agencia.

5. 6. 3. PUBLICIDAD DIRECTA

Este es el sector que más consultas y quejas origina por parte de los ciudadanos, después de los ficheros de morosidad. La queja más frecuente manifiestada ante la Agencia es el deseo de no recibir más 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 Agencia recomienda al afectado que se dirija 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. 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.

No obstante lo anterior, se pueden emprender principalmente dos acciones preventivas de carácter general con el objetivo de disminuir el nivel de publicidad nominativa. La primera consiste en la solicitud del ejercicio del derecho de cancelación ante el responsable del envío, y la segunda, el ejercicio del derecho de exclusión en los ficheros de abonados de las empresas de telecomunicación, y más en concreto, en los repertorios de abonados de empresas de Telecomunicación.

Respecto de la segunda, 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, 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; pero al mismo tiempo reconoce también el derecho del afectado de exigir su exclusión, en el caso de que no desee aparecer en dichos repertorios.

Hay que destacar que datos como los que proporciona el servicio de IBERTEX 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, y esta negativa tendrá como resultado también una importante disminución de la publicidad nominativa que recibe.

Se recomienda el ejercicio del derecho de exclusión de los repertorios de abonados de Telefónica y otras empresas del sector, 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. 6. 3. 1. PUBLICIDAD DIRECTA A TRAVÉS DE INTERNET

Un tema nuevo que se plantea en este ámbito es el marketing a través de Internet, recabándose las direcciones 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 de la Agencia.

En este sentido, es necesario considerar también que la dirección de correo electrónico 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 el 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, considere el internauta 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.

5. 6. 4. CESIONES DE DATOS CON NATURALEZA TRIBUTARIA

Se tratan en este epígrafe las consultas realizadas por los particulares relativas a datos de naturaleza tributaria.

En concreto, se han recibido diversas consultas sobre la legalidad de la cesión de datos personales procedentes de los censos fiscales de las Administraciones Locales a empresas privadas y particulares, que pretenden utilizar la información para publicidad o fines particulares. Normalmente, se solicita información sobre la matrícula de los impuestos, que de conformidad con la Ley Reguladora de las Haciendas Locales debe estar a disposición del público en los respectivos Ayuntamientos. La Agencia interpreta la expresión "a disposición del público", en el sentido de que tal obligación se exige como consecuencia del deber de proporcionar información individualizada al sujeto pasivo del impuesto o a un tercero, pero nunca puede amparar peticiones masivas que comprendan la totalidad de la Matrícula de un determinado impuesto, o una sección o fracción del mismo.

La Agencia entiende que el principio de confidencialidad establecido con carácter general en el artículo 113 de la Ley General Tributaria debe tener como consecuencia la interpretación restrictiva de la expresión "a disposición del público". Otra interpretación podría llevarnos a considerar los mismos datos como confidenciales y como públicos sin restricción alguna a la vez.

De conformidad con lo expuesto, será necesario que el Ayuntamiento valore caso por caso el interés legítimo de los terceros para poder acceder a la información contenida en los censos fiscales, pero nunca podrá amparar peticiones masivas que comprendan la totalidad de la Matrícula del referido título. Con carácter general, y en relación con cualesquiera consultas realizadas a los ficheros municipales, resulta necesario que el ayuntamiento en su calidad de administrador de la información, proceda a analizar, caso por caso, las solicitudes, así como su fundamento y la relación de los datos solicitados y consultados, con las finalidades para las que se pretenden utilizar, así como que quede constancia de las consultas y cesiones realizadas.

5. 6. 5. FICHEROS DE LA SEGURIDAD SOCIAL

Se han producido quejas impugnando la decisión del Instituto Nacional de la Seguridad Social de reclamar a ciertos particulares, el complemento de mínimos de pensiones basandose en una cesión de datos de la Agencia Tributaria sobre las rentas percibidas. Hay que señalar que es de aplicación el artículo 19 de la Ley Orgánica, que establece la cesión de datos entre Administraciones Públicas; en concreto, el punto 1 del citado artículo dice:

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 de fichero o por disposición posterior de igual o superior rango que regule su uso.

En este sentido, la disposición de creación de los ficheros del Ministerio de Economía y Hacienda, en el que se almacenan los datos sobre el Impuesto sobre la Renta de la Personas Físicas está publicado en el B.O.E. Num. 180 de 29 de julio de 1994, modificado y ampliado mediante Orden publicada en el B.O.E. Num. 192 de 12 de agosto de 1995, y es en estas disposiciones donde se prevé la cesión de datos a la Seguridad Social. Además esta cesión se encuentra prevista en el artículo 36 de la Ley General de la Seguridad Social.

En el caso planteado, nos encontramos ante un procedimiento administrativo de verificación del cumplimiento de los requisitos legales para la percepción del complemento de mínimos para las pensiones del sistema de la Seguridad Social. Esta revalorización está sometida a la percepción de un nivel de rentas. En este caso el Organismo competente, el INSS, ha solicitado la cesión de sus datos a la Administración Tributaria. Esta cesión merece las siguientes consideraciones:

- Es legal porque se ampara en una norma de rango suficiente, de conformidad con el artículo 19 de la Ley Orgánica.

- Los datos solicitados son pertinentes, adecuados y no excesivos en relación con la finalidad para la que se solicitan.

- Estos datos son el punto de partida para un procedimiento administrativo concreto, en el que existe trámites de alegaciones y pruebas que permiten al afectado aportar cuantos documentos estime oportunos en defensa de sus intereses.

- En el marco de este procedimiento se le permite el acceso al expediente administrativo de conformidad con lo establecido en la Ley Régimen Jurídico y Procedimiento Administrativo Común y en lo previsto en la normativa específica.

Como conclusión la Agencia considera la actuación del INSS y de la Agencia Tributaria se ajusta a la legalidad.

5. 6. 6. SOLICITUD DE DATOS DEL PADRÓN POR LOS PARTICULARES

El Padrón Municipal como registro administrativo donde constan los vecinos de un municipio es uno de los ficheros que gozan de una información más actualizada sobre un conjunto importante de personas. El empadronamiento es obligatorio para los residentes en una determinada localidad y sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. El Padrón contiene como datos obligatorios el nombre y apellidos, sexo, domicilio habitual, nacionalidad, lugar y fecha de nacimiento, número de documento nacional de identidad o, tratándose de extranjeros, del documento que lo sustituya, certificado o título escolar o académico que se posea, y cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, conforme el artículo 16 de la Ley de Bases de Régimen Local.

El segundo párrafo del apartado tercero del artículo 16 de la Ley de Bases establece que los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, y en la Ley 30/1992, de 26 de Noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Existen supuestos en los que el acceso a datos del Padrón no estaría sin más permitido. Es el caso de facilitar datos del padrón a un particular con el fin de conocer el lugar de residencia actual de su hijo y de la madre de éste, para poder ejercer como padre el régimen de visitas un fin de semana cada mes, tal y como lo indica la sentencia judicial. Esta cesión excedería en principio la competencia del Ayuntamiento debiendo solicitarse en este caso por vía judicial. En este sentido, hay que tener en cuenta lo establecido por el artículo 37.2 de la Ley de Régimen Jurídico y Procedimiento Administrativo Común. Este precepto establece lo siguiente:

"*El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas..... "*

Otro ejemplo de este tipo de peticiones improcedentes, se encuentra en la solicitud de una Fundación de cesión de

datos de los nombres, apellido y dirección de los mayores de 65 años del Padrón Municipal a fin de conocer la situación real de las personas dentro del proyecto Plan Gerontológico Público. Dado que las Fundaciones no ostentan la condición de Administraciones Públicas, no podrían ampararse en el art. 19 de la L.O. 5/92 como ley habilitante para esta cesión.

5. 6. 7. FICHEROS DE LA DIRECCIÓN GENERAL DE TRÁFICO

La Base de Datos de Vehículos de la Dirección General de Tráfico se reguló mediante Orden del Ministerio del Interior, el 26 de julio de 1994, y de conformidad con esta norma y la inscripción en el Registro General de Protección de Datos, se establece que este fichero contiene los datos identificativos de los titulares de los vehículos, tales como nombre, apellidos y dirección, al igual que los datos identificativos de los vehículos, datos técnicos, trámites, limitaciones, cargas y eventuales poseedores de los mismos.

Este fichero tiene una gran importancia, dada la cantidad de información que contiene, por lo que ha dado origen a numerosas consultas ante la Agencia en relación con el acceso de terceras personas distintas del afectado (titular de los datos) a los datos relativos a su persona.

La Ley Orgánica 5/92 determina que la cesión de datos por parte de una Administración Pública a un fichero de titularidad privada o a un particular requiere o bien el consentimiento del afectado, o que dicha cesión esté prevista en una Ley.

El artículo 5, apartados d) y h), del texto articulado de la Ley sobre el Tráfico, Circulación de Vehículos de Motor y Seguridad Vial, y el apartado III del artículo 244 del Código de la Circulación, disponen que el Registro que contiene los datos esenciales de los vehículos y su titularidad, será público para los interesados legítimos y terceros mediante simple nota informativa o la expedición de certificación.

En concreto el artículo 244 del Código de la Circulación establece lo siguiente:

"I. En las Jefaturas Provinciales de Tráfico existirá un Registro-Archivo de automóviles, remolques y semiremolques, en el que contarán los datos esenciales de los mismos, la fecha de sus permisos de circulación y cuantas vicisitudes sufran posteriormente aquéllos y su titularidad.

II. La Jefatura Central de Tréfico llevará un Registro General de todos los vehículos sujetos a matrícula y necesitados de permiso de circulación.

III. Los Registros a los que se refieren los párrafos I y II anteriores tendrán carácter puramente administrativo, serán públicos para los interesados legítimos y terceros mediante simples notas informativas o certificaciones, y los datos que figuren en ellos no prejuzgarán las cuestiones de propiedad, cumplimientos de contratos y, en general, cuantas de naturaleza civil puedan suscitarse respecto a los vehículos."

La procedencia de facilitar información sobre los vehículos o sobre la titularidad de ellos viene limitada por el interés legítimo del solicitante. El concepto de interés legítimo requiere la apreciación de las circunstancias del supuesto de que se trate, aunque, en principio, se presume que lo ostenta todo aquél que solicite información de esos Registros de modo individualizado, dado el carácter público de los datos, sin perjuicio de que los encargados puedan exigir su acreditación e incluso denegar la información solicitada cuando por sus circunstancias deba calificarse de abusiva, sin que, por tanto, pueda apreciarse interés legítimo.

La Agencia de Protección de Datos considera que la cesión de sus datos a un tercero por parte de la Dirección General de Tráfico no sería contraria, en principio, a la Ley Orgánica, por haberse realizado al amparo de las normas citadas, que prevén expresamente la cesión.

Por otra parte se han producido reclamaciones de ciudadanos como consecuencia de la cesión de sus datos personales (incluido el domicilio) a particulares y el posterior uso indebido de los mismos. En relación con este tema, la Dirección General de Tráfico ha manifestado que quedan registradas en sus sistemas informáticos, tanto las consultas realizadas por los propios funcionarios de la Dirección General, como las solicitudes de información realizadas por los particulares, por lo que los afectados podrían conocer la identidad de aquellas personas que han sido destinatarias de sus datos personales mediante el ejercicio del derecho de acceso.

5. 6. 8. FICHEROS POLICIALES

La pregunta más frecuente en este ámbito trata sobre los requisitos acreditativos necesarios para la cancelación de antecedentes policiales, tras el cumplimiento de la pena y prescripción de los antecedentes penales.

En este sentido, hay que tener en cuenta lo establecido en el artículo 20.2 de la Ley Orgánica, que determina que 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 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.

Por su parte, el apartado 4 del mismo artículo determina que 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.

El artículo 21 de la Ley Orgánica establece las excepciones a los derechos de acceso, rectificación y cancelación para los ficheros de las Fuerzas y Cuerpos de Seguridad, pudiendo denegarse el ejercicio de estos derechos 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 están realizando. La valoración de estos peligros estará en relación directa con la naturaleza del delito de que se trate.

Esta serie de preceptos aplicados al caso concreto, determinan, por un lado, que la cancelación de los antecedentes policiales que haya dado lugar a una condena concreta requiere la correspondiente certificación negativa de antecedentes penales. Podrían mantenerse estos datos, si se acredita por parte de la Policía que existen otras causas abiertas en las Audiencias o en los juzgados, o que la causa concreta que obra en los archivos policiales ha concluido con auto de sobreseimiento o sentencia absolutoria.

Por último, sería posible evaluar si la cancelación del dato podría implicar 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 están realizando. En todo caso, el ciudadano tiene siempre la posibilidad de recurrir ante la Agencia por la denegación de la cancelación de los datos policiales, que evaluará si el mantenimiento del dato está justificado.

5. 6. 9. SANIDAD Y ASISTENCIA SOCIAL

En este capítulo se tratan las cuestiones relativas al sector de la Sanidad, tanto pública como privada, así como las cuestiones relacionadas con la asistencia social que prestan las Administraciones Públicas a los afectados, en la medida en que los ciudadanos plantean cuestiones a este respecto. Se incluyen las consultas relacionadas con el ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados en relación con su historia clínica.

La importancia de este tipo de consultas es extraordinariamente relevante, desde el punto de vista de la Ley, toda vez que el dato sanitario tiene la consideración de especialmente protegido.

En este ámbito, existe una frecuente contradicción entre los principios de intimidad y de salud pública, que se suele resolver a favor de la intervención pública garante del interés general, establecida en la legislación sanitaria, pero con las limitaciones y garantías de la Ley Orgánica, relativas a adecuación y pertinencia de los datos solicitados en relación con el fin buscado, el cumplimiento del deber de secreto de las personas que tienen acceso a los datos, al igual que la adopción de las medidas técnicas y organizativas que impidan el acceso indebido a los mismos, y, en último término, la garantía de los derechos del afectado.

Además, la realización de estudios epidemiológicos requiere un largo proceso de mantenimiento de datos personales con vistas al seguimiento de las enfermedades, que implica el almacenamiento de datos que reflejan fielmente el estilo de vida del afectado, y en los que informaciones aparentemente irrelevantes pueden adquirir, a la larga, una gran trascendencia.

Esta peculiaridad plantea un conflicto entre el derecho de cancelación de los datos y la necesidad de conservarlos para la realización de estudios epidiomiológicos, para los que el mantenimiento de los datos es imprescindible.

5. 6. 9. 1. HISTORIAL CLÍNICO: DERECHOS DE ACCESO Y CANCELACIÓN

Con carácter previo a la contestación a estas cuestiones, es necesario tener en cuenta que la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal, 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 hospitales públicos. En consecuencia, no se aplicarán los criterios siguientes a los historiales clínicos en soporte papel. Esta observación es especialmente relevante en este ámbito, dado que en el momento presente la mayor parte de los historiales clínicos no se encuentran automatizados.

Las consultas de los ciudadanos plantean si tienen derecho a solicitar copia de su historial clínico en hospital público y copia de todo su historial médico. La Ley Orgánica 5/92 reconoce el derecho de acceso en el artículo 14 que establece:

1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

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 mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible sin utilizar claves o códigos convencionales 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 al afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

También consultan los ciudadanos sobre si tienen derecho a cancelar los datos en el historial clínico de un hospital público una vez finalizado el tratamiento en dicho hospital, planteando además cómo se puede solicitar dicha cancelación, y si existe un plazo mínimo para ejercerla, y finalmente la posibilidad de interponer una reclamación ante la Agencia, en caso de negativa por parte del hospital.

Para la contestación de estas cuestiones hay que tener en cuenta lo establecido en el artículo 15 de la Ley Orgánica relativo al derecho de rectificación y cancelación:

1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.

2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

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 fichero y el afectado.

De lo anteriormente expuesto, se deduce que, aunque existe el derecho de cancelación por parte del afectado, este derecho viene limitado en aquellos supuestos en los que exista un deber de conservación de los datos. Esta restricción para la cancelación de los datos se recoge además en el artículo 22, como otras excepciones a los derechos de los afectados, en el apartado segundo que establece que : *el apartado 1 del artículo 15 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 automatizado 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.*

A este respecto habrá que tener en cuenta lo establecido en la Ley General de Sanidad, en los artículos 8 y 23. En este sentido, el artículo 8 de la Ley General de Sanidad considera como actividad fundamental del sistema sanitario, la realización de los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica.

Por su parte, el artículo 23 de la misma Ley General prevé que para la consecución de los objetivos de la intervención pública en relación con la salud individual y colectiva, las Administraciones Sanitarias, de acuerdo con sus competencias, crearán los Registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria.

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 además por las normas penales y civiles para los supuestos de responsabilidad por posibles negligencias médicas.

5. 6. 9. 2. CESIÓN DE DATOS DE MUFACE AL INSALUD

Se han producido quejas de algunos ciudadanos por la cesión de datos entre el INSALUD y MUFACE para evitar la duplicación de la cobertura sanitaria prohibida por el Ordenamiento Jurídico. Es necesario señalar que la cesión mutua de datos entre INSALUD y MUFACE se ampara en el artículo 19 de la Ley Orgánica, en la medida en que ambas entidades ejercen competencias idénticas. Por todo ello, en el supuesto planteado no sería necesario el consentimiento de los afectados para realizar dicha cesión, que tiene como finalidad legítima el control del cumplimiento de las leyes por

parte de las Administraciones Públicas competentes.

5. 6. 9. 3. PETICIÓN DE DATOS EXCESIVOS PARA ASISTENCIA SOCIAL

En la consulta se plantea a la Agencia si se ajusta a derecho la exigencia por parte del departamento de Bienestar Social de un Ayuntamiento, de que el ciudadano presente fotocopia de todos los movimientos realizados durante el año en la cartilla de ahorro, para solicitar una ayuda domiciliaria. En otras ocasiones el interesado había presentado la declaración de la renta, el certificado de percepciones de la Seguridad Social, las declaraciones de Hacienda de bienes y el recibo del alquiler de la vivienda.

En principio, los datos solicitados podrían ser excesivos y contrarios, en consecuencia, al artículo 4 de la Ley Orgánica. En este supuesto, se trataba de una petición excepcional con el fundamento legal correspondiente, y no de una información que se solicita con carácter habitual a quienes solicitan la ayuda domiciliaria.

No obstante, la Agencia consideró que la solicitud de estos datos era excesiva, carente del suficiente rango legal y contraria a la privacidad, lo que comunicó al Ayuntamiento en cuestión, que aceptó la recomendación.

5. 6. 9. 4. ESTUDIOS FARMACOLÓGICOS

Se ha planteado la legalidad del cupón de respuesta de publicidad de médicos en relación con el grado de intensidad del dolor de sus pacientes y los resultados de un producto analgésico, bien entendido que los datos de salud de los pacientes se envían previamente disociados por el médico, y que los datos que constan en el cupón son tan sólo los datos identificativos del doctor.

La información que solicitan en relación con los pacientes podría ser cedida por los médicos sólo en la medida en que los datos se encuentren disociados y no puedan atribuirse a persona física identificada o identificable. En este supuesto, el fichero resultante tendría la naturaleza de un fichero meramente estadístico, pero incluyendo datos potencialmente identificativos de personas físicas determinadas.

El problema que se podría plantear, es que los datos de las personas pudieran llegar a resultar identificables. En el supuesto de poder resultar identificables, el médico debería solicitar el consentimiento de los afectados para la cesión caso por caso para su proyecto, so pena de incurrir en infracción de la Ley Orgánica.

5. 6. 9. 5. CESIÓN DE DATOS HOSPITALARIOS A LA ADMINISTRACIÓN TRIBUTARIA

Las clínicas privadas consultan a la Agencia sobre el deber de entregar datos de salud a la Agencia Tributaria en el marco de su plan de inspecciones. En concreto son conflictivos el Libro de Registro de Ingresos y Altas de enfermos, Libro de Quirófano, y Libro de Sala de Partos en el que consten datos identificativos del paciente, tales como nombre y apellidos, número de D.N.I., o cualesquiera otros que puedan servir de modo directo o indirecto para la identificación de estas personas, así como los listados que faciliten la relación de enfermos en conexión con el médico.

El artículo 11 de la Ley 5/92, determina que la cesión de datos por parte del responsable del fichero a un tercero se podrá llevar a cabo mediante la autorización previa del afectado, o bien por que se prevea esta posibilidad en una Ley. En este caso la norma en que pretende ampararse la cesión es la Ley General Tributaria en el articulo 111. En este precepto se determina lo siguiente en el apartado 1 párrafo 1º:

1. Toda persona natural o jurídica, pública o privada, estará obligada a proporcionar a la Administración Tributaria toda clase de datos, informes o antecedentes con trascendencia tributaria, deducidos de sus relaciones económicas, profesionales o financieras con otras personas.

Pero esta obligación de carácter general encuentra una excepción aplicable al caso en el apartado 5 de este mismo precepto:

5.La obligación de los demás profesionales de facilitar información con trascendencia tributaria a la Administración de la Hacienda Pública no alcanzará a los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad, cuya revelación atente al honor o a la intimidad personal y familiar de las personas....

Los profesionales no podrán invocar el secreto profesional a efectos de impedir la comprobación de su propia situación tributaria.

Además, los datos relativos a salud son datos especialmente protegidos de conformidad con el artículo 7 de la LORTAD y existe un principio general de confidencialidad de los datos en los artículos 8, 10 y 23 de la Ley 14/1986 de 25 de abril, General de Sanidad, motivo por el que la Agencia considera que los datos relativos a las operaciones quirúrgicas y demás intervenciones médicas en relación con los pacientes, son datos privados no patrimoniales, que los médicos, o el hospital conocen por razón del ejercicio de su actividad, y su revelación atenta contra la intimidad de las personas afectadas.

De lo anteriormente expuesto y en relación con las peticiones concretas de la Agencia Tributaria, se deduce que los Hospitales no podrán aportar información alguna en la que consten datos identificativos del paciente, tales como nombre y apellidos, número de D.N.I., o cualesquiera otros que puedan servir de modo directo o indirecto para la iden-

tificación de estas personas. Por lo que se refiere a los listados solicitados, no se podrá facilitar la relación de enfermos en relación con el médico, dado que esta información puede ser utilizada para averiguar, en efecto, datos relativos a salud, especialmente protegidos por la LORTAD, que carecen de relevancia patrimonial, y afectan a la intimidad de las personas.

Sin embargo, la solicitud por parte de la Agencia Tributaria de las intervenciones de los médicos sin que esta información se relacione, ni se pueda relacionar con los pacientes es conforme con la legislación vigente aplicable al caso y no podría ampararse en la intimidad ni confidencialidad de los historiales clínicos, y sería de aplicación el 2º párrafo del apartado 5º del artículo 111, que no permite a los profesionales ampararse en el secreto profesional para impedir la comprobación de la propia situación tributaria.

5. 6. 10. RELACIONES LABORALES Y DESEMPLEO

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.

El ámbito de las relaciones laborales implica 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, incidencias de la relación laboral, junto a otros relativos a la vida familiar como el estado civil, el número de hijos, o minusvalías

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 a partir del descuento de las cuotas sindicales.

De modo más mediato, las empresas pueden disponer además de datos de salud voluntariamente aportados por el trabajador para su utilización por los servicios médicos de la empresa.

El "fichero de personal", entendido en un sentido amplio, es una de las fuentes originarias de datos personales que alimentan las grandes bases de datos de las Administraciones Públicas, en virtud de las leyes que imponen la obligación, normalmente a los empresarios, de facilitar la información.

De este modo, tenemos un gran número de bases de datos de empresas con gran cantidad y calidad de información, junto con la información almacenada en las grandes bases de datos públicas que en el caso de la Seguridad Social, por ejemplo, agrupan la práctica totalidad de la información sobre trabajadores asalariados, o el Instituto Nacional de Empleo que agrupa a los desempleados.

El panorama se complica más aún si tenemos en cuenta que muchas pequeñas empresas contratan con gestorías la gestión de sus ficheros de personal, que actúan como intermediarios entre las empresas y las Administraciones Públicas. Todo ello sin olvidar el papel imprescindible de intermediación llevado a cabo por el sistema bancario.

Por último, la creación de las Agencias de colocación, tanto públicas como privadas, abre un nuevo frente de almacenamiento de la información relativo a la vida laboral.

El contrato de trabajo como punto de partida de la relación laboral, en el ámbito de la protección de datos, es una excepción de la exigencia del consentimiento para el tratamiento automatizado de los datos, de conformidad con todas las previsiones legales que regulan este sector, siempre que sean necesarias para el mantenimiento de la relación laboral o contractual.

El conocimiento de la vida laboral del trabajador que permiten las técnicas de automatización de la información puede arrojar, con precisión, un perfil socioeconómico y personal que el afectado tiene derecho a mantener reservado.

Las consultas planteadas a la Agencia en relación con cesiones de datos a representantes de trabajadores y sindicatos se han solucionado, con carácter general, con base en lo dispuesto en el artículo 11 que exige el consentimiento del afectado o la existencia de una ley, y por tanto, en la mayoría de los supuestos, poniendo en juego la Ley Orgánica de Libertad Sindical y el Estatuto de los Trabajadores, con la L.O. 5/95 y la existencia o no del consentimiento del afectado.

5. 6. 10. 1. CESIONES DE DATOS DE LA EMPRESA A LOS SINDICATOS.

Como ya hemos señalado, el artículo 11 de la Ley Orgánica exige con carácter general la necesidad del consentimiento del afectado para las cesiones, salvo que la cesión esté prevista por una ley.

En este sentido, en el artículo 11 de la Ley Orgánica de Libertad Sindical se prevé que el empresario proceda al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado, y previa conformidad siempre de éste, por lo que la cesión de datos por parte del empresario se circunscribe, exclusivamente, a los datos estrictamente necesarios para cumplir la obligación de pagar la cuota. Para los datos que excedan del cumplimiento de la misma será necesario además el consentimiento del trabajador así como la conformidad del empresario.

También se consulta sobre la legalidad de entregar al Comité de empresa la copia básica del contrato, con el detalle de

los salarios de los trabajadores, porque el empresario entiende que la entrega de esta información podría afectar a la intimidad personal de conformidad con la Ley Orgánica 1/1982, de 5 de mayo, relativa a la protección del honor y la intimidad.

El artículo 11 de la LORTAD regula las cesiones y establece con carácter general la necesidad del consentimiento del afectado para la cesión. Es posible, no obstante, que la cesión se prevea en una norma que tenga rango de Ley. En este sentido, el artículo 8 del Estatuto de los Trabajadores del Real Decreto Legislativo 1/1995 de 24 de marzo(por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores), relativo a la forma del contrato establece lo siguiente, en el apartado tercero:

3. a) El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores.

Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad, el domicilio, el estado civil y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, pudiera afectar a la intimidad personal.

La copia básica se entregará por el empresario, en un plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega. Posteriormente, dicha copia básica se enviará a la oficina de empleo. Cuando no exista representación legal de los trabajadores también deberá formalizarse copia básica y remitirse a la oficina de empleo.

En los contratos sujetos a la obligación de registro en el Instituto Nacional de Empleo la copia básica se remitirá, junto con el contrato, a la oficina de empleo. En los restantes supuestos se remitirá exclusivamente la copia básica.

b) Los representantes de la Administración, así como los de las organizaciones sindicales y de las asociaciones empresariales, que tengan acceso a la copia básica de los contratos en virtud de su pertenencia a los órganos de participación institucional que reglamentariamente tengan tales facultades, observarán sigilo profesional, no pudiendo utilizar dicha documentación para fines distintos de los que motivaron su conocimiento.

El Preámbulo de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal establece que: *El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.*

Por lo que se refiere a la Ley Orgánica 1/1982 de 5 de mayo, en el artículo 2º apartado 2 se establece que: *No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiese otorgado al efecto su consentimiento expreso.*

A este respecto, el Tribunal Constitucional ha señalado en su Sentencia de 22 abril 1993, dictada en el Recurso 190/1991, que el acceso a la información relativa a la retribución no permite en modo alguno la reconstrucción de datos del trabajador incluidos en la esfera de su intimidad, datos retributivos que pueden ser conocidos por los representantes de los trabajadores en uso de las facultades que les confiere el artículo 64.1.8.a) del Estatuto de los Trabajadores (en el texto refundido es el 64.9.a), sin que con ello se viole derecho constitucional alguno.

De lo anteriormente expuesto, se deduce que las empresas deberán entregar al Comité de Empresa la información solicitada, dado que así se encuentra previsto en el Estatuto de los Trabajadores, y dado que la esfera de la intimidad que se trata de proteger mediante la Ley Orgánica 1/1982, de 5 de mayo, no se extiende a los datos laborales que se solicitan en este caso.

5. 6. 10. 2. PROCESAMIENTO DE DATOS DE SALUD CON MOTIVO DE REVISIONES MÉDICAS EN LAS EMPRESAS.

Se plantea a la Agencia de Protección de Datos la legalidad de procesar los datos de salud del personal de un organismo, efectuadas con motivo de las revisiones médicas en las empresas, sin el consentimiento del afectado, a pesar de su carácter de datos especialmente protegidos. A este respecto, argumentan que el artículo 6. 2 de la Ley Orgánica excepciona del consentimiento a aquellas personas vinculadas por una relación laboral, así como que el artículo 8 de la Ley Orgánica exime de la necesidad de recabar el consentimiento previo a los centros sanitarios públicos y privados

y los profesionales de la salud correspondientes para que puedan proceder al tratamiento automatizado de los datos de carácter personal de conformidad con lo dispuesto en las diversas leyes sanitarias.

La ley aplicable al caso sería la 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, que regula los servicios médicos de las empresas y Administraciones con carácter general. Su artículo 22 establece la vigilancia periódica del estado de salud de los trabajadores en función de los riesgos inherentes al puesto de trabajo como un derecho de los mismos. Además señala que: "*Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad".*

En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo.

2. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre 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.

.....

4. Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador .El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

En conclusión, la Agencia entiende que es necesario solicitar el consentimiento del afectado con carácter general para proceder a la informatización de sus datos de salud, salvo en los supuestos en que la obtención y tratamiento de los mismos sean necesarios para el mantenimiento de la relación laboral, de conformidad con los artículos 6 y 8 de la Ley Orgánica 5/92, salvo lo dipuesto en el artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

5. 6. 10. 3. DENEGACIÓN DE DATOS DE INCAPACIDAD LABORAL TRANSITORIA (I.L.T). A LOS DELEGADOS DE PREVENCIÓN POR PARTE DE LA EMPRESA.

Los Delegados de Prevención han solicitado a la Dirección de su empresa la relación anual del año 1997 de las situaciones de I.L.T. indicando nombre y apellidos, diagnóstico o patología, categoría laboral, lugar de trabajo, y fecha de inicio y terminación de la baja así como el cómputo total de los días de aquélla. La finalidad de esta petición consiste en analizar las causas de las bajas laborales y las irregularidades detectadas consistentes, al parecer, en la transformación de accidentes de trabajo en bajas por enfermedad común tanto desde el primer parte de baja, como en caso de recidiva. La Dirección de la empresa se niega a incluir en la relación citada el nombre y apellidos de los trabajadores y el lugar del accidente de trabajo.

La pregunta que se formula es si la Ley ampara la negativa de la Empresa, o por el contrario legitima la petición de los Delegados de Prevención solicitantes. Y ,en el caso de que la negativa de la empresa resulte legítima, desean conocer cuál es la vía o procedimiento para la investigación del supuesto fraude empresarial y el análisis de las causas del absentismo sin vulnerar la Ley, dado que consideran imprescindible la relación nominal de trabajadores para combatir el supuesto fraude indicado.

La ley sanitaria aplicable al caso sería la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales que regula los servicios médicos de las empresas y Administraciones con carácter general.

Tal y como se indica en el apartado cuarto del artículo 22 de la Ley 31/95 de Prevención de Riesgos Laborales, el acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

El empresario y las personas u órganos con responsabilidades en materia de prevención (los representantes sindicales) serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia

preventiva.

A tenor de lo establecido en estos preceptos, la negativa a entregar la relación nominal de los trabajadores parece conforme con la legislación aplicable al caso.

5. 6. 10. 4. CARÁCTER ADECUADO DE SOLICITUD DEL DOMICILIO DE LOS TRABAJADORES POR PARTE DE LA EMPRESA

Se plantea ante la Agencia la legalidad de la solicitud del domicilio del trabajador en lugar de un apartado de correos, para su inclusión en la base de datos de la empresa, alegando que el domicilio puede ser preciso para su localización por parte de la empresa.

El Tribunal Constitucional ha argumentado (Sentencia 99/1994) que la relación laboral tiene como efecto la sumisión de ciertos aspectos de la vida del trabajador a las necesidades de la organización productiva, pero no bastaría afirmar el interés empresarial para comprimir los derechos fundamentales del trabajador. Esto determina que el uso de la información sobre los trabajadores por parte de la empresa debe estar plenamente justificado por las necesidades del puesto de trabajo.

No obstante, la dirección del trabajador es un dato que el empresario necesitaría para el desarrollo de la relación contractual, dado que en algunos modelos oficiales de contratación de los contratos como el de prácticas, de aprendizaje o a tiempo parcial se requiere el dato del domicilio del trabajador. Este modelo debe sellarse por parte del INEM. También el empresario debe conocer el domicilio del trabajador a afectos de la cumplimentación de los modelos oficiales de Alta en la Seguridad Social, por ejemplo. En cambio, en la entrega que de la copia básica de los contratos se debe hacer a los representantes de los trabajadores, se excluye el dato del domicilio para preservar la intimidad. Existen numerosas normas en el ámbito laboral que implican el conocimiento del domicilio por parte del empresario a estos efectos.

En el ámbito del cumplimiento de las obligaciones laborales en sentido estricto, la obligación de facilitar el cambio del domicilio por parte del trabajador vendrá motivada por la necesidad de esta información para el desempeño del puesto en cuestión, de conformidad con lo establecido en el artículo 4 de la Ley Orgánica, que establece que los datos han de ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que se obtuvieron.

Como conclusión, hay que señalar que no parece que la solicitud del dato del domicilio, con la matizaciones expuestas contradiga la legislación vigente, si se cumplen los requisitos expuestos, toda vez que la información personal se solicita en el medio laboral exclusivamente, en el marco de una relación contractual y para un fin de tipo laboral.

5. 6. 10. 5. LEGALIDAD DE LA PUBLICACIÓN DE UNA GUÍA DE LOS TRABAJADORES INCLUYENDO LA FOTO EN LA RED INTERNA DE LA EMPRESA.

Se consulta sobre la legalidad de difundir una guía de datos de empleados, en la que figure una fotografía digitalizada de cada empleado en el WEB interno de la empresa y, en su caso, si es posible solicitar que eliminen la fotografía basándose para ello en alguna ley o disposición al respecto, bien entendido que se trate de información de uso interno.

La fotografía asociada con un nombre e incluida en un fichero automatizado tiene el carácter de dato personal, de conformidad con el articulo 1 del Real Decreto 1332/1994, y la Ley Orgánica 5/92. En este precepto, en su apartado cuatro, se establece que serán considerados datos de carácter personal: 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.

La Sentencia del Tribunal Constitucional de 22 abril 1993, en el 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 consecuencia, la identidad (de la que la imagen fotográfica es un importante atributo) no tiene por qué vedarse dentro de una relación laboral, y la muestra de la identidad del trabajador, que actúa en relación directa con sus compañeros de empresa puede resultar necesaria para la adecuada comunicación entre el personal de una determinada empresa, por lo que la inclusión del dato podría resultar adecuada y proporcional al fin lógico de una guía de empleados de la empresa.

No obstante, el Tribunal Constitucional ha argumentado (Sentencia 99/1994) que la relación laboral tiene como efecto la sumisión de ciertos aspectos de la vida del trabajador a las necesidades de la organización productiva, pero no bastaría afirmar el interés empresarial para comprimir los derechos fundamentales del trabajador. Por ello, los requerimientos de la empresa aptos para restringir el ejercicio del derecho a la intimidad y a la propia imagen, han de estar especialmente cualificados por razones de necesidad estricta, que debe ser acreditada. Esto determina que otros usos de la información de la guía de los trabajadores de cara al exterior por parte de la empresa deben estar plenamente justificados por las necesidades del puesto de trabajo. En este sentido, el derecho a la imagen de los empleados impediría al empresario su difusión de cara a terceros distintos de los propios empleados, salvo en los supuestos de contacto con el público, o en posiciones accesibles al mismo.

Como conclusión, hay que señalar que no parece que el comportamiento descrito contradiga por sí mismo la legislación vigente, si se cumplen los requisitos expuestos, toda vez que la información personal que se difunde se hace en el medio laboral exclusivamente y en el marco de una relación contractual.

5. 6. 11. PROYECTOS DE INVESTIGACIÓN GENEALÓGICA

La investigación genealógica por encargo plantea diversas cuestiones en relación con la protección de datos. En este ámbito, se pueden distinguir la investigación ascendente y la descendente. En la primera, relativa a las personas fallecidas la Ley Orgánica se aplicaría de modo muy limitado, ya que el artículo 2 de la misma limita su ámbito de aplicación a las personas físicas, condición que se pierde con el fallecimiento. El problema se plantea, más concretamente, en la investigación descendente, por lo que se refiere a personas físicas contemporáneas con las que éstas puedan aparecer emparentadas, así como los usos médicos que pueden unir la genealogía con la genética, con el fin de poder determinar enfermedades hereditarias, y las consecuencias potenciales sobre el sujeto.

Existe en primer lugar la obligación de los titulares de los archivos de comunicar a la Agencia la existencia de ficheros informatizados de árboles genealógicos en tanto que contienen datos relativos a personas físicas vivas en sus sistemas.

A este respecto, estarían excluidos del ámbito de aplicación de la Ley Orgánica, de conformidad con el artículo 2.3 c), los datos derivados del Registro Civil que se rigen por su legislación específica. Ahora bien, la automatización de esta información en combinación con otros datos entra plenamente dentro del ámbito de aplicación de la Ley.

Por lo que se refiere a los datos de descendientes que viven en la actualidad, será necesario el consentimiento a que se refiere el artículo 6 de la Ley Orgánica, que exige dicho consentimiento para el tratamiento automatizado, salvo que la información se haya obtenido en una fuente de las que la Ley Orgánica y el Reglamento definen como fuente accesible al público.

Además si los datos recabados son especialmente protegidos, tales como religión obtenida de los archivos parroquiales, o bien datos de salud, será necesario el consentimiento expreso de los afectados, o de los herederos en su caso.

5. 6. 12. COLEGIOS PROFESIONALES.

La 2/74 Ley de Colegios Profesionales, de 13 de febrero, con sus modificaciones posteriores, establece el carácter obligatorio de la colegiación para poder ejercer ciertas profesiones. Los Colegios Profesionales suelen publicar las listas de sus colegiados para dar a conocer a sus miembros, y al público en general, el hecho de que una persona, con las titulaciones legalmente exigidas, pertenece a un determinado grupo profesional. La publicación de estos datos está amparada, en muchos casos, por los Estatutos de cada Colegio Profesional

La utilización de estos datos para fines comerciales o de otro tipo, que tiene un carácter masivo, ha sido causa de frecuentes consultas y quejas por parte de los colegiados, dado que entienden que ésta no es la finalidad de la colegiación, ni de la publicación de los listados de colegiados.

La colegiación obligatoria prevista por el Ordenamiento Jurídico para determinadas profesiones, combinada con las técnicas automatizadas del tratamiento de los datos, convierte a estos ficheros en una fuente de información de gran utilidad para la publicidad directa, para el control fiscal por parte de las Administraciones Tributarias, o el de incompatibilidades de funcionarios.

El artículo 11 de la Ley Orgánica 5/92, en conexión con el artículo 1 del Real Decreto 1332/94 de desarrollo de la Ley Orgánica, otorga la consideración de fuentes accesibles al público a los datos publicados en forma de listas de personas pertenecientes a un grupo profesional.

La publicación de los listados de colegiados que realizan algunos Colegios Profesionales, plantea problemas en relación con el principio del consentimiento establecido en la Ley Orgánica, que, referido a la publicación del listado de colegiados, debe entenderse limitado a determinados datos personales que resultan indispensables para el ejercicio de la profesión, como nombre, apellidos o domicilio profesional. Para la publicación de otros datos personales sería indispensable la prestación del consentimiento del titular de los datos.

No obstante, el colegiado tiene la posibilidad de dirigirse a su Colegio Profesional para solicitar la exclusión de sus datos personales de las listas publicadas, de modo análogo a lo establecido en el artículo 26 de la Ley Orgánica 5/92 para los abonados a los servicios de telecomunicación.

MEMORIA DE 1997 - CÓDIGOS TIPO

Las actividades realizadas durante 1997, en cumplimiento de lo previsto en el artículo 31 de la Ley Orgánica 5/1992, en relación con la inscripción de códigos tipos no ha ocasionado nuevas inscripciones en el Registro General de Protección de Datos.

Durante este año se han iniciado dos nuevos expedientes correspondientes a los dos nuevos códigos tipo depositados en el Registro para los que se solicitaba su inscripción.

Por una parte, la primera de las solicitudes recibidas, que realmente tuvo su entrada en 1996, aunque la tramitación para su inscripción se ha realizado en 1997, corresponde al Código de Conducta del Fichero Informativo de Automóviles (F.I.A.), presentado por la Asociación ICEA de Investigación Cooperativa entre Entidades Aseguradoras. Sin embargo, no ha sido posible realizar la inscripción, pues tras varias modificaciones en la redacción de este Código, aún han quedado algunos aspectos que plantean problemas de adecuación a la Ley Orgánica 5/1992, y al no haber sido subsanados por el responsable del Código tipo han impedido su inscripción.

Por otra parte, en julio de 1997, se recibió de la Asociación Española de Marketing Directo, el código tipo regulador de las Listas Robinson, del que una vez analizado, se desprenden una serie de cuestiones, que no parecen garantizar los principios de la Ley Orgánica 5/92.

En ambos casos, la tecnología empleada es el principal incoveniente que impide garantizar la calidad de los datos, pues se distribuyen en soportes magnéticos, a los que resulta practicamente imposible realizar un seguimiento, que evite la obsolescencia de su información, y en ningún caso estaban aportando mayores garantías de lo ya establecido en la legislación básica.

MEMORIA DE 1997 - ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES DE LOS DISTINTOS PAÍSES EN MATERIA DE PROTECCIÓN DE DATOS.

1. DIRECTIVA MARCO

El artículo 29 de la Directiva crea el Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales. Éste se compone de un representante de la autoridad de control designada por cada estado miembro, actuando, en representación de España, la Agencia de Protección de Datos.

Entre los cometidos del Grupo figuran el conseguir una aplicación homogénea de la propia Directiva en los países miembros, y estudiar el nivel de protección existente dentro de la Comunidad y en los países terceros.

De conformidad con lo establecido en el art. 29.5 de la Directiva, la D:G. XV, de la Comisión Europea, desempeña las funciones de Secretaría del Grupo.

El Grupo de Protección de las personas en lo que respecta al tratamiento de datos personales, al que se refiere el artículo 29 de la Directiva 95/46/CE, ha venido reuniéndose con regularidad en el año 1997.

De entre las múltiples actividades realizadas en dicho período, merecen ser comentadas las siguientes: las tareas dirigidas a llevar a cabo la transposición de la Directiva dentro de cada una de las legislaciones nacionales; el establecimiento de las primeras orientaciones sobre transferencias de datos personales a países terceros; el estudio de los problemas que plantea la aplicación del artículo 9 de la Directiva, en cuanto se refiere al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria y los problemas que plantea la aparición de Internet.

A) Transposición de la Directiva 95/46/CE

El Grupo, en esta materia, ha venido efectuando un seguimiento constante cada vez que se ha reunido. Se ha constatado dentro del mismo una doble preocupación: por un lado, tratar de cumplir del plazo legal establecido para la transposición que, conforme al artículo 32 de la Directiva, finaliza el 24 de octubre de 1998; por otro, vigilar para que, en la medida de lo posible, las tareas de transposición no incrementen las diferencias en la actualidad existentes entre las diversas legislaciones en materia de protección de datos personales, de manera que hagan inviable el deseo de eliminar los obstáculos a la circulación de datos personales, haciendo posible, como señala el considerando octavo de la Directiva, que el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, sea equivalente en todos los Estados miembros.

Debe recordarse que son dos los países que ya han efectuado la transposición de la Directiva a su derecho interno: Italia, mediante la Ley 675/96, de 31 de Diciembre, Boletín Oficial de 8 de Enero de 1997 y Grecia, por Ley 2472/97, Gaceta de 24 de Octubre de 1997.

En cuanto al cumplimiento del plazo fijado para la transposición, la mayoría de los países integrantes del Grupo calculan que los Proyectos de Ley, que en la actualidad ya se encuentran en los respectivos Parlamentos, lograrán su aprobación inmediatamente después de las vacaciones de verano. En España, las actuaciones dirigidas a efectuar la transposición se encuentran algo más retrasadas, si bien este tema concreto será desarrollado al tratar de manera particular la situación de la protección de datos personales dentro de nuestro país.

Por último, debe señalarse que las tareas de transposición en esta materia no se agotan con las que se refieren específicamente a la Directiva 95/46/CE, sino que a las mismas deben añadirse, igualmente, las que sean necesarias para incorporar a nuestro 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, ya que el artículo 15.1 de ella impone a los Estados miembros la obligación de poner en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma a más tardar el 24 de octubre de 1998. La fijación de una misma fecha para llevar a cabo la incorporación de ambas Directivas a los derechos internos de los países miembros no es mera coincidencia, sino la constatación una vez más de la obligada remisión de toda la normativa europea en favor de la Directiva Marco cuando la materia que se regule afecte directa o indirectamente a la protección de los derechos y libertades fundamentales a los que se refiere aquélla. Por ello, no debe extrañar que el artículo 14.3 de la Directiva en materia de Telecomunicaciones (97/66/CE) atribuya al Grupo del artículo 29 la competencia necesaria para ejercer las funciones especificadas en el artículo 30 de la Directiva 95/46/CE.

B) Orientaciones que, a juicio del Grupo del artículo 29 de la Directiva Marco, se hace necesario establecer en materia de las transferencias internacionales de datos.

Una de las mayores preocupaciones del Grupo del artículo 29 se centra en el alcance y orientación que debe darse al contenido de los artículos 25 y 26 de la Directiva 95/46/CE, en cuanto se refieren a la regulación de las transferencias internacionales de datos.

a) Introducción

Considera el Grupo que, si bien es imposible abordar todas las cuestiones que puedan surgir en relación con dichos preceptos, es necesario analizar los aspectos concretos que se consideran más importantes. De entre los mismos, el Grupo muestra una especial preocupación respecto del significado y alcance que ha de darse al término **adecuación**, al que se refieren los apartados 1 y 2 del artículo 25 de la Directiva. Queda fuera del examen efectuado, el estudio de las excepciones al requisito de "nivel de protección adecuado", al que dedicará la atención en el futuro, ya que no considera necesario llevarlo a cabo en este momento, por entender que la formulación de las excepciones contenidas en el artículo 26 es bastante limitada y que probablemente existirán un gran número de casos que caigan fuera de su alcance.

Ahora bien, con carácter previo, señala que no hay que olvidar que el término "adecuado" también se utiliza en el apartado 2 del artículo 26, que prevé la posibilidad de soluciones ad hoc, especialmente de naturaleza contractual, para situaciones donde exista una falta de protección adecuada con arreglo al apartado 2 del artículo 25. No obstante, entiende el Grupo, que desde el punto de vista procedimental, la Directiva trata estos casos de forma diferente: así, mientras que en virtud del artículo 25 los Estados miembros deberán notificar a los demás Estados miembros y a la Comisión los casos donde no se garantiza una protección adecuada y por lo tanto se bloquea la transferencia, por aplicación del artículo 26 la situación se invierte y los Estados miembros deberán informar a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan.

b) Cuestiones Procedimentales

Partiendo de que el artículo 25 prevé un enfoque caso por caso en el cual la evaluación de la adecuación se realiza para cada transferencia individual o categorías individuales de trasferencias, entiende el Grupo que, dado el gran número de transferencias de datos personales que salen y saldrán de la Comunidad diariamente y la multitud de participantes en las mismas, ningún Estado miembro, con independencia del sistema que escoja para aplicar el apartado 1 del artículo 25, podrá garantizar el examen detallado de cada uno de los casos que se le presenten. Se hará, por tanto, necesario el desarrollo de mecanismos que racionalicen el procedimiento de toma de decisiones. Dicha racionalización se efectuará con independencia de quien sea el que tome la decisión, ya sea el controlador de los datos, la autoridad de control o algún otro organismo establecido por los Estados miembros.

Como posibles soluciones a dicho problema, el Grupo analiza fundamentalmente dos:

* **Listas Blancas.**

La elaboración de una "lista blanca" de países terceros, de los que puede presumirse que garantizan un nivel de protección adecuado, es evidentemente un mecanismo útil para poder lograr esta racionalización.

Es claro que la lista podría ser "provisional" o "únicamente orientativa", dejando al margen los casos específicos que puedan presentar dificultades concretas. La dificultad mayor que puede presentar este procedimiento radica en el hecho de que muchos países terceros no tienen una protección uniforme en todos los sectores económicos. Así, si se examina las listas que el Consejo de Europa elabora para señalar las características que ofrecen las legislaciones de protección de datos en cada país, se observa que muchos tienen legislaciones en esta materia en el sector público pero no en el privado. En Estados Unidos la situación es más compleja, dado que existen leyes específicas para áreas concretas, tales como la información sobre créditos y los registros de alquiler de videos, pero no en otros. Además, los países que tienen constituciones federales no suelen presentar una uniformidad en la materia de protección de datos personales, existiendo a menudo diferencias entre los distintos países que componen una federación.

Surge igualmente el problema de determinar quién debería tomar la decisión relativa a la inclusión en la lista. El Grupo del artículo 29 reconoce que no tiene competencias en esta materia, ya que la función aparece encomendada, en primer lugar, a los Estados miembros y, posteriormente, a la Comisión en virtud del procedimiento establecido en el artículo 31 de la Directiva. No obstante, el Grupo admite que cualquier trabajo que realice en esta materia producirá cuando menos el ejercicio de proporcionar una orientación relativa a una amplia gama de casos, todo ello sin perjuicio de su facultad de emitir dictámenes, conforme al artículo 31. Por último, debe señalarse que, la no inclusión en la "lista blanca", no supone que automáticamente se encuentre en la "lista negra", sino que aún no se dispone de una orientación general relativa a dicho país.

* **Análisis de riesgos de transferencias específicas.**

La utilización del anterior sistema no supone la eliminación de otros muchos supuestos en donde el país tercero en cuestión no figura en la lista blanca. La forma en que los Estados miembros traten los mismos dependerá mucho de la manera en que se incorpore al Derecho nacional el artículo 25 de la Directiva. Así, si se otorga a la autoridad nacional de control la función específica de autorizar transferencias de datos (como es el caso de nuestro país, conforme a los artículo 32 y 33 de la Ley Orgánica 5/1992) el sistema podría adoptar la forma de un conjunto de criterios que permitirían considerar que una transferencia concreta o una categoría de transferencias suponen una amenaza real a la vida privada.

En el futuro, un Grupo de Trabajo elaborará un documento más específico y detallado señalando las categorías de transferencias que considera plantean riesgos específicos a la vida privada. A titulo de ejemplo, pueden señalarse:

- Aquellas transferencias que afecten a categorías sensibles de datos, definidas en el artículo 8 de la Directiva.
- Transferencias que supongan un riesgo de pérdida financiera (por ejemplo, pago con tarjetas de crédito por Internet).

- Transferencias que supongan un riesgo a la seguridad personal.
- Transferencias realizadas a efectos de tomar una decisión que afecte significativamente al individuo (tales como decisiones de contratación o promoción, concesión de créditos, etc).
- Transferencias que supongan un riesgo de afectar a la reputación del individuo.
- Transferencias que puedan utilizarse en acciones concretas que constituyan una considerable invasión de la vida privada de los individuos, tales como las llamadas telefónicas no deseadas.
- Transferencias repetitivas que supongan grandes volúmenes de datos (tales como datos de transacciones procesados en redes de telecomunicaciones).
- Transferencias que impongan la recogida de datos de forma especialmente cubierta o clandestina (por ejemplo "Chivatos" (cookies) Internet).

c) Alcance de la expresión "protección adecuada".

Para el Grupo, el objeto de la protección de datos es proporcionar seguridad a los individuos cuyos datos son procesados. Ello se logra básicamente mediante una combinación de derechos para el sujeto de los datos y de obligaciones para aquellos que los procesan. Es claro que los derechos y obligaciones establecidos en la Directiva 95/46/CE se basan en los establecidos en el Convenio del Consejo de Europa número 108 (1981), que a su vez son parecidos a los incluidos en las directrices de la OCDE (1980) o en las orientaciones de la ONU (1990).

La expresión "protección adecuada" es entendida por el Grupo, utilizando como punto de partida a la Directiva 95/46/CE, ya que es la única de los textos anteriormente citados que incluye aspectos procedimentales referidos a disposiciones sobre responsabilidad, sanciones, recursos, autoridades de control y de notificación, como un requisito mínimo para que la protección pueda considerarse eficaz. Esta lista mínima debería contener los principios básicos siguientes:

1. **El principio de limitación del propósito**: los datos deberán tratarse para un propósito específico o comunicarse posteriormente únicamente en la medida en que ello no sea incompatible con el propósito de la transferencia. Las únicas excepciones a este principio, serían las establecidas en el articulo 13 de la Directiva 95/46/CE, que son las que se consideran necesarias dentro de una sociedad democrática.

2. **La calidad de los datos y el principio de la proporcionalidad**: los datos deberán ser exactos y, cuando sea necesario, actualizados. Los datos, además, deberán ser adecuados, pertinentes y no excesivos en relación al objeto por el que transfieren o tratan.

3. **El principio de transparencia**: deberá proporcionarse a los individuos información respecto al propósito del tratamiento y a la identidad del controlador de datos en el país tercero, así como cualquier otra información que sea necesaria para garantizar la equidad.

4. **El principio de seguridad**: el controlador de los datos deberá adoptar las medidas pertinentes que garanticen la seguridad.

5. **Los derechos de acceso, rectificación y cancelación**: el titular de los datos deberá tener derecho a obtener una copia de todos los datos de él que sean tratados. Igualmente se le deberá reconocer su derecho a rectificar dichos datos cuando resulten inexactos. En determinadas ocasiones se le deberá reconocer el derecho a oponerse a un determinado tratamiento.

6. **Restricciones a las transferencias sucesivas a otros países terceros**: las transferencias sucesivas de datos personales a partir del país tercero de destino a otro país tercero únicamente se admitirán cuando el segundo país tercero también garantice un nivel adecuado de protección.

Por otra parte, se trata de identificar los objetivos subyacentes de un sistema procedimental de protección de datos, que para el Grupo se concentran fundamentalmente en tres:

1. **Proporcionar un buen nivel de cumplimiento de las normas**, que necesariamente exigirá un elevado nivel de concienciación entre los controladores de datos respecto de sus obligaciones por un lado, y entre los sujetos (titulares) de los datos respecto de sus derechos y su forma de ejercicio, por otro.

2. Proporcionar **apoyo y ayuda a los sujetos de datos individuales** en el ejercicio de sus derechos. Los individuos deber ser capaces de ejercer sus derechos de forma rápida y eficaz, sin costes prohibitivos.

3. Proporcionar una **reparación adecuada** a las partes perjudicadas en los supuestos de incumplimiento de las normas en las que se basa la transferencia internacional.

d) Aplicación de la teoría anterior a la práctica española en materia de protección de datos

Como se expone en otro lugar de la presente Memoria, la Agencia de Protección de Datos ha venido autorizando solicitudes de transferencias de datos a terceros países, por lo que se ha visto obligada a interpretar los artículos 32 y 33 de la Ley Orgánica 5/1992, de 29 de octubre.

En dicha tarea, ha querido evitar siempre, por un lado que se produjeran desviaciones no queridas por el legislador en

la aplicación de los principios contenidos en el artículo 4 de la Ley Orgánica, o disminuciones en el ejercicio de los derechos, que hicieran prácticamente imposible el ejercicio de los mismos. Así, por un lado, ha exigido que se especificara la finalidad perseguida con la trasferencia de los datos personales; por otro, ha otorgado al consentimiento del titular del dato, el efecto de excluir la autorización previa, ante el silencio que del mismo guarda el artículo 33 de la Ley Orgánica 5/1992, a diferencia de lo que ocurre en la Directiva conforme a lo establecido en el artículo 25.a) de la misma (salvo "que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista"); por último, ha exigido formalmente el respeto a los principios de proporcionalidad, exactitud y cancelación de los datos.

Igualmente ha tratado de establecer unas garantías, a modo de mecanismos procedimentales, que aseguren la pervivencia de aquéllos. Así, se ha buscado, como requisito sine qua non, hacer efectivo el ejercicio de los derechos de acceso, rectificación y cancelación desde nuestro propio país, evitando que la aplicación de cualquier otro sistema, aún cuando fuera gratuito, pudiera suponer en la práctica una restricción tácita de dicho ejercicio. Consecuentemente con lo anterior, ha tratado de mantener dentro del territorio nacional a un interlocutor válido que pudiera dar respuesta efectiva a los problemas que pudieran derivarse de dicha transferencia y que, en principio, también hicieran posible el cumplimiento de la sanción impuesta que, tendría como destinatario la empresa o persona solicitante que es la que, en su momento, formuló la solicitud y asumió el cumplimiento de tales obligaciones.

En la elaboración de las disposiciones correspondientes dictadas como consecuencia de lo establecido en el Real Decreto 1332/1994, el Ministerio de Justicia e Interior aprobó la Orden de 20 de febrero de 1995, en la que se establecía una lista de países que se consideraban que ofrecían un nivel de protección suficiente a efectos de autorizar las transferencias internacionales. Dicha elaboración tomó como referencia la lista de países que habían ratificado el Convenio 108 del Consejo de Europa en aquella fecha . El criterio seguido en la citada Orden Ministerial es el propuesto por el Grupo de Trabajo para proceder a dar aplicación a lo dispuesto en los artículos 25 y 26 de la Directiva ya que, a juicio del mismo, tal proceder, por lo que respecta al contenido de los principios básicos, cumpliría con las cinco primeras de las "seis condiciones mínimas" anteriormente establecidas. El Convenio incluye igualmente el requisito de la protección adecuada para los datos sensibles, que debería ser un requisito para la adecuación por lo que a estos datos se refiere.

Al margen del problema que pueda suscitarse ante la distinta redacción que establece la Ley orgánica 5/1992 y la Directiva, en cuanto que la primera habla de "nivel de protección equiparable", mientras que la segunda alude, como ya se ha dicho, a "nivel de protección adecuado" parece que en virtud de esta última disposición serían posibles tres tipos de transferencias:

a) Una comunicación de datos personales por un controlador de datos basado en la Comunidad Europea a otro controlador de datos establecido en un país tercero.

b) Una comunicación de datos personales efectuada por un controlador de datos establecido en la Comunidad a un procesador de un país tercero que procese en nombre de un controlador establecido en la Comunidad.

c) Una comunicación de datos personales por parte de un sujeto (titular) de datos establecido en la Comunidad a un controlador de datos establecido en un país tercero.

Al ser distintas las situaciones que se acaban de enunciar debe ser igualmente distinto el tratamiento que se aplique para cada uno de los supuestos.

C) Problemas que puede plantear la aplicación del artículo 9 de la Directiva.

El artículo 9 de la Directiva establece que en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

Pues bien, la futura aplicación de dicho precepto a cada una de las legislaciones internas de los diversos países ha producido preocupación entre las Autoridades que componen el Grupo del artículo 29 de la Directiva. Ello ha determinado, ante las evidentes diferencias existentes en las leyes nacionales en cuanto a la aplicación de las disposiciones relativas a la protección de datos a los medios de comunicación, que se llevara a cabo un estudio acerca de la situación legal actual, estudio que se efectuó a partir de un cuestionario preparado por el Grupo con fecha 21 de febrero de 1996.

El resultado de dicho cuestionario permitió establecer tres grandes grupos de países:

- Aquellos cuya normativa de protección de datos no contenía ninguna exención expresa en cuanto a la aplicación de sus disposiciones a los medios de comunicación. Esta es la situación actual en Bélgica, España, Portugal, Reino Unido y Suecia.
- Aquellos en que se eximía a los medios de comunicación de la aplicación de varias disposiciones de la normativa de protección de datos. Esta es la situación actual en Alemania, Austria, Finlandia, Francia y los Países Bajos.
- En otros supuestos, se eximía a los medios de comunicación de la normativa general reguladora de la protección de datos, sometiéndolos a disposiciones específicas de Protección de Datos. Este es el caso de Dinamarca, para todos los medios de comunicación, y de Alemania, en relación con las emisoras públicas que no están cubiertas por las leyes de protección de datos federales o de los Länder, pero sí están sujetas a las disposiciones específicas de protección de datos contenidas en los tratados suscritos entre los Länder que las regulan.

De todos modos, como señala el informe de la encuesta, no deberán exagerarse las diferencias entre esos tres modelos ya que, en la mayoría de los casos, con independencia de cualquier exención expresa que pudiera existir, la normativa de protección de datos no se aplica plenamente a los medios de comunicación dado el rango constitucional especial de la normativa sobre libertad de expresión y libertad de prensa. Por otra parte, la normativa ordinaria de protección de datos se aplica,, en general, a las actividades no editoriales realizadas por los medios de comunicación.

En España, como ha señalado Rodríguez Bereijo, la libertad de los medios de comunicación tiene una doble dimensión:

a) La funcional, en tanto libertad de actuación, que comprende no sólo la libre expresión de hechos, ideas u opiniones, sino el derecho a crear medios materiales a través de los cuales se hace posible su comunicación y difusión. Existe, pues, para el citado profesor una conexión lógica entre la libertad de expresión y otros derechos de libertad, también constitucionales, como son la libertad de empresa, el libre ejercicio profesional, etc.

b) La estructural o institucional, que se concreta directamente con el pluralismo político, valor inferior de nuestro ordenamiento jurídico (artículo 1.1 CE) y con la importancia vital en una democracia, de una opinión pública correctamente formulada. Sin el mandamiento de una comunicación pública libre quedarían vaciados de contenido real otros derechos que la Constitución consagra.

Para el autor antes citado, la naturaleza jurídica de la libertad de expresión es que es, ante todo,, un derecho de libertad frente al poder, por lo que básicamente significa ausencia de trabas e impedimentos por parte de la Administración en su proceso de comunicación, y además, significa el reconocimiento y la garantía de una institución política fundamental, que es la opinión pública libre, indisolublemente ligada con el pluralismo político, valor fundamental y requisito de funcionamiento del Estado democrático. Ahora bien, es condición fundamental para reconocer el valor preponderante de las libertades públicas del artículo 20 de la CE. la de que "las libertades se ejerciten en conexión con asuntos que son de interés general por las materias a que se refieren y por las personas que en ellas intervienen y contribuyen, en consecuencia, a la formación de la opinión pública " (STC 107/1988).

Para nuestro Tribunal Constitucional debe distinguirse entre la libertad de expresión y libertad de información. La primera consiste en la formulación de opiniones y relaciones personales, sin pretensión de sentar hechos o afirmar datos objetivos; la segunda, supone suministrar información sobre hechos que pretenden ser ciertos y noticiables (SS TC 105/1983 y 105/1990). Por tanto, libertad de expresión y libertad de información tienen, como derechos, distinto contenido y límites.

Ambas libertades, vistas desde la protección del derecho del honor, ocupan una posición preferente cuando se ejercitan en asuntos de interés público que contribuyan a la formación de la opinión pública. Como establece la STC 19/1996, dicha posición preferente se justifica cuando los destinatarios en la opinión o de la información crítica son personas públicas, decayendo ese valor preferencial de ambas libertades cuando se ejercitan en relación con conductas privadas carentes de interés.

En relación con la intimidad, el criterio fundamental para determinar la legitimidad de las intromisiones de las personas está en la relevancia pública del hecho divulgado, es decir, que siendo verdadera su comunicación a la opinión pública resulta justificada en función del interés público del asunto sobre el que se informa.

Tal doctrina, expuesta sucintamente siguiendo a Rodríguez Bereijo, es a juicio de la Agencia de Protección de Datos, perfectamente conciliable con el artículo 9 de la Directiva 95/46/CE, ya que las limitaciones que en el mismo se prevén, en cuanto sean necesarias para conciliar el derecho o la intimidad con las normas que rigen la libertad de expresión, deberán tener en cuenta la construcción que de la libertad de expresión y de información se ha venido haciendo por el Tribunal Constitucional.

En este campo, el Grupo del artículo 29 de la Directiva establece una serie de conclusiones, que se transcriben a continuación, tendentes a evaluar hasta que punto debe limitarse la aplicación de cada una de las disposiciones de los Capítulos II, IV y VI de la Directiva para proteger a la libertad de expresión ya que a juicio de dicho Grupo ha de

* Las leyes de protección de datos se aplican, en principio, a los medios de comunicación. Las exenciones y excepciones sólo pueden concederse en relación con el Capítulo II, sobre condiciones generales para la licitud del tratamiento de datos personales, el Capítulo IV, sobre transferencia de datos personales a países terceros, y el Capítulo VI, sobre autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales. No pueden concederse exenciones o excepciones a las disposiciones referentes a seguridad. Las autoridades de control **con responsabilidad en la materia** deberán, en todo caso, retener determinados poderes a posteriori.

* Las exenciones y excepciones al amparo del artículo 9 deben respetar el principio de proporcionalidad. Sólo deben concederse exenciones y excepciones en relación con las disposiciones que pudieran hacer peligrar la libertad de expresión y sólo en la medida necesaria para el ejercicio efectivo de dicho derecho conciliándolo con el derecho a la intimidad de datos del interesado.

* Pueden no ser necesarias exenciones y excepciones al amparo del art. 9 en los supuestos en que la flexibilidad de varias disposiciones de la Directiva o exenciones previstas de conformidad con otras disposiciones (que, por supuesto, también deben ser interpretadas restrictivamente) ya permiten alcanzar un equilibrio satisfactorio entre el derecho a la intimidad y el derecho a la libertad de expresión.

* El artículo 9 de la Directiva respeta el derecho de las personas a la libertad de expresión. Las exenciones y excepciones al amparo del artículo 9 no pueden ser concedidas a los medios de comunicación o a los periodistas en cuanto tales, sino únicamente a personas que se ocupen del tratamiento de datos con fines periodísticos.

* Las exenciones y excepciones sólo pueden referirse al tratamiento de datos con fines periodísticos (editoriales) **incluyendo la publicación electrónica**. Cualquier otra forma de tratamiento de datos por parte de periodistas o de los medios de comunicación está sujeta a las normas ordinarias de la Directiva. Esta **distinción** cobra particular importancia en relación con la publicación electrónica. El tratamiento de datos de los subscriptores, con el fin de expedir facturas, o el tratamiento para comercialización directa (incluyendo el tratamiento de datos acerca de la utilización de medios de comunicación con el fin de diseñar perfiles) están comprendidos dentro del régimen ordinario de protección de datos.

* La Directiva exige conciliar dos libertades fundamentales. Con el fin de determinar si las limitaciones a los derechos y obligaciones derivantes de la Directiva guardan proporción con el objetivo de proteger a la libertad de expresión, debería prestarse una atención particular a las garantías específicas de que gozan los particulares en relación con los medios de comunicación. Los límites al derecho de acceso y de rectificación previos a la publicación **podrían ser proporcionados** sólo en la medida en que las personas gozan del derecho de réplica o de obtener la rectificación de la información falsa tras la publicación.

* En todo caso, las personas tienen derecho a disponer de formas adecuadas de reparación en caso de violación de sus derechos .

Al evaluar si guardan proporción las exenciones o excepciones, debe prestarse atención a las obligaciones deontológicas y profesionales de los periodistas, así como a las modalidades de autorregulación proporcionadas por la profesión.

2. EL FENÓMENO INTERNET.

Ya en la memoria del pasado año se hacia alusión a INTERNET y se comentaba los sectores afectados por dicha manifestación tecnológica y en concreto se hacia alusión a los contenidos ilícitos y nocivos que podían cometerse a través de dicha vía. Ello dio origen a una Resolución del Consejo, de 17 de febrero de 1997, sobre contenidos ilícitos y nocivos en INTERNET (D.O. de 6 de marzo de 1997).

En el presente Capítulo de la Memoria no vamos a tratar en profundidad dicho tema, dada las características de globalidad que presenta y que, desde el punto de vista de la Agencia, sí hace necesaria, la dedicación de una apartado monográfico al mismo.

Dentro de la Unión Europea, en materia de Internet, se hace preciso hacer referencia a la Propuesta presentada por la Comisión, de fecha 27 de Noviembre de 1997 que surge como consecuencia del hecho de que Internet se haya convertido en una industria de servicios al público y de la necesidad de adoptar las posibles medidas para luchar contra la utilización ilícita de Internet (consideraciones 1 y 6 de la Propuesta).

La misma va dirigida a que por el Consejo de la Unión Europea (véase Diario Oficial de las Comunidades Europeas 13 de febrero de 1998) se emita una Decisión por la que se adopte un Plan plurianual de acción comunitaria para fomentar la seguridad en la utilización de Internet.

En élla se señala que, por un lado, la Comisión y los Estados miembros deben seguir prestando especial atención a la coordinación de los grupos que trabajan en esta materia (considerando 15) con la finalidad de limitar el flujo de contenidos ilícitos en Internet, para lo que es esencial la cooperación del sector y un mecanismo eficaz de autorregulación (considerando 16) y la necesidad de fomentar la oferta a los usuarios de mecanismos de filtros y alentar la creación de sistemas de calificación como por ejemplo la norma PICS (Plataforma for Internet Content Selection), a la vez que, de forma conjunta se alientan actividades de sensibilización de usuarios en esta materia (considerando 20).

El Plan tiene prevista una duración de cuatro años, desde el 1 de enero de 1998 al 31 de diciembre del 2001 (art. 1) y tiene como objetivo, conforme al art. 2, fomentar la creación de un entorno favorable para el desarrollo de la industria de Internet promoviendo la seguridad en la utilización de Internet. Para cumplir con este objetivo, señala una serie de actuaciones (art. 3) que consisten fundamentalmente en:

- Fomentar la autorregulación industrial y los mecanismos de supervisión de los contenidos (especialmente los destinados a contenidos como la pornografía infantil, el racismo y el antisemitismo).
- Alentar a la industria a ofrecer herramientas de filtrado y mecanismos de calificación que permitan a padres y profesores seleccionar los contenidos apropiados y, al mismo tiempo, los capaciten para decidir a qué contenidos lícitos desean tener acceso.
- Mejorar entre los usuarios el conocimiento de los servicios ofrecidos por la industria, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet.
- Llevar a cabo medidas de apoyo como la evaluación de las repercusiones jurídicas.
- Realizar actividades para fomentar la cooperación internacional en los campos mencionados.
- Efectuar cualquier otra actividad que contribuya a la consecución de los objetivos establecidos en el art. 2.

3. CONSEJO DE EUROPA

* En fecha 13 de febrero de 1997 el Comité de Ministros adoptó la Recomendación R(97) 5, sobre la protección de datos médicos. Ver Anexo.

En la misma se define el dato médico como todo dato de carácter personal referido a la salud de una persona y el dato genético como cualquier dato relacionado con los caracteres hereditarios de un individuo o que, vinculados a dichos caracteres, compongan el patrimonio de un grupo de individuos emparentados.

Su ámbito de aplicación afecta tanto a la recogida como al tratamiento automatizado de datos médicos que siempre deberá efectuarse, como señala su artículo 3, con el necesario respeto de los derechos y libertades fundamentales, especialmente el derecho a la vida privada que deberá garantizarse tanto en la recogida como en el tratamiento.

La referida Recomendación (se halla en el anexo de la Memoria) deberá ser tenida en cuanta como criterio orientativo de cualquier regulación que dentro de nuestro derecho interno se efectúa en materia de datos de salud, en general, o de datos médico en partículas.

* Igualmente, el antiguo proyecto de Recomendación de datos con fines estadísticos fue adoptado como Recomendación (R (97), 18) en la reunión del Comité de Ministros, de 30 de septiembre de 1997.

En su exposición de motivos se justifica la publicación de la misma con apoyo en dos ideas fundamentales: que el Consejo es consciente de las necesidades, tanto en el sector público como en el privado, de estadísticas fiables para el análisis y comprensión de la estructura y la evolución de la sociedad contemporánea y para la definición de políticas y de estrategias; que es igualmente consciente de dicha necesidad de regulación por el desarrollo progresivo de las normas jurídicas nacionales y supranacionales tanto en materia de las actividades estadísticas como en el terreno de la protección de los datos de carácter personal.

Entre otros aspecto fundamentales, se definen las expresiones relativas a los "datos de identificación", "para fines estadísticos" y "resultados estadísticos" y se delimita su campo de aplicación, señalando que comprende a la recogida y tratamiento automatizado de datos personales con fines estadísticos". En otro orden de cosas, se regulan en concreto determinadas materias, como el respeto de la vida privada (artículo 3), las condiciones que deben concurrir en la recogida y tratamiento de datos con fines estadísticos (artículo 4), los derechos de acceso y de rectificación, para los que se admite que pueden ser objeto de limitaciones cuando no existe ningún riesgo de atentado a la vida privada de la persona concernida y los datos se tratan exclusivamente con fines estadísticos (artículo 7.2). Por último, se regula el movimiento de los datos tratados para dicha finalidad.

* Igualmente se halla muy avanzado el proyecto de Recomendación sobre datos de carácter personal recogidos y tratados con fines de seguros.

* Dentro del sector de las nuevas tecnologías, merece destacarse la redacción de un documento, aprobado en la reunión del 14 al 17 de octubre de 1997, sobre la protección de la vida privada en Internet o líneas directrices sobre la protección de las personas con vistas a la recogida y tratamiento de datos de carácter personal en las inforrutas, de modo que puedan ser integrados o anexados en códigos de conducta. Sobre dicho documento se volverá a incidir más adelante al tratar el tema de Internet.

* Dentro de las actividades llevadas a cabo por el Comité Director para la Bioética, merecen destacarse tanto los trabajos efectuados por el Grupo de Trabajo sobre genética humana como los relativos al Grupo de Trabajo sobre la investigación biomédica. Igualmente debe señalarse el Grupo de Trabajo para el transplante de órganos.

* Igualmente en el grupo de nuevas tecnologías se están efectuando estudios sobre lo que viene denominándose tarjetas inteligentes (cartes à puce), es decir aquellas que contienen una circuito integrado que posee una memoria electrónica limitada con la finalidad de almacenar datos. Su apariencia es la de una tarjeta de crédito, si bien pueden ser de dos formas diferentes: la denominada carta pasiva, que está dotada simplemente de una memoria en la que pueden registrarse y leerse los datos mediante un ordenador y la denominada tarjeta inteligente propiamente dicha que tiene un microprocesador y un sistema de explotación que puede llevar a cabo tratamientos informáticos con plena autonomía.

Aún cuando en la actualidad su capacidad de memoria es muy limitada, en un futuro próximo serán capaces de almacenar grandes volúmenes de datos (todas las operaciones financieras, la historia médica u otros aspectos de la vida cotidiana).

A) INTERNET

Anteriormente se comentó que la mundialización de la sociedad de la información, en general, y el fenómeno Internet, en particular, ha creado en todos los organismos internacionales la necesidad de establecer una serie de normas tendentes a obtener una regulación uniforme de sus efectos jurídicos. Ello hace que tales esfuerzos se traten conjuntamente bajo esta rúbrica y no como actividades parciales de cada uno de los organismos internacionales.

Con carácter previo, debe señalarse que en lo referente a Internet se producen dos posturas enfrentadas abiertamente: por un lado, la de aquellos que partiendo de la idea de que Intenet es una red informática sin normas, mantienen, quizá por asociarla a sus ambiciones de libertad, que cualquier tentativa de regulación es una forma inútil de burocracia ya

que "es imposible administrar la red a través de medios jurídicos". Por otro, la de los que entienden que al tratarse de un sistema de comunicación de datos personales ha de someterse a una normativa concreta, que precise el grado y alcance de la misma.

Como ocurre siempre en situaciones parecidas, igualmente coexisten dos hechos enfrentados: la necesidad de efectuar una regulación derivada de la naturaleza de los derechos que pueden resultar afectados y la casi imposibilidad de que en la práctica pueda llevarse a efecto dicha regulación ya que el fenómeno Internet rompe con los viejos esquemas jurídicos (como el principio de la territorialidad de las leyes), produciendo un casi absoluto vacío legal.

Es claro que la regulación jurídica de la red debería efectuarse partiendo de la naturaleza y características de la misma. Es decir, si se trata de un fenómeno de globalización, de mundialización del sistema, con posibilidad de conexiones en todo el universo, con la probabilidad de que el dato personal se traslade a cualquier punto del mundo, se precisaría un sistema jurídico que pudiera atajar los posibles excesos que se cometieran en la aplicación del mismo. Ello solamente podría lograrse a través de convenios internacionales que produjeran una globalización de las normas jurídicas de aplicación a dicho fenómeno.

Como esa solución, la única, siendo posible, es lenta porque lleva tiempo tratar de mover voluntades y buscar coincidencias entre la mayoría de los Estados, los organismos internacionales, en el ámbito de sus competencias, y los Comisarios de protección de datos, en Grupo o en actuaciones individuales, han tomado nota de la existencia del problema y han tratado de buscar las soluciones mínimamente eficaces.

Todas esas actuaciones individuales poseen tres notas de coincidencia, comunes a todas ellas:

a) La necesidad de reforzar, siempre y en todo caso, la coordinación internacional.

b) La necesidad de fomentar los códigos de conducta , es decir las autoregulaciones de los sectores dominantes en la red con el propósito de limitar su supremacía en beneficio de los derechos de los usuarios.

c) La necesidad de comunicar a cada usuario las medidas que pueden adoptar en cada caso con vista a hacer efectiva una mejor defensa de sus derechos individuales.

* La Comisión Europea, partiendo de la idea que son muchos los sectores implicados, no solo la protección de datos personales (nacimiento de un mercado electrónico mundializado, la necesidad de interconexiones internacionales, etc) subraya la importancia que debe darse al desarrollo de un marco jurídico coherente, ya que no es suficiente trasladar los marcos jurídicos existentes para fenómenos "fuera de línea" a los fenómenos "en línea", porque, o no pueden dar respuesta, o no son capaces de darla de manera apropiada a la naturaleza del problema. Por ello, señala la Comisión, la economía mundial en red exige un marco específico apropiado que cubre la totalidad de los aspectos técnicos, comerciales y jurídicos. Tal necesidad puesta de manifiesto no sólo por la celebración de la Conferencia ministerial de Bonn, anteriormente aludida, sino también la organizada por la OCDE, (noviembre de 1997) o en Roma por la Organización Dialogo Comercial Trasatlántico (noviembre de 1997) o la Conferencia ministerial del Consejo de Europa (diciembre de 1997), debe ir dirigida a la determinación de los problemas claves y de los medios con que se cuente para su resolución.
Con la finalidad de despejar tales hechos la Comisión auna, por un lado, una postura plenamente activa en tal sentido, comprometiéndose en la medida de lo posible a llevar a cabo actividades de esta naturaleza y, por otro, a invitar al sector industrial, a lo largo de 1998, a participar en reuniones de expertos que permitan presentar sus posiciones respectivas de forma más coordinada y de facilitar intercambios de información. Además, propugnará una carta internacional tendente a alcanzar un acuerdo multilateral respecto de un método de coordinación dirigido a desmantelar los obstáculos al mercado electrónico mundial, a señalar términos jurídicos, a dar carta de naturaleza a los trabajos que se desarrollan en la actualidad en los instancias internacionales existentes, y , por último, a favorecer la participación del sector privado y de los grupos sociales afectados

* La necesidad de fomentar los códigos de conducta es igualmente sentida por todos los Organismos internacionales. De entre ellos destaca la actividad llevada a cabo por el Consejo de Europa que ha constituido un Grupo de Proyecto, sobre la protección de datos que, en fecha 3 de octubre de 1997 ha elaborado un trabajo titulado "La protección de la vida privada en Internet". Dicho trabajo recibe igualmente la denominación de "Líneas Directrices sobre protección de las personas en relación con la recogida y tratamiento de datos de carácter personal en las inforrutas que pueden ser anexadas o integradas mediante códigos de conducta".

Como se establece en su Exposición de Motivos, el documento enuncia los principios de una conducta leal para los usuarios y los suministradores de servicios y de contenido. Partiendo de la base de que Internet implica unas responsabilidades para cada acción y comporta riesgos para la vida privada, afirma que es importante conducirse de manera que cada uno pueda autoprotegerse y promover a la vez buenas relaciones con los demás.

El citado documento aparece dividido en una serie de consejos dirigidos bien a los usuarios, a los suministradores de servicios y a los suministradores de contenido en Internet. Para los primeros, se establecen, entre otras, las siguientes reglas:

- Recordar que Internet no es seguro. Evitar la utilización del correo electrónico para mensajes confidenciales a menos que se utilice el cifrado (encriptación).
- Utilizar todo medio disponible para asegurar la protección de la vida privada.
- Recordar que cada transacción utilizada, cada sito de Internet visitado deja una "huella". Estas "huellas electrónicas"

pueden ser utilizadas con el fin de aprovecharse de vuestra personalidad e incluso de vuestras inclinaciones íntimas"
- Si la Ley lo autoriza, sería conveniente la utilización de un pseudónimo.
- No entregar más datos personales que los que sean necesarios.
- No entregar al suministrador de servicios más datos personales que los que sean necesarios con fines de facturación.
- Recordar que vuestra dirección de correo electrónico es un dato de carácter personal.
- Evitar que os soliciten muchos datos de carácter personal.
- Exigir información acerca de cuales de vuestros datos personales son conservados por el suministrador de servicios o por un tercero en Internet: modificarlos si son inexactos o hacerlos suprimir si son demasiados o están desfasados.
- No enviar correos malintencionados, ya que pueden volverse contra vosotros, con consecuencias jurídicas adversas.
- Recordar que vuestra dirección de correo electrónico u otros datos de carácter personal que os conciernen pueden ser incluidos en guías o anuarios. No vaciléis en solicitar la finalidad de los mismos y exigir ser excluido si no deseáis figurar en ellos.

Para los suministradores de servicios de Internet se establecen, entre otros, los siguientes.

- Utilizar todos los procedimientos disponibles y las nuevas técnicas que garanticen la vida privada de los usuarios así como la seguridad física y lógica de las redes.
- No leer, ni modificar ni suprimir el contenido de los mensajes enviados a otros usuarios.
- No permitir la lectura o la injerencia en los mensajes o no revelar la identidad oculta a través de pseudónimos más que a las autoridades debidamente habilitadas provistas de autorización específica.
- Fijar reglas para la conservación y la impresión de mensajes e informar a los ciudadanos de las mismas.
- No recoger ni conservar otros datos personales de los usuarios que aquellos que sean necesarios para:

a) Fines de facturación o comprobación.

b) Desarrollar y poner en el mercado sus propios servicios si el usuario ha dado su consentimiento explícito a que sus datos sean utilizados con fines de marketing.

- En ningún caso efectuar comunicación de datos personales salvo si:

a) El usuario ha dado su consentimiento después de haber sido informado de que otro recibirá sus datos y de la finalidad para la que van a ser utilizados.

b) Exista una obligación legal que imponga dicha comunicación.

c) Sea requerido por otro suministrador de servicios de redes u operador para efectuar operaciones o con fines de facturación.

- Cuidar de que los usuarios sean informados de los siguientes puntos antes del abono o del comienzo de la utilización de los servicios:

a) Qué tipo de datos de carácter personal se van a recoger o tratar.

b) Qué utilización se va a efectuar respecto de los datos personales.

c) El período de tiempo en que los datos serán conservados antes de ser suprimidos.

d) Los riesgos que la utilización de Internet puede suponer para la vida privada.

e) El derecho de oposición a la utilización de los datos de carácter personal para la prestación de servicios o su inclusión en anuarios.

- Informar a los usuarios sobre los riesgos conocidos en materia de seguridad en las redes así como los procedimientos para reducir dichos riesgos.
- No conservar datos personales un período más largo de lo estrictamente necesario para cumplir con la finalidad del tratamiento a menos que se halla previsto en la Ley, en virtud de disposición de derecho general, civil o fiscal.

Para los suministradores de contenido el documento establece las siguientes obligaciones:

- No recoger datos personales que no sean absolutamente necesarios.

- Utilizar todos los medios disponibles para proteger la vida privada de todos los visitantes de páginas web.

- Cuando alguien visite vuestra página, se debe informar inmediatamente de:

a) Qué datos de carácter personal han sido recogidos.

b) Qué tipos de datos personales se recogen y tratan

c) Qué Ley permite la recogida y el tratamiento.

d) De qué manera (finalidad) se van a utilizar los datos personales recogidos de esta forma.

e) Durante que tiempo los datos serán conservados antes de ser suprimidos.

- Pedir a los visitantes su autorización para utilizar la dirección para finalidades posteriores de marketing o de correo.
- No comunicar (ceder) los datos de carácter personal a menos que:

a) El usuario que haya dado su consentimiento explícito después de ser informado que otro recibirá sus datos y los fines para los que vayan a ser utilizados.

b) Que se trate de una obligación impuesta por la Ley.

- Si se va a publicar un anuario (una lista de visitantes) respetad el deseo de los usuarios tanto quieran ser incluidos como excluidos.

Además, en el citado trabajo con carácter general se alude al flujo transfronterizo de datos personales en el sentido de establecer una doble consideración:

a) La de utilizar la encriptación (claves) cuando se efectúen envíos por Internet.

b) Antes de enviar datos de carácter personal a otro país, informarse de si el mismo tiene Ley de protección de datos personales o ha ratificado el Convenio 108 del Consejo de Europa.

c) Si el país no ha ratificado el Convenio (o no tiene Ley de protección de datos) la persona que va a recibir los datos personales deberá firmar un contrato tipo en el que establezca las salvaguardas oportunas.

La actuación de la Agencia de Protección de Datos en esta materia va dirigida a establecer un doble tipo de medidas, por un lado, tratar de impulsar el establecimiento de códigos de conducta entre que participan, en cualquier medida, en Internet, de manera que, a través del proceso de autorregulación, puedan establecerse una serie de garantías en beneficio de los titulares de los datos; por otro, efectuando una serie de recomendaciones a los usuarios en la utilización de la red a fin de que adopten las medidas de precaución que estimen necesarias. En este sentido, la Agencia presentó, en Julio del año pasado, una publicación dirigida a cubrir esta última finalidad.

4. COOPERACIÓN INTERNACIONAL: PARTICIPACIÓN EN GRUPOS DE TRABAJO DE ÁMBITO INTERNACIONAL.

4. 1. INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (GRUPO DE BERLÍN).

A lo largo de 1997 el International Working Group on Data Protection in Telecommunications (en adelante IWG) ha continuado sus trabajos que se materializaron en dos reuniones celebradas en el año.

La primera, se celebró en primavera en París y la segunda, en otoño, en Berlín. Ambas reuniones se celebraron junto con las del grupo GERI (Groupe Européen Sur Les Réseaux Internationaux) debido a la coincidencias tanto en los representantes como en las agendas, de hecho es previsible que en posteriores convocatorias el grupo GERI quede absorbido dentro del grupo IWG, ya que en la práctica, el único hecho diferencial era que el IWG tiene un alcance mundial mientras que GERI se circunscribe a la UE.

Los principales temas abordados en ambas reuniones han sido los siguientes:

Se elaboraron unos comentarios al Libro verde sobre la protección de los menores y la dignidad humana en los servicios de información y audiovisuales (COM(96)483 FINAL). En dichos comentarios se recoge la necesidad de un equilibrio entre la protección de la privacidad (se pide expresamente que los usuarios puedan mantener su anonimato en las redes de comunicación) y la necesidad de perseguir los comportamientos ilegales. Se apuesta por que la responsabilidad sobre los contenidos recaiga sobre los creadores de la información y no sobre los usuarios finales. Y se apunta que el hecho de que por estas redes circule información ilegal no debe significar que se vigile todo el tráfico que por ella circula.

Se aboga también por la supresión de la práctica habitual hoy día de que multitud de Web registren los accesos, las lecturas y la información recabada por los usuarios sin avisarles previamente.

Asimismo, en el documento, se hace una mención positiva de la aparición de la Resolución del Consejo de Telecomunicaciones de la Unión Europea del 28 de Noviembre de 1996, que solicita a la Comisión Europea que favorezca la investigación en los campos de filtrado y clasificación de la información y desarrollo de las tecnologías avanzadas de privacidad. Se solicita que las tecnologías avanzadas de privacidad sean incluidas en el 5º Programa Marco para la Investigación y Desarrollo Tecnológico así como que en los grupos de trabajo que en este sentido se creen se incorporen representantes de los Comisionados de Protección de Datos.

Con respecto a las políticas de cifrado se siguen con especial interés un año más, sin que se haya podido constatar todavía cual va a ser la tendencia dominante en los países de nuestro entorno. Parece existir un opinión generalizada,

aunque no materializada todavía, entre los representantes de las Autoridades de Control en el sentido de que se legisle lo menos posible en estos temas y dejar la máxima libertar al ciudadano a la hora de utilizar técnicas de cifrado que garanticen la confidencialidad de sus comunicaciones. Únicamente Francia, dentro de la UE, ha desarrollado legislación al respecto claramente intervencionista y limitativa del uso y empleo del cifrado, sin que, no obstante, todavía no haya definido completamente el modelo que va a seguir. Por último se esta trabajando en la elaboración de una posición común sobre la política de cifrado.

Un aspecto de especial importancia que se sigue en el grupo de trabajo es el de difusión de datos de salud a través de redes de comunicaciones, ya sean privadas o públicas como es el caso de Internet. Existe un sentir generalizado de que este tipo de datos han de enviarse de forma cifrada como forma de garantizar la confidencialidad. El problema que surge, no resuelto todavía, es el de la gestión de las claves.

Otro aspecto de interés es el de la publicación por las diferentes administraciones públicas nacionales de datos públicos en redes de comunicaciones en general y en Internet en particular. En este aspecto si se observa una división entre diversos países. Determinados países nórdicos consideran que el ciudadano tiene derecho de acceso a determinados documentos públicos y en este sentido publican sentencias e incluso información tributaria con datos personales. La mayoría de los países, en cambio, no publican este tipo de información, y sí se hace, se eliminan los datos personales.

Especial seguimiento se está realizando a los sistemas que permiten la selección de contenidos en el acceso a la información a través de Internet, como por ejemplo los estándares PICS (Plataforma para la Selección de Contenidos) y los diferentes vocabularios que en torno a ellos surgen: eTrust, Direct Marketing Association (Asociación de Marketing Directo de USA) y Privacy International. También se sigue con interés los mecanismos que se proponen como garantía de confianza en el etiquetado.

Se ha seguido con especial interés la aparición en diversos países de repertorios públicos de abonados a servicios de telecomunicación en formato CD-ROM. En algunos casos con facilidades discutibles desde el punto de vista de la privacidad como la búsqueda inversa (obtención de los datos personales a partir del número de teléfono.).

Por último, se están siguiendo las diferentes legislaciones que en materia de telecomunicaciones están apareciendo en diversos países europeos y especialmente sus repercusiones en lo que respecta a la privacidad y a la protección de datos.

4. 2. EUROPEAN DATA PROTECTION COMMISSIONERS WORKING PARTY ON POLICE FILES (GRUPO DE TRABAJO SOBRE FICHEROS POLICIALES).

El año 1997 ha conocido una gran actividad de este grupo de trabajo, actividad que ha girado fundamentalmente en la elaboración de un borrador de Reglamento Interno de la futura Autoridad de Control Común (ACC) establecida por el Convenio Europol (en adelante "el Convenio"), habiendo sido España uno de los primeros países en ratificarlo (abril de 1997).

El Convenio establece en su Articulo 24 la creación de una Autoridad de Control Común independiente, cuya misión será revisar, de acuerdo con lo establecido en el Convenio, las actividades de Europol para asegurar que se respetan los derechos de las personas en relación con los datos almacenados y procesados por Europol. La ACC estará formada por dos representantes de cada una de las Autoridades de Control Nacionales en materia de protección de datos.

Dentro del mismo artículo 24 se establece que dentro de la ACC se deberá establecer un Comité de Apelación para examinar los recursos que contra las decisiones de Europol respecto a los derechos de comprobación, rectificación y cancelación puedan interponer los particulares. Este Comité estará formado por un representante de cada Autoridad Nacional.

Asimismo, el artículo 24 establece que la ACC aprobará por unanimidad su Reglamento Interno, que deberá ser sometido al Consejo Europeo para su aprobación. Por ello, en enero de 1997, durante la Presidencia Holandesa de la Unión, el Ministro de Justicia de los Países Bajos, remitió una nota oficial a los Comisionados Europeos en materia de Protección de Datos señalando que, aun no existiendo todavía la ACC puesto que el Convenio no había entrado en vigor pero dado que los procesos de confección de este tipo de Reglamentos suelen ser largos y laboriosos, sería interesante que se fuera redactando un Proyecto de Reglamento para que la puesta en marcha de la ACC fuera lo más inmediata posible tras la entrada en vigor del Convenio.

Por ello, el grupo ha mantenido cinco reuniones a lo largo del año 1997 en los meses de febrero, abril, mayo, septiembre y noviembre, todas ellas en la sede de la Autoridad de Control Holandesa (Registratiekamer) en La Haya, salvo la mantenida el 15 de septiembre, que se celebró en Bruselas.

En la primera de ellas se estableció el procedimiento de trabajo para la redacción del Proyecto de Reglamento. Dado que existía un primer borrador que había sido redactado por la delegación alemana, se consideró que la mejor manera de continuar el trabajo era encargar a un grupo reducido de delegaciones la confección de un borrador del documento. Dicho borrador iría evolucionando a la luz de las posteriores discusiones en el seno del Grupo. Por lo tanto, se encargó a las delegaciones de Alemania, Holanda e Irlanda la elaboración del borrador.

A lo largo de las reuniones mantenidas en 1997, se ha puesto de manifiesto la existencia de dos posturas diferentes

dentro del seno del grupo sobre la relación entre las Autoridades Nacionales y los representantes que ellas eligen para formar parte de la Autoridad de Control Común y en la configuración del Comité de Apelaciones y las cualificaciones de sus miembros.

Estas dos posturas son la defendida fundamentalmente por Alemania y Austria, que consiste en que en la práctica se rompa todo vínculo entre las Autoridades Nacionales y sus representantes una vez nombrados para, de esta manera, reforzar su independencia y en la exigencia y verificación, por parte de la Autoridad de Control Común, de una cierta cualificación legal preestablecida a los miembros del Comité de Apelación.

El motivo fundamental alegado para ello (principalmente por la delegación alemana) es la existencia de requerimientos constitucionales de su país para ello. Además opinan que el Comité de Apelación se debe configurar como un Tribunal de Justicia, ya que es la última instancia de apelación prevista por el Convenio.

Por otro lado, las delegaciones de Francia, Dinamarca, Italia y España, defienden una postura más ajustada a lo que el Convenio Europol establece, defendiendo que la cualificación de los representantes debe ser juzgada, y de hecho lo es, por las Autoridades Nacionales de cada Estado Miembro cuando realizan los nombramientos. Asimismo, se defiende que las Autoridades Nacionales tengan la potestad de cesar libremente a sus representantes ya que estos no actúan a título personal, sino como representantes de las mismas.

Por su parte, los integrantes del Grupo de Redacción, intentan aproximar posturas para llegar a un documento que sea asumible por todas las partes, ya que debe ser aprobado por unanimidad.

4. 3. PROYECTO DE CATÁLOGO DE LEGISLACIÓN DE LAS AGENCIAS INTERNACIONALES EN INTERNET PROMOVIDO POR LA AGENCIA DE PROTECCIÓN DE DATOS.

Siguiendo las pautas marcadas en la Directiva Europea (1) relativa a la protección de datos, según lo indicado en su Considerando 64 (2) y su artículo 28.6 (3), respecto a los aspectos de comunicación y cooperación entre las autoridades de control europeas, la Agencia planteó, a principio del año 1997, la posibilidad de implantación de un sistema basado en el acceso a través de la red Internet, que permitiera el almacenamiento, recuperación y consulta, de toda documentación y publicación relacionada con el tema de la protección de datos a nivel internacional. Se pretendía agrupar, de este modo, toda la información disponible sobre esta materia en un único servidor Web, y dotarla de un mecanismo de búsqueda ágil y versátil para aumentar así su accesibilidad.

4.3.1. Posibles aproximaciones

Teniendo en cuenta tanto el proyecto original como las aportaciones realizadas por otros países, y las soluciones adoptadas por otros organismos ante problemas similares, se plantearon tres posibles alternativas:

1.- Depósito Centralizado.

Se recogerían en una base de datos central, todos los documentos enviados por los países participantes. Los documentos serían uniformizados bajo un mismo formato y publicados en páginas Web. Todos los países podrían participar en el proyecto.

2.- Inventario Centralizado.

En lugar de almacenar los documentos en el punto central, se almacenaría únicamente una ficha por cada documento. Los participantes rellenarían un breve formulario por cada documento que quieran incorporar. Este formulario recogería información como: título, tipo de documento, resumen, términos de búsqueda y dirección. En el campo de dirección se almacenaría la localización exacta en Internet del original del documento.

En el caso de documentos que no estuvieran en Internet, se almacenaría en la base de datos central tanto la ficha como el original del documento. Todos los países podrían participar en el proyecto.

3.- Búsqueda distribuida.

El punto central sólo contendría el motor de búsqueda, las páginas de enlace, y el área de comunicaciones. La búsqueda se realizaría recorriendo cada uno de los servidores Web de los participantes. Sólo podrían participar los países que en la actualidad tuvieran presencia en la red.

4. 3. 2. Solución propuesta

Teniendo en cuenta diversos factores como el impacto económico, la velocidad de respuesta y la participación de las Autoridades de Protección de Datos, la Agencia española apostó por la solución denominada *Inventario Centralizado*, por tres motivos:

Era considerablemente más económica que el depósito centralizado, al contener sólo referencias a los documentos, y aquellos originales que no estuvieran ya en Internet.

Proporcionaba tiempos de respuesta aceptables, al realizar las búsquedas en el punto central, en lugar de recorrer diferentes servidores.

Promovía la participación de todas las Autoridades de Protección de Datos, animando especialmente a aquellas que aún no hubieran utilizado las posibilidades que brinda el medio Internet.

4. 3. 3. Conferencia de Viena

Las posibles aproximaciones al sistema, su coste estimado, y sus ventajas y desventajas fueron expuestas en la conferencia de primavera de las Autoridades de Protección de Datos Europeas, que se celebró en Viena en el mes de Abril de 1997. Bajo el título de " Spanish Proposal on Compiling Legislation and General Information Via Internet" los representantes europeos fueron informados de la propuesta española, que fue acogida en principio con gran interés, aunque no faltaron los comentarios críticos, dirigidos sobre todo a los aspectos centralizadores del sistema, y a la financiación de los costes de implantación.

4. 3. 4. Cuestionario y presupuesto

Tras la Conferencia se elaboró un presupuesto aproximado de los costes de implantación y mantenimiento del sistema, que fue enviado a las Autoridades de Protección de Datos europeas junto con un cuestionario para conocer el grado de interés en participar en el proyecto, y el nivel de presencia de cada uno de los países en la red Internet.

De los cuestionarios recibidos se concluyó que al menos la mitad de los países que respondieron a la consulta estaban interesados en el desarrollo de este sistema, y que al menos cuatro de los países europeos no contaban todavía con servidores Web de información sobre su organismo o sobre legislación de protección de datos. Cabe destacar el gran interés mostrado por las Autoridades de Protección de Datos de Berlín, y su disposición a colaborar en el proyecto.

4. 3. 5. Otros desarrollos similares

Dada la alta probabilidad de que ya se hubieran intentado iniciativas parecidas al sistema planteado, se trató de localizar los proyectos similares a través de búsquedas en Internet, y a través de contactos con colegas europeos. Existía la posibilidad de participar en alguno de los sistemas ya en funcionamiento siempre que se cumplieran unas condiciones mínimas en cuanto al contenido, la finalidad y el patrocinio de los mismos. Se encontraron varios sistemas de recogida de legislación sobre protección de datos, pero ninguno de ellos encajaba completamente con la idea original, bien porque sólo recogían parte de la información que se requería, bien por estar orientados al sector privado, o bien por tratarse de sistemas cerrados, sin posibilidad de incorporación de nueva información.

Los dos sistemas encontrados con más coincidencias con el planteado por la Agencia se describen a continuación:

- Privacy Exchange

Proyecto del Center for Social and Legal Reseach (EE.UU), todavía en fase de desarrollo a final de 1997. Recogería legislación sobre protección de datos a nivel internacional, regulación, órdenes administrativas y publicaciones gubernamentales, así como códigos de conducta de asociaciones profesionales, y publicaciones relacionadas con la privacidad en Internet.

Orientado específicamente a las necesidades del comercio y la industria, y patrocinado por grandes empresas con interés en el tratamiento automatizado de datos. Sustituyen la opción del motor de búsqueda por un servicio de consultas a través de correo electrónico.

- DAPRO- Data Protection on the European Union

Proyecto incluido en el Programa de Aplicaciones Telemáticas de la Comisión europea (DG XIII C), promovido por el Instituto de Informática Jurídica de la universidad de Hannover, y dirigido tanto a la Administración pública como a la empresa privada. En fase de desarrollo a finales de 1997.

El sistema está orientado a realizar un estudio comparativo de la Directiva Europea con las legislaciones de los estados miembros. En un primera fase contendrá la legislación sobre protección de datos de Alemania, Suecia y Gran Bretaña, así como textos relevantes de la Unión Europea. En una segunda fase se realizará un análisis e integración de la directiva europea y se incluirá un sistema hipertexto de información. Y en una tercera, y última fase, se recibirán comentarios y documentación sobre las actividades para la transposición de los distintos países.

Al estar íntimamente ligado a informar en el periodo de transposición de la Directiva, se desconoce si permanecerá una vez completada su función inicial. La incorporación de información de otros países además de los ya incluidos, quedaba supeditada a la acogida que tuviera el sistema una vez funcionara con los primeros participantes.

4. 3. 6. Una línea de acción común.

Las autoridades de protección de datos de Berlín, y las autoridades españolas, decidieron seguir una línea de acción común en el desarrollo de un sitio Web de contenido documental relacionado con la temática de la protección de datos.

De común acuerdo se decidió comenzar con el desarrollo de un sistema acorde con la solución de inventario centralizado, tal y como se expuso en la reunión celebrada en Viena en Abril de 1997. Se trataría de desarrollar un sistema abierto y flexible con la posibilidad de incorporar tanto nueva información como de admitir nuevos colaboradores

5. SISTEMA DE INFORMACIÓN SCHENGEN

España firmó el Acuerdo de adhesión al Convenio de aplicación del Acuerdo de Schengen en fecha de 25 de junio de 1991 y con la aprobación de la Ley Orgánica 5/1992 y la creación de la Agencia, se cumplieron las condiciones requeridas en el artículo 117 del Convenio para participar en el Sistema de Información de Schengen (SIS).

El principal objeto del SIS es, con la ayuda de la información transmitida en dicho 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; éste se ha visto ampliado con la incorporación de Austria, Grecia e Italia, al aplicar estos países el Convenio desde finales de 1997.

El SIS consta de una parte nacional en cada uno de los países que aplican el Convenio y de una unidad de apoyo técnico central ubicada en Estrasburgo. Este Sistema permite a las autoridades habilitadas de cada país, mediante un procedimiento de consulta automatizada, disponer de descripciones de personas y de objetos. 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 se establecen los principios y mecanismos destinados a garantizar una adecuada protección de los datos de carácter personal residentes 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 SIS no atentan contra los derechos de la persona que se trate. Asimismo, se indica que toda persona tendrá derecho a solicitar a esta autoridad de control 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 428/1996, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, encomienda a ésta el ejercicio del control aquí mencionado.

Por otra parte, en el artículo 115 del Convenio se establece la creación de una Autoridad de Control Común 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 en el artículo 10 del Real Decreto mencionado, se establece que el Director de la Agencia designará a los dos representantes que formarán parte de la Autoridad de Control Común.

5. 1. EL SISTEMA DE INFORMACIÓN SCHENGEN EN ESPAÑA

Como en años anteriores, no se ha recibido en esta Agencia ninguna reclamación o tutela de derechos relacionadas con el SIS. Ello está en concordancia con el número de reclamaciones que se han recibido en el sector de los ficheros de las Fuerzas y Cuerpos de Seguridad.

Durante el año de 1997, se ha consolidado la participación de la Policía Autónoma Vasca en el SIS, con la ubicación en sus instalaciones de un equipo informático que mantiene una copia de la información del SIS español, equivalente a la que mantienen en sus centros informáticos el Cuerpo Nacional de Policía y la Guardia Civil.

Indicar que durante este año la Inspección de Datos no ha realizado ninguna revisión especial sobre el SIS, pero sí que se han planificado las futuras inspecciones a realizar en el próximo año 1998 y en las que se revisarán las instalaciones donde se encuentran ubicados los subsistemas que componen el SIS español.

5. 2. IMPLICACIONES DE LAS DECISIONES DE LA AUTORIDAD DE CONTROL COMÚN

De los trabajos desempeñados por la Autoridad de Control Común (ACC), y de los cuales puede encontrarse información más detallada en el Informe de Actividades de marzo de 1997 - marzo de 1998 elaborado por dicha Autoridad y que se presenta como Anexo en esta Memoria, cabe destacar los siguientes en cuanto a que afectan directamente a la Agencia:

- Elaboración de folletos sobre el derecho de acceso al SIS:
Con el fin de dar a conocer la existencia del SIS y la posibilidad que tienen los ciudadanos de ejercicio de los derechos que el Convenio les reconoce, la ACC decidió publicar un folleto explicativo dirigido al público en general y que fuera distribuido en los puntos de cruce autorizados de las fronteras exteriores de Schengen. Para ello, la ACC ha solicitado la colaboración de las autoridades nacionales de control, de las instancias Schengen y de las autoridades competentes de los Estados. Por ello, dado que esta Agencia entiende que es primordial informar a las personas de los derechos

que el Convenio les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal, es por lo que tratará de colaborar en la realización de esta campaña de información relativa al SIS, teniendo en cuenta que la dotación presupuestaria con la que se cuenta para la realización de campañas de difusión es muy limitada.

- Seguridad de las oficinas SIRENE:
A raíz de una importante fuga de información confidencial proveniente del SIS, en concreto de la Oficina SIRENE belga, la ACC ha solicitado a las autoridades nacionales de control que informen a la ACC del estado de la seguridad de las instalaciones donde se encuentren los SIS nacionales y las Oficinas SIRENE. Por tanto, y coincidiendo con las inspecciones de oficio que había previsto realizar la Inspección de Datos para comprobar el estado de la seguridad de los diferentes sistemas que componen el SIS, la revisión de este sistema será una tarea prioritaria para el año 1998.

- Elaboración de dictámenes:
Varios han sido los dictámenes emitidos por la ACC en relación con cuestiones planteadas por sus propios representantes o por otras instancias y cuyo texto íntegro se encuentra en el anexo citado anteriormente. Dado que el artículo 115 del Convenio determina que la ACC tendrá competencia para analizar las dificultades de aplicación o interpretación que pudieran surgir con motivo de la explotación del SIS, para estudiar los problemas que pudieran plantearse en el ejercicio del control independiente efectuado por las autoridades de control nacionales de los países en los que se aplica el Convenio o en el ejercicio del derecho de acceso al sistema, así como para elaborar propuestas armonizadas con vistas a hallar soluciones comunes a los problemas existentes, esta Agencia tendrá en cuenta los dictámenes emitidos por la ACC como criterio interpretativo y de aplicación del Convenio de Schengen.

- Presupuesto autónomo para la ACC:
Las Autoridades Schengen han aprobado una línea presupuestaria propia para la ACC, pero ésta es tan reducida (2.839.950 francos belgas para el año 1997) que la participación española en esta autoridad sigue siendo gravosa para esta Agencia, teniendo en cuenta que sus representantes deben desplazarse a Bruselas o Estrasburgo, lugares donde habitualmente se celebran las reuniones de la ACC.

---

1 Directiva 95/46/CE del parlamento europeo y del consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
2 Considerando 64: "Las autoridades de los distintos estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones, de forma que se garantice el pleno respeto de las normas de protección en toda la Unión Europea. "
3 Art. 28.6: "Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil".

6. OTRAS ACTIVIDADES

* En este apartado merece sin duda destacar la Decisión del Parlamento Europeo, de 10 de julio de 1997 (Diario Oficial de las Comunidades Europeas de 25 de septiembre), relativa al acceso del público a los documentos del Parlamento Europeo. En la misma, se regula el acceso a los mismos, la forma en que ha de procederse para lograr tal fin y la negativa a efectuar dicho acceso (art. 5) cuando la publicación del documento pudiera perjudicar:

- la protección del interés público, en particular en materia de seguridad pública, intereses económicos de la Comunidad Europea, procedimientos jurisprudenciales y actividades de investigación de la institución.
- la protección del secreto comercial e industrial
- la protección del individuo y de la vida privada.
- la protección del carácter confidencial solicitado por la persona física o moral que haya facilitado alguna información contenida en el documento o exigido por la legislación del Estado miembro que haya aportado parte de dicha información.

* Igualmente ha de señalarse que se ha aprobado 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 (Diario Oficial de 30 de enero de 1998). En la Memoria del año pasado ya se hacía una amplia referencia al contenido de la misma, por lo que no se va a reproducir dicho contenido en la presente. Ahora bien, a juicio de la Agencia se hace preciso efectuar dos breves consideraciones: por un lado, que el plazo de transposición al derecho interno de cada Estado miembro se hace coincidir con el señalado por la Directiva 95/46/CE; por otro, que es interesante destacar que el art. 15. 2 de la misma se otorga validez al denominado consentimiento tácito respecto a los tratamientos que se hallen en curso el día de la entrada en vigor de la citada Directiva, al disponer que "No obstante lo dispuesto en el apartado 3 del art. 6, no será necesario el consentimiento respecto al tratamiento en curso el día de entrada en vigor de las disposiciones nacionales adoptadas con arreglo a la presente Directiva. **En tales casos se informará a los abonados sobre este tratamiento y**, si no expresan su reprobación en un período que determinará el Estado miembro, **se considerará que han dado su consentimiento**.

* La Comisión Europea y la República Federal de Alemania organizaron conjuntamente la Conferencia Ministerial Europea titulada "Las redes mundiales de información: aprovechar su potencial", celebrada en Bonn (Alemania) del 6 al 8 de julio de 1997. El objetivo de la misma fue el de mejorar el conocimiento general del uso de las redes mundiales de información, señalar los obstáculos a su utilización, debatir las posibles soluciones y entablar un diálogo abierto sobre las posibilidades de ampliar la cooperación europea e internacional en dicha materia.

Del contenido global de la Declaración que se elabora a su finalización merece la pena destacar, por un lado, la referencia que se efectúa a la seguridad y a la confidencialidad (preceptos 35 y 36 de la misma) en donde se establece que la seguridad de la información es una de las cuestiones fundamentales para la aparición de la sociedad mundial de la información y se reconoce que es de suma importancia poder disponer de una potente tecnología de codificación para el comercio electrónico y que se esforzarán por conseguir la disponibilidad internacional y la libre elección de productos de criptografía y servicios interoperables con el fin de contribuir de manera eficaz a la protección de los datos y a la confidencialidad de la información; por otro, se alude, para desarrollarla, a la protección de los datos (puntos 49 a 52) refiriéndose en concreto a :

- que los datos personales de los usuarios de las redes mundiales de información sólo deberán recogerse y tratarse en caso de que el usuario haya dado su consentimiento consciente o de que su recogida o tratamiento estén autorizados por ley y se ofrezcan las garantías jurídicas adecuadas y las herramientas técnicas para proteger el derecho del usuario a la intimidad.
- que los Ministros acuerdan realizar un esfuerzo común en favor del establecimiento de principios mundiales sobre libre circulación de la información, protegiendo al mismo tiempo el derecho fundamental a la intimidad y los datos personales y **empresariales**, basándose en el trabajo emprendido por la Unión Europea, el Consejo de Europa, la OCDE y las Naciones Unidas.
- se reconoce el principio de que en las situaciones en las que el usuario pueda decidir mantenerse en el anonimato fuera de línea también pueda hacerlo en línea.
- se insta a la industria a aplicar medios técnicos para garantizar la intimidad y proteger los datos personales en las redes mundiales de información, como la navegación, los medios de pago y el correo electrónico anónimos.

MEMORIA DE 1997 - ANÁLISIS Y VALORACIÓN DE LOS DIVERSOS PROBLEMAS DE LA PROTECCIÓN DE DATOS EN ESPAÑA

1. INTRODUCCIÓN

La aplicación de la Ley Orgánica 5/1992, de 29 de octubre, en el año 1997, puso de manifiesto una serie de problemas jurídicos, algunos ya tratados en Memorias anteriores, tal como el de los ficheros de solvencia patrimonial, el de la inexistencia de un reglamento sobre las medidas de seguridad a las que deben sujetarse los ficheros de datos personales, o el del tratamiento de los datos de salud. A ellos no se va a referir la presente Memoria ya que no presentan peculiaridades específicas distintas a las de otros años.

Pero también en 1997 se pusieron de manifiesto nuevos problemas de aplicación de la Ley Orgánica. Fundamentalmente debe hacerse referencia a dos de ellos: las guías telefónicas como instrumentos suministradores de datos personales y la recogida de datos personales a través de las denominadas macroencuestas.

2. GUÍAS TELEFÓNICAS

Las guías telefónicas aparecen reguladas en el artículo 26 de la Ley Orgánica en cuanto que dispone que "los números de teléfono y demás servicios de telecomunicaciones, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso público, pero el abonado podrá pedir su exclusión".

Dicho precepto debe ser puesto en relación, en cuanto a la referencia que efectúa al calificar a los repertorios de abonados como de acceso público, o lo que en dicha materia dispone el artículo 2.2 de la propia Ley Orgánica, que excluye del ámbito de aplicación de la misma a las denominadas fuentes accesibles al público.

Tal conclusión, basada en principio en una correcta interpretación de los diversos preceptos de la Ley orgánica que regulan las fuentes accesibles al público, supone, en principio, la utilización por parte de terceros de los datos contenidos en los repertorios telefónicos, sin necesidad del consentimiento del titular del dato.

Es cierto que este puede pedir la exclusión de sus datos personales de dicho repertorio, pero tal actuación, incluso de llevarse a cabo con éxito, determina una serie de inconvenientes para el solicitante. En concreto, deben de tratarse dos aspectos: por un lado, si la petición de exclusión muta la naturaleza jurídica del dato personal, pasando de ser un dato obtenido de fuente accesible al público a dato que goza de la protección normal de la Ley Orgánica. De ser así, debería determinarse el procedimiento a seguir para lograr dicha finalidad y la vinculación que dicha petición podría tener para terceras personas, es decir, si desde el momento de tal petición el tercero que utiliza los datos debe abstenerse de cualquier tratamiento; igualmente debería determinarse el alcance de la responsabilidad por incumplimiento. Por otro, la determinación del mecanismo adecuado que haga efectiva dicha exclusión. En esta materia debe partirse del hecho real de la existencia de una guía-papel y de una guía-electrónica; en la primera, es prácticamente imposible la exclusión automática de la guía a solicitud del interesado, dada su configuración como un todo inalterable que se proyecta, casi perpetúa, en un período de tiempo determinado (no inferior a dos años), sin que, por otra parte, la exclusión en la última guía suponga que el tercero que lleva a cabo el tratamiento tenga la obligación de utilizar la última versión de la misma, y no siga utilizando ediciones anteriores, lo que determinaría la ineficacia de toda maniobra tendente a lograr la exclusión.

Tal dificultad no se produciría en la denominada guía-electrónica en cuanto que las altas y bajas en los mismas son automáticas y se ejecutan al momento. Ahora bien, la utilización de las mismas no deja de plantear problemas en otro orden de cuestiones. Así, la posibilidad de efectuar lo que se viene denominando búsqueda inversa, es decir, la averiguación de quien es el titular del teléfono partiendo simplemente del mismo o la posibilidad de búsquedas masivas que, combinadas con técnicas de fragmentación, permitan seleccionar determinados usuarios, que responden a ciertos rasgos que les hagan susceptibles de ser destinatarios de determinadas propagandas.

En resumen, la cuestión de las guías telefónicas se relaciona con el concepto de fuentes accesibles al público y deberá ser revisada en nuestra legislación no sólo con la finalidad de dar a aquéllas el contenido y regulación propia de la Directiva 97/66/CE, sino también para tratar de eliminar su conexión con las denominadas fuentes accesibles al público, siempre que en tal expresión no se respete el principio de la finalidad que determinó precisamente el que se efectuara dicha publicación.

Tal regulación debería igualmente tener en cuenta al derecho de oposición del titular del dato en los términos definidos en la Directiva 95/46/CE pero, a su vez, debería tener un apoyo decidido en nuestro ordenamiento jurídico de manera que se permitiera una inclusión parcial en la guía que permitiera eliminar los peligros de utilización posterior, sin renunciar a las ventajas que pueda suponer la inclusión en la misma. En este sentido, debe recordarse que la Comisión francesa ha publicado un Acuerdo, de fecha 8 de julio de 1997, en donde trata de hacer frente a dicho problema y que la Ley Francesa, de 26 de julio de 1996, ha incorporado al Derecho francés dos nuevas garantías: la posibilidad de solicitar la inscripción incompleta de su nombre o la de la dirección en una guía telefónica.

3. ENCUESTAS DE OPINIÓN

También en 1997, se ha puesto de manifiesto la tendencia a someter a un gran número de ciudadanos a la contestación de encuestas que, por el volumen de sus datos o por la petición de autorización para efectuar cesiones a terceras personas, permite averiguar que van a ser posteriormente objeto de comercialización con la finalidad de convertirse en instrumento necesario para llevar a cabo determinadas campañas de publicidad.

La regulación que la Ley Orgánica ofrece en esta materia es igualmente escasa. Así, el artículo 30 se refiere a los ficheros relativos a encuestas o investigaciones y dispone que:

1. "Sólo se utilizarán de forma automatizada datos de carácter personal en ... trabajos de protección de mercados ... si el afectado hubiera prestado su consentimiento a tal efecto.
2. Los datos de carácter personal tratados automatizadamente con ocasión de tales actividades no podrán ser utilizados con finalidad distinta ni cedidos de forma que puedan ser puestos en relación con una persona concreta".

Por otra parte, el artículo 29, al regular los denominados ficheros de publicidad, permite dar información del dato que se haya obtenido "de documentos accesibles al público o se hayan facilitado por los propios afectados u obtenidos con su consentimiento". Igualmente el número 2 del citado precepto establece que "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".

Si la aplicación de ambos preceptos, de manera independiente, no deja de originar problemas en la práctica, la aplicación combinada de dichas normas lógicamente produce un aumento de los inconvenientes. Así, si puede mantenerse que la realización de una macroencuesta con fines comerciales supone la aplicación sucesiva del artículo 30 y del artículo 29 de la Ley Orgánica, los problemas de interpretación de las citadas normas serán, cuando menos, complejos en cuanto al tema de las cesiones de forma que los datos no puedan ponerse en relación con una persona concreta (artículo 30.2) o la manera en que pueda hacerse efectiva la revocación del consentimiento para el tratamiento de los datos con fines de publicidad (artículo 29.2).

En esta materia debería dotarse a la Agencia de facultades de intervención previas de modo que la misma pudiera participar, vía la correspondiente autorización, en la determinación de los datos a obtener (no sólo en cuanto al número sino también respecto de la naturaleza de los mismos) y en la especificación de la forma en que debieran instrumentarse las garantías mínimas que la Ley Orgánica establece en cuanto a la información en la recogida, la determinación del cesionario y la posibilidad de hacer efectiva la revocación de la autorización del tratamiento.

4. DATOS DE AFILIACIÓN SINDICAL

Se hace preciso aludir, aún cuando tenga fecha de 13 de enero de 1998, a la Sentencia del Tribunal Constitucional número 11/1998, que, resolviendo la utilización de unos datos de afiliación sindical, efectúa una moderna interpretación del artículo 18.4 de la Constitución Española.

La referida sentencia parte del reconocimiento de la doctrina en su día sentada por la sentencia 254/1993, para señalar que en la relación del artículo 18.4 con el 28.1, ambos de la Constitución Española, el primero de ellos, en cuanto establece limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, es "un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego la libertar sindical", por 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 la persona ..., 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 ...".

A. La citada resolución abre una nueva vía de interpretación del contenido del artículo 18.4 de la Constitución Española, no en cuanto a su valor en sí mismo,, sino en lo que supone de derecho instrumental para el respeto de otros derechos fundamentales.

MEMORIA DE 1997 - OTRAS ACTIVIDADES

1. PROYECTO DE REAL DECRETO POR EL QUE SE APRUEBA EL REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

La Ley Orgánica 5/1992 prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativa 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 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.

Ante la situación expuesta, en la primavera de 1996, la Agencia comenzó a trabajar en un borrador de Reglamento de Medidas de Seguridad con objeto de desarrollar lo dispuesto en los artículos 9 y 43.3 h) de la Ley Orgánica 5/1992. Este borrador fue remitido al Ministerio de Justicia, por si deseaba tenerlo en consideración para la elaboración del susodicho Reglamento y de modo que se manifestara abiertamente el interés de la Agencia por su publicación.

Como paso previo a la elaboración del borrador en sí, se realizó un estudio que puso de manifiesto la necesidad de realización del reglamento de medidas de seguridad y, a la vez, presentó consideraciones sobre el alcance del mismo.

Concluido el estudio, se preparó un plan de actuación para la redacción del borrador de reglamento de medidas de seguridad que debía ser remitido al Ministerio de Justicia, analizando diferentes posibilidades para abordar el proyecto.

El resultado fue un documento remitido al Ministerio de Justicia que lo acogió favorablemente y que ha servido de punto de partida para el desarrollo del proyecto del reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

1.1. PLAN DE ACTUACIÓN

En primer lugar, se delimitó el modo de abordar la elaboración del borrador, analizándose las ventajas e inconvenientes ofrecidas por las tres alternativas que fueron evaluadas: realizar un único reglamento general de aplicación para todos los ficheros, elaborar una serie de desarrollos sectoriales considerando sus características propias, o bien desarrollar el borrador estableciendo las medidas de seguridad en función de la configuración del sistema de información.

La primera de las opciones descartada fue el modelo de un reglamento de seguridad adecuado a las diferentes configuraciones de los sistemas de información existentes. El grado de definición que podría haber alcanzado el reglamento hubiera sido mucho mayor que el ofrecido por el borrador redactado, ya que hubiera permitido concretar en detalle las medidas para cada uno de los diferentes entornos considerados. No obstante, presentaba dos graves inconvenientes que la hacían prácticamente inviable.

En primer lugar, la constante evolución de las tecnologías de la información, y por ende en materia de seguridad de los sistemas de información, podrían dejar el reglamento obsoleto en un corto periodo de tiempo o incluso antes de su publicación. Por otra parte, el gran número de configuraciones de sistemas de información existentes planteaba problemas para su clasificación y selección.

El modelo de un reglamento que tratara separadamente sectores diferentes de actividad económica fue descartado en términos análogos. Las particularidades de cada sector podrían haberse reflejado en el reglamento, adecuando medidas más específicas a los procedimientos aplicados en los mismos. No obstante, la dificultad en establecer qué sectores merecerían un tratamiento diferenciado y cuáles no, fue el motivo fundamental para desestimar esta alternativa.

En ambos casos, se consideró también la posibilidad de que el reglamento elaborado fuera completado mediante la autorregulación propia, paradigma estimado por la Agencia como mecanismo óptimo para garantizar el cumplimiento de la normativa vigente.

Así pues, el modelo del borrador de un reglamento único general de medidas de seguridad exigibles a todos los ficheros se convirtió en la alternativa más viable. Esta alternativa condicionó que el objetivo a alcanzar consistiera en la definición de un marco global de actuación donde posteriormente se puntualizarían aquellos aspectos susceptibles de interpretación. Estas puntualizaciones podrían materializarse principalmente en dos formas diferentes: Instrucciones del Director de la Agencia disipando dudas interpretativas y, volviendo sobre la autorregulación, el desarrollo de códigos tipos que permitieran profundizar en el contenido del reglamento, en base a las características de los diferentes sectores de actividad o configuraciones de los sistemas de información.

El plan diseñado para alcanzar el objetivo propuesto se llevó a cabo en las siguientes etapas:

* Confeccionar una relación exhaustiva de temas, concernientes a los tratamientos automatizados de datos personales, que exigen garantías de seguridad.

* Elaborar una relación de medidas de seguridad susceptibles de ser aplicadas para garantizar la confidencialidad e integridad de cada uno de los diferentes temas obtenidos como resultado del trabajo realizado en la etapa anterior.

* Clasificar los datos de carácter personal en diferentes tipologías.

* Realizar, en base a los resultados obtenidos en la etapa anterior, una clasificación definitiva, de tal forma que se agruparan en una misma categoría todas aquellas tipologías cuyos requisitos de seguridad sean idénticos para cada tema.

* Seleccionar las medidas de seguridad concretas que debe cumplir cada una de las categorías definitivas.

* Redactar el borrador de reglamento.

Se creó un primer grupo de trabajo encargado de elaborar un índice de temas en materia de confidencialidad e integridad que debían ser considerados para garantizar la seguridad de los datos de carácter personal, incluyendo aspectos como: el acceso no autorizado a los datos, las consultas masivas de datos, la exactitud de la información, el peligro de cruces potenciales de información para enriquecer el fichero, etc. Una vez elaborado el índice se iniciaron dos líneas de trabajo simultáneas.

La primera línea de trabajo consistió en confeccionar una relación exhaustiva de las medidas de seguridad aplicables, incluyendo tanto medidas de carácter organizativo como de carácter técnico. En la relación aparecían medidas como: control de acceso, distribución de soportes, registros de auditoría, etc.

Para confeccionar esta relación se utilizó documentación de origen y contenido muy diverso, como los "Criterios de Evaluación de la Seguridad de la Tecnología de la Información. (ITSEC)" (Commission of the European Communities. 1991); "A Code of Practice for Information Security Management" (Department of Trade and Industry, U. K. 1993); o el Anteproyecto de Real Decreto de Medidas de Seguridad (Ministerio de Justicia. 1993) que no llegó a publicarse.

La segunda línea de trabajo se centró en la clasificación de los diversos tipos de ficheros atendiendo al estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos, criterios establecidos en la Ley Orgánica 5/1992. Para establecer las tipologías se consideraron aspectos como: ideología, religión y creencias; origen racial, salud y vida sexual; investigaciones policiales; infracciones penales y administrativas; solvencia patrimonial; ficheros de publicidad; etc.

Por cada una de las tipologías de ficheros recogida en la clasificación, se asignó el nivel de seguridad exigible para cada uno de los temas contenidos en el índice de materias de seguridad. Este nivel de seguridad podía ser de tres tipos: básico, medio y alto, siguiendo el planteamiento propuesto en "General Recommendations on Data Security" (Swedish Data Inspectorate) o "Dutch Data Security Standards" (Draft) (The Dutch Data Protection Authority. 1996)

Una vez completada la asignación de los niveles de seguridad en el modo descrito, se comprobó que la totalidad de las tipologías de ficheros examinadas podrían ser reagrupadas en cuatro grandes categorías.

La primera categoría estaría formada por todos los ficheros automatizados que traten datos de carácter personal. El nivel de seguridad exigido sería el básico.

La segunda categoría estaría compuesta por los ficheros que traten datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por lo dispuesto en el artículo 28 de la Ley Orgánica 5/1992. El nivel de seguridad exigido sería el medio.

La tercera categoría comprendería aquellos ficheros que traten datos suficientes de tal modo que permitan obtener una evaluación de la personalidad del afectado. El nivel de seguridad exigido se encontraría entre el básico y el medio.

Finalmente, la cuarta categoría la constituirían los ficheros que trataran datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin contar con el consentimiento de los afectados. El nivel de seguridad exigido sería el alto.

Como último paso previo a la redacción del borrador de reglamento, se seleccionaron las medidas seguridad que debían de cumplirse para garantizar la seguridad en los niveles, alto, medio y básico; así como las medidas que serían de aplicación a la tercera categoría de datos mencionados: todas las de nivel básico más algunas de nivel medio. En la selección de las medidas se tuvo presente el estado de la tecnología, criterio establecido en la Ley Orgánica 5/1992, y el coste de la aplicación de las medidas de seguridad, criterio establecido en la Directiva Europea de Protección de Datos. Asimismo, las medidas de seguridad que se establecen para cada uno de los niveles se configuran como mínimos exigibles, sin perjuicio de otras disposiciones legales vigentes.

En el caso de que un fichero pudiera contener tipos de datos que encajaran en diferentes categorías, cada tipo de datos deberá cumplir los requerimientos de seguridad correspondiente según lo dispuesto en el reglamento.

1.2. TRAMITACIÓN DEL REGLAMENTO

A finales de 1996 la Agencia había terminado el borrador de reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

El citado borrador fue remitido al Ministerio de Justicia para facilitar un punto de partida para su tramitación y poner de manifiesto la preocupación que para la Agencia suponía la inexistencia de desarrollo reglamentario en cuanto impedía la aplicación de determinados principios de la Ley Orgánica.

La acogida del borrador de reglamento por parte del Ministerio de Justicia fue favorable y a partir de enero de 1997, la Agencia colaboró activamente con el Ministerio en la redacción definitiva del borrador del reglamento.

En marzo de 1997, se mantuvo una reunión con expertos en la materia, procedentes de diversos sectores: universidad, auditoría informática, Administración Pública, agrupaciones de empresas del sector de tecnologías de la información, etc., para obtener una mayor diversidad de puntos de vista sobre el reglamento. Como resultado de la reunión se obtuvieron conclusiones que enriquecieron el texto.

Durante la tramitación del expediente, la Agencia ha continuado colaborando con el Ministerio de Justicia durante la evolución del reglamento en sus diversas fases.

1.3. ESTRUCTURA DEL REGLAMENTO

El Proyecto de Real Decreto del reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, ha mantenido durante su proceso de tramitación las características contenidas en el borrador inicial propuesto por la Agencia, sin haber sufrido variaciones significativas. El borrador del reglamento se articulaba en seis capítulos y una disposición transitoria.

El Capítulo I "Disposiciones Generales" establece el ámbito de aplicación, define los conceptos básicos utilizados en el reglamento y presenta una clasificación de los datos de carácter personal, asignando un nivel de seguridad a cada una de las categorías. Además, en éste se incluyen aspectos relativos al acceso a datos a través de redes de telecomunicaciones, el régimen de trabajo domiciliario y los ficheros de uso temporal.

El ámbito de aplicación se circunscribe a la definición de las medidas 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, para garantizar la seguridad de tales datos, con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales.

El borrador establece tres niveles de seguridad: básico, medio y alto. Aunque, a lo largo del proceso de definición de las medidas de seguridad para cada uno de estos niveles se tuvieron presentes el estado de la tecnología, criterio mencionado en el artículo 9.1. de la Ley Orgánica 5/1992, y el coste de la aplicación de las medidas de seguridad, criterio mencionado en el artículo 17 de la Directiva de la Unión Europea, el principio que rigió, desde su inicio, fue el del "mínimo privilegio" (traducción de la expresión inglesa "Need-to-know"). Este concepto restringe el acceso de los usuarios únicamente a los datos necesarios que precisen inexcusablemente para el desempeño de sus funciones.

Los Capítulos II, III y IV disponen cuáles son las medidas de seguridad determinadas en cada nivel. No obstante, estas medidas de seguridad establecidas para cada uno de los niveles se configuran como mínimos exigibles, sin perjuicio de otras disposiciones legales vigentes -como el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado- o de la política interna de la propia organización.

El capítulo II determina cuáles son las medidas de seguridad definidas para el nivel de seguridad básico. La premisa de partida ha sido la necesaria existencia de un documento de seguridad donde se plasmen las medidas adoptadas en la organización para cumplir las exigencias descritas en el reglamento, contemplando aspectos como: funciones y obligaciones del personal, registro de incidencias, identificación y autenticación, control de acceso y gestión de soportes. Se configura, por consiguiente, el citado documento como un elemento fundamental para la implementación de la seguridad de la organización y para el control de su implantación.

El capítulo III determina cuáles son las medidas de seguridad definidas para el nivel de seguridad medio. Estas medidas de seguridad alcanzan un mayor grado de exigencia sobre los apartados descritos en el capítulo II y, además, se introducen nuevos requerimientos como la existencia de un responsable de seguridad, la realización de auditorías del cumplimiento del propio reglamento o ciertas restricciones sobre los datos de pruebas.

La función definida para la figura del responsable de seguridad es únicamente la coordinación en materia de seguridad, es decir, forzar la designación de una o varias personas que se ocupen de la implantación y el cumplimiento de los procedimientos de seguridad en el seno de la organización. Este hecho no debe llevar a confusión sobre las responsabilidades derivadas del incumplimiento de lo dispuesto en el reglamento de medidas de seguridad, ya que las sanciones ocasionadas por las infracciones que pudieran producirse no recaerán, en ningún caso, sobre el responsa-

ble de seguridad sino sobre el responsable del fichero.

El borrador de reglamento propugnaba que los sistemas de información se sometieran a una auditoría interna o externa, al menos, cada dos años. En relación con el cumplimiento de este precepto, baste reseñar dos aspectos que podrían presentar una cierta controversia. En primer lugar, las dudas que, en algunos entornos, suscita la realización de una auditoría por parte de personal de la propia organización en relación con la independencia necesaria para practicarla. En segundo lugar, así como para los auditores de cuentas existe un censo oficial, no existe ningún registro oficial de los profesionales que puedan desempeñar tareas conocidas como "auditor informático" o "auditor de seguridad de los sistemas de información".

Al margen de los aspectos cuestionados, la obligación de someter el funcionamiento de la organización a una auditoría que determine el grado de cumplimiento del reglamento, permitirá proporcionar al responsable del fichero una visión independiente, en la que pueden constatarse problemas existentes en la actual situación.

El capítulo IV determina cuáles son las medidas de seguridad definidas para el nivel de seguridad alto. Estas medidas continúan incrementando el grado de exigencia sobre algunos de los apartados descritos en los capítulos II y III, y, a su vez, se introducen nuevos conceptos como el registro de auditoría de los accesos realizados o el cifrado en la transmisión de las comunicaciones.

El Capítulo V trata de las infracciones y sanciones. El incumplimiento de las medidas de seguridad descritas en el Reglamento constituye infracción grave de acuerdo con lo establecido en el artículo 43.3 h) de la Ley Orgánica 5/1992, difiriendo los procedimientos sancionadores que debe aplicarse a los ficheros de titularidad pública y a los ficheros de titularidad privada.

En el caso de ficheros de titularidad privada, la infracción podría ser sancionada con multa de 10.000.001 a 50.000.000 de conformidad con el artículo 44.2 de la citada Ley. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al grado de cumplimiento de las medidas de seguridad definidas en el reglamento, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia. 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.

Por su parte, cuando se trate de ficheros de los que sean responsables las Administraciones Públicas debe aplicarse, en cuanto al procedimiento y a las sanciones, lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

El Capítulo VI señala cuales son las competencias del Director de la Agencia en relación con las medidas de seguridad. Dichas competencias son las que aparecen reconocidas en el artículo 36 de la Ley Orgánica 5/1992, si bien aplicándolas, en concreto, al proyecto de reglamento: 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 normativa y 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 reglamento.

Por último, se ha establecido una disposición transitoria para señalar un plazo que haga factible la implantación de las medidas de seguridad del reglamento en los ficheros existentes, teniendo en cuenta en algún caso su complejidad tecnológica y el coste económico que pueden suponer para las organizaciones. Aunque los ficheros existentes en el momento de la entrada en vigor de reglamento dispondrán de un periodo transitorio de adaptación, aquellos ficheros de creación posterior a la entrada en vigor deberán ajustarse desde el inicio de su actividad a lo dispuesto en el reglamento.

En el caso de sistemas de información que se encuentren en funcionamiento en el momento de la entrada en vigor del reglamento, las medidas de seguridad de nivel básico previstas deberán implantarse en el plazo de seis meses, y las medidas de seguridad de nivel medio y alto en el plazo de un año. Además, en el caso de sistemas de información que se encuentren en funcionamiento y no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el reglamento, la adecuación de los mismos y la implantación de las medidas de seguridad pertinentes deberán realizarse en el plazo máximo de tres años.

La inscripción de los ficheros en el Registro General de Protección de Datos servirá de referencia para determinar los ficheros existentes en el momento de la entrada en vigor del reglamento. La Agencia, ante la obligación recogida en el artículo 38 de la Ley Orgánica 5/1992, considerará como inexistente todo aquel fichero que no figure inscrito en tal fecha en el Registro General de Protección de Datos.

1.4. CONCLUSIONES

El borrador del reglamento determina qué medidas de índole técnica y organizativa deben existir en una organización para garantizar 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.

Además, hay que reiterar que 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, tipificado en el artículo 43. 3. h) de la Ley Orgánica 5/1992, y, en consecuencia, ha determinado la imposibilidad de garan-

tizar el cumplimiento del principio de seguridad.

También debe destacarse que el borrador de reglamento determina los requerimientos que deben satisfacer los sistemas de información para garantizar la seguridad de los datos personales, 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, y teniendo siempre presente que su aplicación fuera posible a un coste "razonable". Además, el borrador procura no definir explícitamente, aunque en ocasiones resulta inevitable, los procedimientos a instaurar en las entidades para garantizar el cumplimiento los requerimientos exigidos, intentando no alterar su funcionamiento o su organización interna.

La publicación del reglamento finalmente aprobado supondrá una gran avance, debido a la falta de normativa existente en la materia, ya que, hasta la fecha, ningún país europeo ha publicado un reglamento de medidas de seguridad de obligado cumplimiento y de las repercusiones que, previsiblemente, el que aquí se ha descrito producirá sobre las organizaciones.

El objetivo perseguido en el momento de redactar el reglamento era establecer las bases para impulsar la implantación de medidas de seguridad en las organizaciones que garanticen el cumplimiento del principio de seguridad de datos establecido en el artículo 9 de la Ley Orgánica 5/1992, confiando en que el proceso se concluiría con autorregulaciones sectoriales.

La experiencia obtenida de aplicación del reglamento permitirá comprobar el grado de acierto en su elaboración y determinar sus deficiencias; así como ser empleada para la corrección de los problemas localizados.

2. RECOMENDACIONES A USUARIOS DE INTERNET

A lo largo del segundo trimestre de 1997, la Agencia, consciente del auge y difusión de las tecnologías basadas en Internet, elaboró un conjunto de recomendaciones encaminadas a orientar a los usuarios de Internet sobre aquellos aspectos relativos a la protección de su intimidad en el uso de los servicios electrónicos que ofrece la red Internet.

El desarrollo de estas recomendaciones finalizó con la publicación de las mismas, tanto en formato electrónico como en formato impreso, en Julio de 1997. En concreto, las Recomendaciones se presentaron a los medios de comunicación en el transcurso del Seminario celebrado en la Universidad Internacional Menéndez Pelayo sobre *La protección de los datos personales en España: situación y perspectivas*, dirigido por la Agencia. En estas mismas fechas, se daba de alta en la sede Web de la Agencia (http://www.ag-protecciondatos.es), la versión en formato electrónico del documento, que es libremente accesible a todos los usuarios. Adicionalmente la Agencia, como organismo para el que tienen especial importancia las relaciones con las autoridades de control de protección de datos europeas e internacionales, ha traducido a los idiomas francés e inglés las Recomendaciones, con el objetivo de presentarlas y difundirlas en todos aquellos foros de carácter internacional en los que participa. Además, el carácter transnacional del fenómeno Internet, impone la actuación coordinada de las autoridades de control del ámbito europeo, como pone de manifiesto la preocupación y trabajos que sobre el tema se han desarrollado en el Consejo de Europa, la Comisión Europea, etc.

Los objetivos perseguidos por la Agencia al elaborar las Recomendaciones se pueden resumir en los aspectos que a continuación se detallan.

En primer lugar, la rápida adopción de las tecnologías y servicios Internet por el colectivo general de consumidores, ha decantado una situación de rápido crecimiento y aparición de empresas y entidades que se relacionan con los usuarios por vía electrónica. Junto a la velocidad de aparición de servicios de publicidad, promoción de productos y servicios con fines comerciales a través de las páginas electrónicas en Internet, surge un nuevo contexto de relación con el consumidor, en el que a veces, dada la urgencia con que se desarrollan y promueven los servicios electrónicos, no se considera o sencillamente no existe, mecanismo alguno o procedimiento que garantice el respeto a los derechos que ampara la Ley Orgánica 5/1992. En especial, se observa la escasa atención que en las páginas electrónicas se concede a los principios de la protección de datos, como la calidad de datos, el derecho de información en la recogida de datos de carácter personal, el consentimiento del afectado, el deber de secreto, la cesión de datos a terceros o la seguridad de los datos de carácter personal.

La Agencia, observadora activa de esta situación, encontró necesario difundir entre los consumidores y usuarios de servicios electrónicos, aquellos aspectos más importantes en relación con la protección de los datos de carácter personal.

La finalidad perseguida era, por una parte, promover entre los usuarios o consumidores la adopción de una actitud activa de vigilancia y control de los datos de carácter personal que en el uso de los servicios electrónicos pudieran transferir de forma voluntaria o inadvertida, y por otra, que los propios usuarios, como agentes participantes del medio exigieran a los proveedores de servicios un tratamiento de los datos de carácter personal adecuado a los principios de la protección de datos.

No debe olvidarse que, a pesar de que Internet supone un contexto relativamente nuevo donde tienen lugar relaciones entre los usuarios o consumidores y las empresas y organizaciones que prestan servicios a través de este medio, en modo alguno está exento de adecuar estas nuevas formas de relación con los principios de protección de datos de carácter personal que nuestra legislación garantiza a todos los ciudadanos.

En segundo lugar, la propia naturaleza del medio en que se producen estas relaciones, plantea una situación intrínseca de tratamiento automatizado de cualquier dato de carácter personal que pudiera recolectarse, transmitirse o ser objeto de tratamiento en virtud de las relaciones que el usuario establece con los proveedores de servicios. Desde el punto de vista de la protección de datos, esta situación es especialmente preocupante por la potencia del propio medio, donde tienen lugar intercambios de información con una velocidad, volumen y ubicuidad sin precedentes en otros contextos.

En la redacción de las Recomendaciones se puso especial énfasis en que éstas fueran fácilmente accesibles al público al que se dirigían, elaborándolas de forma estructurada y utilizando un lenguaje lo más cercano posible a la terminología que se emplea de forma coloquial entre los usuarios y empresas que participan en el medio. La línea de exposición adoptada recorre las principales categorías de servicios electrónicos a los que se tiene acceso habitualmente a través de la red Internet, revisando detalladamente en cada caso, los aspectos más relevantes relativos a la protección de datos de carácter personal.

La Agencia, después de un estudio cuidadoso de cada servicio, y en contacto con entidades participantes del medio, como asociaciones de usuarios, empresas del sector, etc., ha intentado plasmar en las Recomendaciones aquellos aspectos, que a su juicio, deberían tener presentes, en cada caso, los usuarios o consumidores de los mismos, con el fin de no ser objeto de prácticas no compatibles con los principios de la protección de datos.

Asimismo, se informa de los mecanismos genéricos que ocasionalmente pudieran utilizar los usuarios de servicios Internet para evitar en la medida de lo posible las situaciones de riesgo en lo relativo a la recogida, tratamiento y difusión de los datos de carácter personal. En lo que sigue, y de manera sintética, se relacionan las conclusiones más importantes de cada servicio analizado.

En el servicio de páginas electrónicas World Wide Web, es especialmente destacable la recogida y/o difusión de datos de carácter personal, muchas veces sin que el usuario sea consciente de que el software que utiliza para acceder a estos servicios puede suministrar datos personales de manera inadvertida, y que además estos datos pueden ser accesibles de forma global por todos aquellos que tienen acceso a la red Internet. En este sentido, las Recomendaciones intentan transmitir al usuario que se acostumbre a utilizar activamente todos los mecanismos disponibles para evitar la transmisión *inadvertida* de datos de carácter personal, así como asegurarse, en el caso de transmitir voluntariamente estos datos, de que éstos sean protegidos con los mecanismos de seguridad adecuados, como cifrado, firma digital, etc.

En cuanto al servicio de correo electrónico y otros servicios de difusión asociados, como las listas de distribución y los grupos de noticias, los aspectos generales que se han querido destacar en las Recomendaciones son por una parte, la falta de seguridad de este servicio (en el sentido de que los mensajes de correo pueden ser falsificados o se puede suplantar la personalidad del emisor del mensaje) y por otra, la difusión pública de las opiniones vertidas en los mensajes dirigidos a las listas de distribución o foros de discusión, las cuales pueden ser malinterpretadas o someterse a utilizaciones no previstas o deseadas por el autor. Adicionalmente, las direcciones de correo constituyen uno de los datos más estrechamente vinculados con cada usuario, y además en ocasiones se asocian con el nombre y otros datos reales de la persona, lo cual puede permitir la recopilación o asociación de otro tipo de información de carácter personal, como profesión, intereses, aficiones, etc., para su posterior tratamiento con diversas finalidades. En este aspecto, las Recomendaciones están dirigidas a hacer consciente al usuario de estos aspectos, de forma que preste especial atención al contenido, destinatarios e información de carácter personal que vierte en los mensajes de correo que envía a través de este servicio.

Es en los servicios incipientes de comercio electrónico, donde cobran especial importancia cuestiones que pueden causar mayor preocupación a los usuarios de este medio, en la medida en que es precisamente en ellos donde se centran los intereses comerciales y económicos de los prestatarios del servicio, y donde más fácilmente se pueden plantear situaciones no compatibles con los derechos que ampara la Ley 5/92, en beneficio de otros intereses más prioritarios para el proveedor del servicio.

Temas tales como la garantía de anonimato en las transacciones efectuadas con el llamado dinero electrónico, la seguridad de las transacciones electrónicas y las técnicas de publicidad y de marketing empleadas en este tipo de servicios (como por ejemplo, el envío a través del correo electrónico de publicidad no deseada, o la elaboración de perfiles de interés o de consumo en función del comportamiento mostrado por el usuario a la hora de utilizar los servicios electrónicos), cobran todo su sentido en este tipo de servicios.

A este respecto, la Agencia ha intentado, en sus Recomendaciones, impulsar la atención activa de todos los usuarios en cuanto a los mecanismos a utilizar tanto por parte del consumidor como del prestatario del servicio para garantizar con eficacia la protección de los datos de carácter personal que estén involucrados en las transacciones efectuadas a través de servicios de comercio electrónico.

Por último, en los servicios de conversación electrónica o "chating" es especialmente destacable el hecho de que los usuarios de este servicio pueden ser identificados, asociando su seudónimo a datos de carácter personal reales, y permitiendo, por tanto, asociar las opiniones y comentarios vertidos en las conversaciones a la persona real. En este caso, el objetivo de las Recomendaciones es advertir de este riesgo a los usuarios de este servicio, y promover entre ellos el uso de mecanismos de opacidad que hagan imposible la asociación de su identidad real con la identidad que adoptan cuando se convierten en interlocutores en las charlas electrónicas.

3. CONFERENCIA EN LA UNIVERSIDAD DE VERANO MENÉNDEZ PELAYO CON EL TÍTULO :" LA PROTECCIÓN DE

DATOS EN ESPAÑA: SITUACIÓN Y PERSPECTIVAS DE FUTURO"

Se ha organizado una Conferencia en la Universidad de Verano Menéndez Pelayo con el título :" La protección de datos en España: situación y perspectivas de futuro", orientada a favorecer un encuentro entre expertos e interesados en esta materia que permitiera proporcionar una aportación al necesario proceso de difusión de la regulación legal y reglamentaria en materia de intimidad y datos personales automatizados.

* En la Conferencia se abordaron los siguientes temas:

- La Agencia de Protección de Datos ante las exigencias de la sociedad

- Situación actual de la protección de datos

- Ficheros con fines de publicidad: problemas actuales

- Los delitos informáticos en el Código Penal

- La protección de datos personales y la lucha contra la criminalidad internacional

- Internet y la delincuencia informática

- Intimidad e Internet

- Influencias económicas y sociales en Internet

- Internet frente a la protección de los menores y a la dignidad humana

- La intimidad frente a la prestación de servicios por parte de las Administraciones Públicas

- Tratamiento de datos personales y libertad de expresión

- Ficheros de morosos : problemas actuales

- Las transferencias internacionales de datos

- El futuro de la protección de datos

4. CONFERENCIA EUROIBEROAMERICANA SOBRE PROTECCIÓN DE DATOS PERSONALES

Se ha organizado **una Conferencia EuroIberoamericana sobre Protección de Datos Personales** a la que han asistido Autoridades de Protección de Datos Europeas y representantes de países Iberoamericanos. La Conferencia ha tenido como objetivo primordial el promover un encuentro entre profesionales que aportara un intercambio de opiniones, ideas y experiencias en relación con el proceso de elaboración de disposiciones legales y reglamentarias en esta materia que debe desarrollarse en los países latinoamericanos, y al propio tiempo contribuir con la experiencia europea en relación con la protección de datos personales.

Los representantes de los Países Iberoamericanos, las Autoridades de Control del Artículo 29 de la Directiva 95/46/CE y la Unión Europea (Dirección General XV de la misma) han mantenido en Madrid (España), , durante los días 12 y 13 de junio de 1997, una reunión en materia de protección de las personas físicas en lo que respeta al tratamiento de sus datos personales.

Como consecuencia de las deliberaciones habidas en la misma CONSTATAN.

La inexistencia en los países que integran Iberoamérica, de una legislación general y concreta relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos regida por principios tales como el de consentimiento, de finalidad, de proporcionalidad, de veracidad y de seguridad y en donde se reconozca y posibilite el ejercicio de los derechos de información, acceso, rectificación, cancelación y el derecho de oposición.

A la vista de lo anterior, teniendo en cuenta que, como dispone el apartado 2 de la Directiva 95/46/CE, "los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de la personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como el bienestar de los individuos", ACUERDAN emprender las siguientes medidas:

Impulsar ante los Gobiernos de sus respectivos países el desarrollo de medidas concretas en materia de protección de personas físicas en lo que respeta al tratamiento de datos personales.

Solicitar de la Conferencia de Ministros de Justicia de los países Iberoamericanos, que introduzca en el orden del día de su próxima reunión el tema de la protección de datos personales automatizados, y en desarrollo de las Recomen-

daciones ya aprobadas en anteriores reuniones, estudie la posibilidad de adoptar una ley tipo relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Comunicar al Grupo del artículo 29 cualquier cambio legislativo que se produzca en cada país a fin de que aquél pueda cumplir mejor con los cometidos señalados en el artículo 30 de la Directiva y en concreto en el apartado 1.b).

Poner a disposición de los países Iberoamericanos , por parte de las Autoridades de Control que integran el Grupo del artículo 29, cualquier información que pudiera resultar útil a los fines del presente documento. Entre otros, remitir a aquellos el informe anual sobre la situación de la protección de las personas físicas, al que se refiere el apartado 6. del artículo 30 de la Directiva.

Impulsar en la medida de lo posible el establecimiento de contactos bilaterales entre la Unión Europea (Dirección General XV) con los países Iberoamericanos, así como con la Organizaciones Internacionales en las que los mismos se encuentren integrados.

5. PRIMERA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES

Se ha convocado la **PRIMERA EDICIÓN DEL PREMIO "PROTECCIÓN DATOS PERSONALES",** con una dotación de un millón de 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 "Utilización y control de Datos Laborales Automatizados" presentada por Juan José Fernández Domínguez y Susana Rodríguez Escanciano. De la referida obra la Agencia ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional.

La obra premiada aborda las siguientes materias:

- Incidencia de la informática en la organización del trabajo. La erosión del contrato de trabajo típico
- Régimen Jurídico vigente en materia de tratamiento automatizado de datos personales. Aspectos generales y su trascendencia laboral.
- Repercusión específica de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal en el Derecho del Trabajo y de la Seguridad Social.

6. PARTICIPACIÓN EN DIVERSAS ACTIVIDADES DE ÁMBITO NACIONAL.

Durante 1997 la Agencia ha continuado su participación en diversas actividades en materia de protección de datos en el ámbito nacional como son congresos, seminarios, jornadas, grupos de trabajo y comisiones en diversos ámbitos y que a continuación procedemos a detallar.

6.1. GRUPO DE EXPERTOS EN INFORMACIÓN Y DOCUMENTACIÓN CLÍNICA PROMOVIDO POR EL MINISTERIO DE SANIDAD Y CONSUMO.

El Ministerio de Sanidad, ante la necesidad de desarrollar los derechos de los ciudadanos en materia de información y documentación clínica, expresados inicialmente en la Ley General de Sanidad, decidió crear un Grupo de Trabajo para que se encargara del estudio de los avances producidos en su definición, así como de elaborar propuestas para su desarrollo futuro.

Con este motivo, en junio de 1997, se recibió en la Agencia una invitación del Ministerio de Sanidad y Consumo, para participar en el Grupo de Expertos en Información y Documentación Clínica, constituyéndose dentro del mismo cuatro subgrupos de trabajo encargados de elaborar un documento de recomendaciones de actuación en relación con la información y documentación clínica que pudiera servir de base para una normativa posterior.

A lo largo de las diversas reuniones mantenidas, se puso de manifiesto que la problemática existente en materia de protección de datos se refiere fundamentalmente a los siguientes aspectos:

Mentalización en el sector médico: El problema principal es la reticencia del sector médico para aceptar algunas de las normas impuestas por la Ley Orgánica 5/1992, principalmente la relativas al acceso a la historia clínica y la cancelación de datos, ya que ésta es considerada una Ley demasiado general para que pueda aplicarse a los datos relativos a la salud de las personas.

Por esta razón es por la que en el documento final consta que se observa una necesidad urgente de abordar la definición de los principios esenciales de carácter general en relación con la historia clínica y la información en ella contenida, incorporando estos principios y su definición a una Ley específicamente sanitaria de rango legal suficiente.

Derecho de acceso: Sanitariamente la Historia Clínica es un conjunto de documentos que informan exhaustivamente acerca de la patología de los pacientes tratados en lo que se refiere a antecedentes y tratamiento aplicado.

La Historia Clínica está formada tanto por datos que se encuentran en soporte informático como por datos que no lo están. Dada la problemática existente en cuanto a la propiedad de la Historia Clínica, el sector médico no ve con claridad los datos que deben facilitarse a los pacientes ante una solicitud de los mismos, ya que en ella existen no sólo datos clínicos sino valoraciones de los mismos aportadas por los médicos.

Sin embargo la Ley Orgánica 5/1992 es muy clara a este respecto. Simplemente considera que si existen datos de carácter personal informatizados, el afectado tiene derecho a conocer la totalidad de los mismos.

Por otra parte, existe la problemática relativa a la información claramente perjudicial para la salud del paciente, respecto a la cual se concreta que es necesario tener en cuenta las excepciones establecidas en el artículo 14 de la Ley Orgánica 5/1992, así como el artículo 10 del Convenio sobre Derechos Humanos y Biomedicina que, después de establecer en el apartado 2, a modo de regla general que "toda persona tendrá derecho a conocer toda información obtenida respecto a su salud", prevé en su apartado 3 que "de modo excepcional, la Ley podrá establecer restricciones, en interés del paciente, con respecto al ejercicio de los derechos mencionados en el apartado anterior".

Período de conservación de los datos relativos a la salud: Otro problema existente es respecto al tiempo durante el que los datos pueden ser conservados. La Ley Orgánica 5/1992, en su art. 4.5 expresa que *los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados*, y, aunque en el mismo artículo se indica que reglamentariamente se determinará el procedimiento por el que se decida el mantenimiento íntegro de determinados datos, en el sector médico no se conoce de forma exacta cuando dejan de ser necesarios a pesar de haberse solucionado la patología tratada, ya que algunas de ellas pueden tener ciertas consecuencias con el transcurso del tiempo y la medicina, al no ser una ciencia exacta, necesita recabar en muchas ocasiones datos históricos sobre los pacientes.

Asimismo otra de las razones que implica la conservación de datos es la epidemiológica, respecto a la que el sector médico indica que en algunos casos es necesario conocer exactamente al paciente con objeto de poder realizar un seguimiento.

Así en el documento final queda escrito: "En cualquier caso, es preciso que, como mínimo, de cada uno de los episodios asistenciales contenidos en la historia clínica, se conserve de manera indefinida la identificación personal del paciente, el hecho de su asistencia (fecha, modalidad y unidad del centro y/o médico que la realizó) y los diagnósticos y procedimientos quirúrgicos realizados durante la misma.

Información a los afectados: Dado que en las inspecciones realizadas se ha observado que la información proporcionada a los pacientes acerca de los aspectos mencionados en el artículo 5 de la Ley Orgánica 5/1992 es bastante deficiente, se informa al Grupo de Expertos en Información y Documentación Clínica de la obligatoriedad de cumplir este requisito.

En las conclusiones plasmadas en el documento final, en relación a la legislación vigente se indica que "El art. 10 de la Ley General de Sanidad (LGS) constituye en este momento el marco normativo general más importante en relación con la información clínica. Asimismo, es de aplicación en el ámbito sanitario la Ley Orgánica 5/1992. Este marco puede y debe ser armonizado con los artículos. 5 a 9 del Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa firmado en Oviedo en abril de 1997, aún pendiente de su ratificación por las Cortes Generales y publicación en el BOE."

Asimismo se dice que "debe producirse una adecuación de la LGS (Ley General de Sanidad) de modo que el acceso a la información sanitaria por parte de familiares y allegados quede condicionado a la autorización del titular de la información".

Por último se indica que "El acceso a la información de la historia clínica se realizará de acuerdo con las condiciones que establezca la norma, según los supuestos de asistencia sanitaria u otros excepcionales. El paciente tendrá acceso a los resultados de las exploraciones e informes médicos que le permitan conocer de manera adecuada lo que se le ha realizado durante el episodio asistencial, así como los datos que sobre su estado de salud se disponen en la historia clínica".

6.2. SEMINARIO ORGANIZADO POR EL MINISTERIO DE SANIDAD Y CONSUMO CONJUNTAMENTE CON EL CONSEJO GENERAL DEL PODER JUDICIAL.

Durante los días 22 y 23 de septiembre de 1997 se ha celebrado en el Ministerio de Sanidad y Consumo el Seminario conjunto entre este Ministerio y el Consejo General del Poder Judicial. A tal efecto el Subsecretario de Sanidad y Consumo invitó a la Agencia para que designase un representante de la misma para integrarse en el grupo de 25 expertos que corresponde seleccionar al citado Ministerio, para participar en los debates de las jornadas.

Durante dichas Jornadas se puso de manifiesto las discrepancias existentes en torno a la propiedad de la Historia Clínica. Este hecho afecta al derecho de acceso a la misma por parte de los afectados.

A este respecto la Ley Orgánica 5/1992, establece que, en el momento que los datos hayan sido informatizados, cualquier afectado tiene derecho de acceso total a los mismos.

Concretamente, sobre la informatización y automatización de los datos de carácter personal, se puso de relieve el incremento del riesgo real de desprotección que implican, en particular los datos sensibles, al facilitar la posibilidad de su captación, uso y divulgación perniciosa, destacando la necesidad de adoptar medios técnicos y legales en adecuada colaboración, que garanticen su seguridad y utilización adecuada.

En cuanto a la cesión administrativa de datos sensibles para su exclusiva utilización con fines científicos, se insistió en que la misma ha de efectuarse extremando las medidas de seguridad y protección.

Finalmente en la última sesión no dejó de ponerse de relieve que, tras dos intensos días de discusión, el seminario hizo surgir más dudas que soluciones, más preguntas que respuestas.

6.3. PROYECTO HÁBITAT DE LA DIPUTACIÓN DE GRANADA.

El proyecto HÁBITAT persigue la investigación de un nuevo servicio para la puesta en marcha de Sistemas Telemáticos para personas mayores y discapacitadas. Las personas que recibieran el servicio lo harían a través del televisor de la casa, siendo estos servicios tales como Telemedicina, Teleasistencia, control domótico del entorno (persianas, electricidad, etc.), Teletrabajo, Teleformación, contacto a través de un centro de control con familiares, amigos, etc., entre otros.

La entidad promotora de este proyecto es la Diputación Provincial de Granada conjuntamente con otras entidades.

La Diputación de Granada reunió en abril de 1997, a un grupo de expertos en diversas materias, formándose siete subgrupos de trabajo con el objetivo de estudiar la viabilidad del proyecto.

La Agencia participó con un representante de la misma en el grupo nº 7 "Aspectos éticos y jurídicos del proyecto: la intimidad personal, la protección de datos, etc.".

El objetivo de este grupo ha sido definir el marco jurídico que afecta al proyecto HÁBITAT, así como elaborar un documento con la problemática existente.

En relación con la protección de datos, debido a que se desconocen aspectos como modo de recabar los datos de los afectados, así como tipo y forma en la que se pretende prestar los servicios posibles, no ha sido posible precisar las actuaciones a realizar, figurando al respecto en el documento de conclusiones elaborado por el grupo, el siguiente párrafo relativo a la Ley Orgánica 5/1992:

"En relación con la Ley 5/1992 (LORTAD), debemos especificar la conveniencia de tener en cuenta el origen de los datos recabados, que puede obligar a modificar las disposiciones de creación de los ficheros origen de los mismos, así como la inscripción en el Registro General de Protección de Datos, en relación a los fines para los que fueron recabados y las posibles cesiones existentes. En lo que respecta a posibles cesiones en las que estén implicadas entidades privadas, recordamos la necesidad de prestar consentimiento para la cesión de los datos. Destacar asimismo, que cuando se trate de datos especialmente protegidos es necesario el consentimiento expreso".

6.4. JORNADAS PARA LA SEGURIDAD Y EMERGENCIA PÚBLICA.

La Agencia ha participado en las V Jornadas de Sistemas de Información y Comunicación para la Seguridad y Emergencia Pública, que se celebraron en Valencia durante los días 25, 26 y 27 de noviembre de 1997. En las mismas intervinieron representantes operativos y técnicos de diversas Administraciones Públicas con competencias en el tema, entre otros, podemos destacar a: Policía Local, Guardia Civil, Sanidad, Comunidades Autónomas, Dirección General de Tráfico y diversas empresas especialistas en la prestación de servicios o suministro de equipos en el ámbito de seguridad y emergencia pública.

En primer lugar debemos hacer especial mención al Real Decreto 903/1997, de 16 de junio, por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112.

La citada norma incorpora al Derecho Español, lo establecido en la Decisión del Consejo de las Comunidades Europeas de 29 de julio de 1991, la obligación de los Estados miembro de introducir el número telefónico 112 en las respectivas redes telefónicas públicas, así como, en las redes digitales de servicios integrados y en las de los servicios públicos móviles, como número único de llamada de urgencia europeo.

El citado número gratuito podrá utilizarse por los ciudadanos, bien en su propio país o en otro Estado miembro, para requerir, en casos de urgente necesidad, la asistencia de los servicios públicos en materia de atención de urgencias sanitarias, de extinción de incendios y salvamento, de seguridad ciudadana y protección civil.

Los operadores de servicios de telefonía facilitarán la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas al número telefónico 112, sin perjuicio de las medidas que se adopten para garantizar el secreto de las comunicaciones, de acuerdo con lo establecido en el artículo 18.3 de la Constitución, y la protección de los datos personales, conforme a lo dispuesto en la Ley Orgánica 5/1992.

A continuación se reseñan brevemente los principales temas abordados en las citadas Jornadas, específicamente en el

seminario que versaba sobre el tema "Compartir Información" y en el que participó un representante de la Agencia:

- La necesidad de compartir información entre las diversas Administraciones Públicas implicadas en la prestación del servicio de atención de llamadas, con objeto de dar respuesta a la población en situaciones de emergencia. Entre otras, podemos señalar las siguientes instituciones: Fuerzas y Cuerpos de Seguridad, Sanidad, Tráfico, Bomberos y Protección Civil.

- La definición de los Sistemas de Información que necesita el centro prestador de los servicios de urgencia con objeto de cumplir con las funciones que se le encomienden.

- El establecimiento de medidas técnicas y organizativas necesarias para garantizar la confidencialidad de los datos personales manejados por todas las instituciones y personas implicadas.

- El análisis desde el punto de vista legal de la posibilidad de compartir información en relación a lo que establece las diversas normativas vigentes en materia, entre otras, de Protección de Datos, de Sanidad y de Fuerzas y Cuerpos de Seguridad no solamente a nivel nacional sino a nivel europeo e internacional.

Por otra parte, la implantación de este servicio por parte de las Comunidades Autónomas era muy escaso a primeros de 1998, no obstante, algunas de ellas tienen previsto su puesta en servicio a corto plazo.

Asimismo, con objeto de cumplir con lo establecido en el Real Decreto 903/1997, una entidad dedicada a la prestación de servicios de telecomunicaciones ha procedido a la modificación de la inscripción del fichero afectado en el Registro General de Protección de Datos.

6.5. SUBCOMITÉ ISO/IEC JTC 1/SC 27 - INFORMATION TECHNOLOGY - SECURITY TECHNIQUES

Por su especial interés en los aspectos relacionados con las medidas de seguridad aplicadas a los ficheros automatizados que contienen datos de carácter personal, la Agencia participa activamente desde 1996, en las actividades de este Subcomité técnico de la Organización Internacional de Estándares y de la Comisión Internacional de Electrotecnia (en inglés ISO - International Standards Organization e IEC - International Electrotechnical Comission).

El Subcomité ISO/IEC JTC 1/SC 27 forma parte del Comité Técnico de Normalización 71 (en adelante, CTN 71), cuyo ámbito de trabajo son la Tecnologías de la Información. Dentro del CTN 71, el Subcomité SC 27 se especializa en la Técnicas de Seguridad de los sistemas basados en las Tecnologías de la Información. En especial, las actividades principales de este Subcomité se pueden resumir en:

- La identificación de requisitos genéricos y metodologías para la elaboración de requisitos de servicios de seguridad en los sistemas basados en tecnologías de la información.

- El desarrollo de técnicas y mecanismos de seguridad, incluyendo procedimientos de registro y relaciones entre los componentes de seguridad.

- El desarrollo de directrices de seguridad, como por ejemplo documentos de interpretación, análisis de riesgos, etc.

- El desarrollo de documentación de apoyo a la gestión de la seguridad y de estándares en esta materia.

Las actividades del Subcomité SC 27 están divididas internamente en tres grupos de trabajo, denominados Grupo de Trabajo 1 (Requisitos, Servicios de Seguridad Directrices), Grupo de Trabajo 2 (Técnicas y mecanismos de seguridad) y Grupo de Trabajo 3 (Criterios de Evaluación de la Seguridad).

De manera más concreta, los temas principales que desarrolla el Grupo de Trabajo 1, son en primer lugar, la identificación de requisitos de seguridad de las aplicaciones y los sistemas, en segundo lugar el desarrollo de estándares de servicios de seguridad, como por ejemplo, servicios de autenticación, de control de acceso, integridad, confidencialidad, gestión y auditoría, y en tercer lugar, el desarrollo de documentos de soporte a la interpretación de requisitos de seguridad, como por ejemplo, directrices de seguridad, glosarios, análisis de riesgos.

El Grupo de Trabajo 2 centra sus actividades en torno a la identificación de necesidades y requisitos que precisan las técnicas y mecanismos de seguridad en los sistemas y aplicaciones de las tecnologías de la información y el desarrollo de terminología, modelos generales y estándares de utilización de las técnicas y mecanismos de seguridad en los servicios de seguridad. Este ámbito incluye, de manera especial, las técnicas y mecanismos basadas en el cifrado simétrico, asimétrico o sin cifrado , en lo relativo a la confidencialidad de la información, autenticación de entidades, no repudio, gestión de claves de cifrado e integridad de datos aplicada a la autenticación de mensajes, funciones de dispersión o distribución de claves (hash functions) y firma digital.

Finalmente, el Grupo de Trabajo 3 se dedica al desarrollo de estándares para la evaluación y certificación de la seguridad de los sistemas basados en las tecnologías de la información, de sus componentes y de productos. En particular, se incluyen en su ámbito, las redes de ordenadores, los sistemas distribuidos, servicios de aplicación asociados, etc.

La Agencia participa especialmente en las actividades del Grupo de Trabajo 3, junto con los demás representantes del cuerpo nacional español del Subcomité SC 27. A la sección española del SC 27 pertenecen las principales empresas y

entidades nacionales dedicadas a la seguridad de la información, tanto del sector privado como del sector público.

- A lo largo del año 1997, han tenido lugar un total de cinco reuniones plenarias de la sección española del SC 27, en las que en síntesis, se han revisado un gran número de documentos y se han comenzado los preparativos para organizar la Conferencia Plenaria (Plenary meeting) del ISO/IEC JTC 1/SC 27 en Madrid, en abril de 1999.

7. ÓRGANOS CORRESPONDIENTES A LAS COMUNIDADES AUTÓNOMAS

El artículo 40 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, dispone que las funciones reguladas en el 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.

Durante el año 1997, la Comunidad de Madrid pone en marcha la Agencia de Protección de Datos de la Comunidad de Madrid, creando de esta forma la primera Agencia Autonómica. Por otra parte, ha sido presentado a informe en la Agencia de Protección de Datos el Proyecto de Ley sobre Informática y Protección de Datos de la Administración de la Comunidad Autónoma de Aragón.

Comunidad de Madrid

La Agencia de Protección de Datos de la Comunidad de Madrid fue creada como una Entidad de Derecho Público independiente, por la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid (BOE nº 170, de 18 de julio de 1995) que desarrolla, en el ámbito de sus competencias, la Ley Orgánica 5/92. Mediante la Ley 13/1997, de 16 de junio, se introdujeron una serie de modificaciones, precisando la naturaleza y funciones de la Agencia de Protección de Datos de la Comunidad de Madrid, a fin de facilitar su puesta en marcha.

La puesta en funcionamiento de la Agencia de Protección de Datos de la Comunidad de Madrid requería la constitución de su Consejo de Protección de Datos, previsto en el artículo 29 de la Ley 13/95, que se produjo el día 30 de julio de 1997, con un Orden del día único, orientado a la designación del Director de la Agencia de Madrid, en cumplimiento de las atribuciones legales que los artículos 29.1 y 29.4 de la Ley 13/95, confieren al Consejo. La designación, por unanimidad, recayó en Doña Rosa María García Ontoso, produciéndose el nombramiento oficial mediante el Decreto 106/1997, de 31 de julio, del Presidente de la Comunidad de Madrid, publicado en el Boletín Oficial de la Comunidad de Madrid nº 185, de 6 de agosto de 1997.

Junto a las acciones anteriores, necesarias para la constitución y puesta en funcionamiento de la Agencia de Protección de Datos de la Comunidad de Madrid, fue necesario proceder a la creación de los puestos de trabajo necesarios para el correcto desarrollo de las competencias y funciones que aquélla tiene encomendadas.

Entre los meses de agosto y septiembre, la Agencia de Madrid ha trabajado fundamentalmente en su propia constitución, en la preparación de su sede y en la contratación del personal de forma que, en el mismo año 1997, ha empezado a realizar los trabajos encomendados.

El Área de Atención al Ciudadano comenzó a funcionar en septiembre, atendiendo las primeras 150 consultas, según datos facilitados por dicho organismo, de las que algunas debieron remitirse a la Agencia de Protección de Datos, por exceder el ámbito competencial de la Agencia de Madrid.

En el mes de noviembre comenzaron unas sesiones formativo-informativas a las que acudieron aproximadamente 100 directivos y cargos de nivel medio de la propia Comunidad de Madrid, responsables de los ficheros y de los tratamientos efectuados con los datos. En dichas sesiones, la Agencia de Protección de Datos de la Comunidad de Madrid les ha dado información sobre la Ley, sobre su aplicación y los derechos de los ciudadanos.

De conformidad con lo establecido en el artículo 40.3 de la Ley Orgánica 5/92, la Agencia de la Comunidad de Madrid, mantiene con la Agencia de Protección de Datos la cooperación institucional y coordinación a que se refiere dicho precepto, siendo de destacar el favorable grado de colaboración establecido entre la Agencia de Protección de Datos y la primera Agencia Autonómica.

Comunidad Autónoma de Aragón

El Proyecto de Ley sobre Informática y Protección de Datos de la Administración de la Comunidad Autónoma de Aragón, prevé la creación del Registro Aragonés de Protección de Datos, como órgano dependiente del Departamento de Presidencia y Relaciones Institucionales de la Diputación General de Aragón. Las funciones que el artículo 36 de la Ley Orgánica 5/92, atribuye a la Agencia de Protección de Datos y cuya asunción por las Comunidades Autónomas autoriza el artículo 40 de la Ley Orgánica 5/92, se distribuyen entre este Registro y el Justicia de Aragón, que actúa a su vez como órgano de conexión del mencionado Registro con la Agencia de Protección de Datos.

La Agencia de Protección de Datos ha analizado este Proyecto de Ley, desde la perspectiva de la adecuación al orden constitucional de la distribución de competencias que establece entre el Registro Aragonés de Protección de Datos y el

Justicia de Aragón, ya que podría contravenir lo dispuesto en los artículos 40 y 41 de la Ley Orgánica 5/92. En este sentido fue evacuado el correspondiente informe con fecha 19 de diciembre.

MEMORIA DE 1997 - ANEXO I - INFORMES PRECEPTIVOS EVACUADOS POR LA AGENCIA DE PROTECCIÓN DE DATOS

Proyecto de Disposición	Solicitado por	Fecha informe
Proyecto del documento "Instrucciones Generales sobre Seguridad y Protección de Datos".	**Presidente Ejecutivo del** Instituto Nacional de la Salud (INSALUD**).**	**7-2-1997**
Anteproyecto de Ley de Modificación de la Ley 13/1995, de 21 de abril, de regulación del uso de informática en el tratamiento de datos personales por la Comunidad de Madrid.	**Viceconsejero de Hacienda de la** Comunidad de Madrid.	**18-2-1997**
Proyecto de Circular sobre Recogida de Información por Funcionarios del Cuerpo Nacional de Policía adscritos al Área de Seguridad Ciudadana, relacionada con el Terrorismo y el Tráfico ilícito de Estupefacientes.	**Secretario de Estado de Seguridad del** Ministerio del Interior**.**	**20-2-1997**
Proyecto de Reglamento del Centro de Documentación Judicial del Consejo General del Poder Judicial.	**Presidente de la Comisión de Estudios e Informes del** Consejo General del Poder Judicial.	**27-2-1997**
Proyecto de Real Decreto sobre Organización del Centro de Investigaciones Sociológicas, Organismo autónomo del Ministerio de la Presidencia.	**Secretario General Técnico del** Ministerio de Justicia.	**4-3-1997**

Proyecto de Disposición	Solicitado por	Fecha informe
Proyecto de Real Decreto sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo, del Ministerio de Trabajo y Asuntos Sociales.	**Secretario General Técnico del** Ministerio de Justicia.	**7-3-1997**
Proyecto de Real Decreto sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo, del Ministerio de Trabajo y Asuntos Sociales.	**Secretario General Técnico del** Ministerio de Justicia **.**	**7-3-1997**
Proyecto de Instrucción de la Secretaría de Estado de Seguridad sobre la organización y funciones de la Inspección de Personal y Servicios de Seguridad.	**Secretario de Estado de Seguridad del** Ministerio del Interior**.**	**10-3-1997**
Proyecto de Orden Ministerial de modificación de la Orden de 22 de julio de 1994, reguladora de los ficheros de tratamiento automatizado de datos de carácter personal del Ministerio de Administraciones Públicas.	**Subdirector General de Informes del** Ministerio de Administraciones Públicas **.**	**13-5-1997**
Proyecto de Real Decreto por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal.	**Secretario General Técnico del** Ministerio de Justicia **.**	**20-5-1997**

Proyecto de Disposición	Solicitado por	Fecha informe
Anteproyecto de Ley Estadística de la Región de Murcia	**Secretario GeneralConsejería de Economía y Hacienda**Comunidad Autónoma de la Región de Murcia	**27-5-1997**
Proyecto del documento "Borrador de orientaciones provisionales para la puesta en funcionamiento de las Unidades de Control Operativo para la prevención de la violencia en los espectáculos".	**Secretario General Técnico del** Ministerio del Interior **.**	**28-5-97**
Proyecto de Orden por la que se regula el funcionamiento del Registro Central de Sanciones Impuestas por Infracciones contra la Seguridad pública en materia de espectáculos deportivos.	**Secretario General Técnico del** Ministerio del Interior	**8-7-97**
Proyecto de Circular de la Tesorería General de la Seguridad Social relativo a cesiones de datos en favor de otras Administraciones.	**Director General de la Tesorería General de la Seguridad Social.** Ministerio de Trabajo y Asuntos Sociales.	**28-7-97**
Proyecto de introducción de un párrafo final en el apartado primero del artículo 113 de la Ley General Tributaria (La APD no se muestra favorable).	**Agencia Estatal de la** Administración Tributaria **(Solicitado a través del Subsecretario de Justicia**	**25-9-97**

Proyecto de Disposición	Solicitado por	Fecha informe
Anteproyecto de Ley de Medidas Fiscales, Administrativas y del Orden Social, y addenda del mismo. (Que acompaña a los presupuestos de 1998).	**Secretario General Técnico del** Ministerio de Justicia	**26-9-97**
Anteproyecto de Ley de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, sobre la protección jurídica de las bases de datos.	**Secretario General Técnico del** Ministerio de Justicia	**1-10-97**
Informe del proyecto de Resolución de la Secretaría de Estado de la Seguridad Social por la que se garantiza la identificación única de las personas físicas y jurídicas en el sistema de información de la Seguridad Social en cumplimiento de lo establecido en el artículo 36.h) de la L.O. 5/1992 y artículo 5.b) del R.D. 428/1993	**Secretario General Técnico del** Ministerio de Justicia	**21-10-97**
Informe sobre el Proyecto de Orden Ministerial por la que se crea y regula el Índice Nacional de Defunciones.	**Secretario General Técnico del** Ministerio de Justicia.	**19-12-97**
Informe sobre Proyecto de Ley del Justicia de Aragón y su adecuación en cuanto a las competencias que atribuye a la Dirección General de Cooperación Autonómica del Ministerio de Administraciones Públicas.	**Secretario General Técnico del** Ministerio de Justicia.	**19-12-97**
		TOTAL = 20

MEMORIA DE 1997 - ANEXO II - CONSEJO DE EUROPA - COMITÉ DE MINISTROS

RECOMENDACIÓN Nº R (97) 5 DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS RELATIVA A PROTECCIÓN DE DATOS MÉDICOS

(adoptada por el Comité de Ministros del 13 de febrero de 1997,durante la 584ª reunión de los Delegados de los Ministros)

El Comité de Ministros, en virtud del Artículo 15.b del Estatuto del Consejo de Europa,

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Recordando los principios generales relativos a protección de datos, correspondientes al Acuerdo para proteger a las personas en cuanto respecta al tratamiento automatizado de datos de carácter personal (Serie de los Tratados Europeos, nº 108), y especialmente su Artículo 6, donde se enuncia que los datos de carácter personal relativos a la salud no pueden ser tratados automáticamente a menos que el derecho interno haya previsto garantías adecuadas;

Consciente del hecho de que el tratamiento automatizado de datos médicos mediante sistemas de información se encuentra cada vez más extendido, no sólo en materia de cuidados médicos, investigación médica, gestión hospitalaria y sanidad pública, sino también fuera del sector de los cuidados sanitarios;

Convencido de la importancia que para la salud de la persona interesada y de sus allegados entrañan la calidad, integridad y disponibilidad de los datos médicos;

Consciente de que el avance de la Ciencia Médica depende en gran medida de la disponibilidad de datos médicos de los individuos;

Persuadido de que es deseable reglamentar la recogida y tratamiento de datos médicos, garantizar el carácter confidencial y la seguridad de los datos de naturaleza personal referidos a la salud, aparte de velar por que se haga uso de los mismos dentro del respeto a los derechos y libertades fundamentales del individuo, sobre todo el derecho a la vida privada;

Consciente de que los avances conseguidos por la Ciencia Médica y los progresos registrados por la tecnología de la información desde 1981 requieren que se revisen varias disposiciones de la Recomendación nº R (81) I, referida a la reglamentación aplicable a los bancos de datos médicos automatizados;

Recomienda a los Gobiernos de los Estados miembros:

- que tomen medidas para que los principios contenidos en el anexo de la presente recomendación se reflejen en su Derecho y en su práctica;

- que garanticen una amplia difusión de los principios contenidos en el anexo de la presente recomendación entre las personas que recogen y tratan datos médicos a título profesional;

Decide que la presente recomendación sustituya a la Recomendación nº R (81) I, relativa a reglamentación aplicable a los bancos de datos médicos automatizados.

Anexo a la Recomendación nº R (97) 5

I. Definiciones

Para los fines de la presente recomendación:

- la expresión "datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable. No se considerará identificable a una persona física si la identificación en sí requiere plazos y actividades al margen de lo razonable. Cuando una persona física no sea identificable, los datos se considerarán anónimos;

- 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;

- la expresión "datos genéticos" se refiere a todos los datos, de cualquier tipo, relacionados con los caracteres hereditarios de un individuo o que, vinculados a dichos caracteres, compongan el patrimonio de un grupo de individuos emparentados.

Hace referencia de la misma manera a todos los datos que afecten a intercambios de información genética (genes) de un individuo o línea genética, con relación a cualquier aspecto de la salud o de una enfermedad, constituya o no un

carácter identificable.

La línea genética estará constituida por similitudes genéticas resultantes de una procreación y compartidas por dos o más individuos.

2. Ámbito de aplicación

2.1 La presente recomendación es aplicable a la recogida y tratamiento automatizado de datos médicos, a menos que la legislación interna prevea otras garantías adecuadas dentro de un contexto específico apartado del ámbito propio de los cuidados sanitarios.

2.2. Un Estado miembro podrá ampliar los principios enunciados en la presente recomendación a los datos médicos que no sean objeto de un tratamiento automatizado.

3. Respeto de la vida privada

3.1 El respeto de los derechos y libertades fundamentales, especialmente del derecho a la vida privada, deberá garantizarse durante la recogida y tratamiento de datos médicos.

3.2. Los datos médicos sólo podrán recopilarse y tratarse de conformidad con las oportunas garantías, que habrán de ser previstas por la legislación interna.

En principio, la recogida y tratamiento de datos médicos sólo debería ser tarea de profesionales dedicados a los cuidados sanitarios o de personas o entidades intervinientes por cuenta de profesionales sanitarios. Las personas o entidades que intervengan por cuenta de profesionales sanitarios y que recojan y traten datos médicos, deberían someterse a las normas de confidencialidad propias de los profesionales sanitarios o normas de confidencialidad equivalentes.

Los responsables de ficheros que no sean profesionales sanitarios sólo deberían recoger y tratar datos médicos dentro del respeto de las normas de confidencialidad equivalentes a las que afectan a un profesional sanitario o bien con el concurso de garantías de eficacia iguales a las previstas por la legislación interna.

4. Recogida y tratamiento de datos médicos

4.1. La recogida y tratamiento de datos médicos deberá llevarse a cabo de manera honesta y lícita, y únicamente con fines determinados.

4.2. En principio, los datos médicos deberán tomarse de la persona interesada. Sólo podrán recopilarse a través de otras fuentes si éstas se ajustan a los principios 4, 6 y 7 de la presente recomendación y con la condición de que ello sea necesario para la finalidad del tratamiento o que la persona interesada no se encuentre en condiciones de aportar los datos.

4.3. Los datos médicos podrán recopilarse y tratarse:

a. si la legislación lo prevé:

i. para fines de salud pública; o

ii. a reserva del principio 4.8, para fines consistentes en prevenir un peligro concreto o para reprimir una infracción penal determinada; o

iii. para otros fines de interés público de importancia; o

b. en la medida en que la ley lo autorice:

i. para fines médicos preventivos o para fines de diagnóstico o terapéuticos referidos a la persona interesada o de un pariente de línea genética; o

ii. para fines de salvaguarda de intereses vitales de la persona interesada o de una tercera persona; o

iii. para finalidades consistentes en respetar una obligación contractual específica; o

iv. para fines de comprobación, ejercicio o defensa de un derecho judicialmente;

c. si la persona interesada o su representante legal, o una autoridad, o cualquier otra persona o instancia designada por la ley lo consienten, para una o varias finalidades y mientras la legislación interna no se oponga a ello.

4.4. Cuando los datos médicos se hayan recogido con fines médicos preventivos o fines de diagnóstico o terapéuticos referidos a la persona en cuestión o a un pariente de la línea genética, podrán tratarse igualmente con finalidad de gestionar un servicio sanitario que revierta en beneficio del paciente, en el caso de que el profesional sanitario ocupado de recoger los datos aporte la gestión o cuando los datos se comuniquen de conformidad con las disposiciones enunciadas en los principios 7.2 y 7.3.

Feto

4.5. Los datos médicos relativos al feto deberían considerarse datos de carácter personal y disfrutar de un grado de protección comparable a la correspondiente a los datos médicos de un menor.

4.6. A menos que la legislación interna lo establezca de otro modo, el poseedor de responsabilidades paternas podrá intervenir en nombre del feto en calidad de persona jurídicamente facultada como persona interesada.

Datos genéticos

4.7. Los datos genéticos recogidos y tratados con fines preventivos, de diagnóstico o terapéuticos con respecto a la persona interesada o con un objetivo de investigación científica, sólo deberían utilizarse con estas únicas finalidades o para permitir a la persona interesada tomar una decisión libre y fundamentada a este respecto.

4.8. El tratamiento de datos genéticos debido a necesidades de procedimiento judicial o de investigación penal debería ser objeto de una ley específica que ofrezca garantías apropiadas.

Estos datos deberían servir exclusivamente para comprobar la existencia de un vínculo genético en el contexto de la administración de la prueba, para prevenir un peligro concreto o la sanción de una determinada infracción penal. No deberían emplearse en ningún caso para determinar otras características que puedan estar genéticamente relacionadas.

4.9. Con distintos fines de los previstos en los principios 4.7 y 4.8, la recogida y tratamiento de datos genéticos deberían estar permitidos, en principio, únicamente por motivos sanitarios y sobre todo para evitar cualquier perjuicio serio para la salud de la persona interesada o de terceros.

Sin embargo, la recogida y tratamiento de datos genéticos con miras a detectar enfermedades, podrán permitirse en caso de superiores intereses y con la condición de que existan garantías apropiadas y definidas por la ley.

5. Informaciones de la persona interesada

5.1. La persona afectada deberá estar informada de los siguientes elementos:

a. existencia de un fichero que contiene sus datos médicos y categoría de datos recogidos o pendientes de recopilar;

b. la o las finalidades para las cuales se tratan o se tratarán los datos en cuestión;

c. llegado el caso, personas u organismos de los cuales se recogen o recogerán los datos;

d. personas u organismos a los cuales -y objetivos para los cuales- podrán comunicarse los datos;

e. posibilidad para la persona interesada, llegado el caso, de no dar su consentimiento, retirarlo y consecuencias de tal retirada;

f. identidad del responsable del fichero y de su representante llegado el caso, así como las condiciones para ejercitar el derecho de acceso y rectificación.

5.2. La persona interesada debería estar informada, a lo más tardar en el momento de proceder a la recogida. Sin embargo, cuando los datos médicos no se obtengan de la persona interesada, ésta debería estar informada de tal recogida lo más rápidamente posible, así como, apropiadamente, de los elementos mencionados en el principio 5.1, salvo si esto careciera manifiestamente de sentido o no resultara factible o si la persona interesada hubiera recibido ya la información.

5.3. La información de la persona interesada deberá ser apropiada y estar adaptada a las circunstancias. Preferiblemente, cada persona interesada debería ser informada de manera individual.

5.4. Antes de llevar a cabo un análisis genético, la persona interesada debería estar informada de los objetivos del mencionado análisis y de la eventualidad de descubrimientos inesperados.

Incapaces legales

5.5. Si la persona interesada fuera una persona legalmente incapaz y no estuviera en condiciones de tomar determinaciones libremente, y si la legislación interna no le permitiera intervenir en su propio nombre, la información deberá aportarse a la persona con capacidad legal para actuar en interés de la persona en cuestión.

Si tuviera capacidad de entendimiento, la persona legalmente incapaz debería ser informada con anterioridad a la recopilación o tratamiento de los datos que le afectan.

Derogaciones

5.6. Podrán derogarse los principios 5.1, 5.2 y 5,3 en los siguientes casos.

a. la información de la persona interesada podrá limitarse si la derogación está prevista por la legislación y constituye una medida necesaria dentro de una sociedad democrática:

i. para prevenir un peligro concreto o para reprimir una infracción penal;

ii. por razones de salud pública;

iii. para proteger a la persona interesada y los derechos y libertades de los demás;

b. en caso de urgencia médica, los datos considerados necesarios para el tratamiento médico podrán recogerse antes de proporcionar la correspondiente información.

6. Consentimiento

6.1. Cuando se pida a la persona interesada su consentimiento, éste debería ser libre, expreso y fundamentado.

6.2. Los resultados de cualquier análisis genético deberían formularse dentro de las limitaciones de objetivos de la consulta médica, diagnóstico o tratamiento para los cuales se obtenga el consentimiento.

6.3. Cuando se aborde el tratamiento de datos médicos referidos a una persona legalmente incapaz que no se encuentre en condiciones de decidir libremente y cuando el derecho interno no permita a la persona interesada intervenir en su propio nombre, se requerirá el consentimiento de la persona que pueda intervenir legalmente en nombre de la persona interesada, el de una autoridad o de cualquier otra persona o instancia designada por la ley.

Si, de conformidad con el principio 5.5 anterior, la persona legalmente incapacitada hubiera sido informada de la intención de recoger o tratar sus datos médicos, debería tomarse en consideración su deseo a menos que la legislación interna se oponga a ello.

7. Comunicación

7.1. No deberán comunicarse los datos médicos, salvo dentro de las condiciones enumeradas en el marco del presente principio y del principio 12.

7.2. En especial, a menos que la legislación interna prevea otras garantías apropiadas, la comunicación de datos médicos sólo podrá llevarse a cabo si el destinatario se somete a las normas de confidencialidad propias de los profesionales sanitarios o a normas de confidencialidad equivalentes, y solamente si se respetan las disposiciones de la presente recomendación.

7.3. Los datos médicos podrán ser comunicados si son pertinentes y:

a. si la legislación prevé la comunicación y constituye una medida necesaria dentro de una sociedad democrática con fines:

i. de salud pública; o

ii. de prevención de un peligro concreto o para sancionar una infracción penal determinada; o

iii. de otro tipo de interés público de importancia; o

iv. de la protección de los derechos y libertades de los demás;

b. si la ley autoriza la comunicación con los fines de:

i. protección de la persona interesada o de un pariente de línea genética; o

ii. salvaguarda de intereses vitales de la persona en cuestión o de una tercera persona; o

iii. respeto de obligaciones contractuales específicas; o

iv. comprobación, ejercicio o defensa de un derecho judicialmente; o

c. si la persona interesada o su representante legal, o una autoridad, o cualquier otra persona o instancia designada por la ley lo consienten para una o varias finalidades y mientras la legislación interna no se oponga a ello;

d. a menos que la persona interesada o su representante legal, o una autoridad o cualquier persona o instancia legalmente designada no se opongan a ello expresamente cuando la comunicación no sea obligatoria, si los datos se han recogido en un contexto preventivo, de diagnóstico o terapéutico libremente escogido y si la finalidad de la comunicación no es incompatible con el fin del tratamiento para el cual se han recogido tales datos, especialmente con objetivos de cumplimiento de cuidados para el paciente o gestión de un servicio sanitario interviniendo en interés del paciente.

8. Derechos de la persona interesada

Derechos de acceso y rectificación

8.1. Todas las personas podrán tener acceso a los datos médicos que se refieran a ellas, ya sea directamente o a través de un profesional sanitario o, en caso de permitirlo la legislación interna, a través de una persona por ella misma designada. Las informaciones habrán de estar accesibles en forma comprensible.

8.2. Podrá negarse, limitarse o diferirse el acceso a datos médicos sólo cuando la ley así lo establezca y:

a. En caso de que esto constituya una medida necesaria para proteger la seguridad del Estado, la seguridad pública o reprimir las infracciones penales dentro de una sociedad democrática; o

b. si el conocimiento de tales informaciones es susceptible de originar un grave atentado contra la salud de la persona interesada; o

c. si la información sobre la persona interesada pone al mismo tiempo de manifiesto informaciones relativas a terceros o, en lo referente a datos genéticos, si tales informaciones son susceptibles de originar un grave atentado contra los parientes consanguíneos o uterinos o contra una persona directamente vinculada con esta línea genética; o

d. si los datos se emplean para fines estadísticos o investigaciones científicas cuando no existan riesgos manifiestos de atentado contra la vida privada de las personas interesadas, especialmente debido al hecho de que los datos no se utilicen para decisiones o medidas relativas a una determinada persona.

8.3. La persona interesada podrá solicitar la rectificación de datos erróneos que le afecten y, en caso de recibir la negativa por respuesta, podrá presentar recurso.

Descubrimientos inesperados

8.4. La persona sometida a un análisis genético debería ser informada de los descubrimientos imprevistos si se cumplen las siguientes condiciones:

a. que la legislación interna no prohíba tal información;

b. que la persona haya solicitado explícitamente esta información;

c. que la información no sea susceptible de conllevar un grave perjuicio:

i. para la salud de la persona; o

ii. para un pariente consanguíneo o uterino de la persona, para un miembro de su familia social o para una persona directamente vinculada a la línea genética de la persona, a menos que la legislación interna prevea otras garantías convenientes.

A reserva de lo expuesto en el párrafo a, la persona deberá estar igualmente informada si los descubrimientos revisten para ella una importancia terapéutica o preventiva directa.

9. Seguridad

9.1. Deberán tomarse medidas técnicas y de organización adecuadas para proteger los datos de carácter personal, tratados de conformidad con la presente recomendación, contra destrucción -accidental o ilícita- y pérdida accidental, así como contra el acceso, modificación, comunicación o cualquier otra forma de tratamiento no autorizada.

Estas medidas habrán de garantizar un nivel de seguridad apropiado, habida cuenta, por una parte, de las condiciones técnicas y, por otra parte, de la sensible naturaleza de los datos médicos y de la evaluación de riesgos potenciales.

Estas medidas deberán ser objeto de un examen periódico.

9.2 Sobre todo con el fin de garantizar la confidencialidad, integridad y exactitud de los datos objeto de tratamiento, así como la protección de los pacientes, deberán tomarse medidas apropiadas tendentes a:

a. impedir a cualquier persona no autorizada el acceso a las instalaciones empleadas para tratar datos de carácter personal (control a la entrada de las instalaciones);

b. impedir que los soportes de datos puedan ser leídos, copiados, modificados o trasladados por una persona no autorizada (control de soportes de datos);

c. impedir la introducción no autorizada de datos en el sistema de información, así como cualquier acceso al conocimiento, modificación o borrado sin autorización de datos de carácter personal memorizados (control de memoria);

d. impedir que sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas con ayuda de instalaciones de transmisión de datos (control de uso);

e. garantizar, con miras al acceso selectivo de los datos, por una parte, y a la seguridad de los datos médicos, por otra parte, que el tratamiento de los mismos se conciba en términos generales de manera que sea posible el tratamiento por separado:

- de las identificaciones y datos relativos a la identidad de las personas;
- de los datos administrativos;
- de los datos médicos;
- de los datos sociales;
- de los datos genéticos (control de acceso);

f. garantizar que pueda comprobarse y verificarse con qué personas o con qué entidades de datos de carácter personal pueden establecerse comunicaciones a través de instalaciones de transmisión de datos (control de comunicación);

g. garantizar que pueda comprobarse y verificarse con posterioridad quién accedió al sistema y qué datos de carácter personal fueron introducidos en el sistema de información, en qué momento y a través de qué persona (control de introducción);

h. impedir que, durante la comunicación de datos de carácter personal, así como durante el transporte de soportes de datos, estos puedan ser leídos, copiados, modificados o borrados sin autorización (control del transporte);

i. salvaguardar los datos mediante constitución de copias de seguridad (control de disponibilidad).

9.3. Los responsables de ficheros médicos deberían, de conformidad con la legislación interna, establecer un reglamento interno apropiado, dentro del respeto de los principios pertinentes de la presente recomendación.

9.4. De ser necesario, los responsables de ficheros que traten datos médicos deberían designar una persona independiente responsable de la seguridad de los sistemas de información y de la protección de datos, con competencia para prestar asesoramiento en la materia.

10. Conservación

10.1. Por regla general, los datos médicos sólo deberán conservarse durante el período necesario para alcanzar el objetivo que requiera recogerlos y tratarlos.

10.2. Cuando la conservación de datos médicos que ya no se utilicen con el objetivo inicial resulte necesaria para el interés legítimo de la salud pública, de la Ciencia Médica, del responsable del tratamiento médico o del fichero con el fin de permitirle ejercer o defender sus derechos judicialmente o con fines de antecedentes estadísticos, habrán de tomarse disposiciones técnicas para garantizar la conservación y seguridad correctas de los datos, teniendo en cuenta la vida privada del paciente.

10.3. A petición de la persona interesada, sus datos médicos deberían ser eliminados, a menos que se conviertan en anónimos o que intereses superiores o legítimos, en especial los enunciados en el principio 10.2, u obligaciones de archivo se opongan a ello.

11. Flujos transfronterizos

11.1. Los principios de la presente recomendación serán aplicables a los flujos transfronterizos de datos médicos.

11.2. Los flujos transfronterizos de datos médicos en dirección a un Estado que haya ratificado el Acuerdo para proteger a las personas en cuanto respecta al tratamiento automatizado de datos de carácter personal y que disponga de una legislación que garantice una protección de datos médicos al menos equivalente, no deberían estar sujetos a condiciones especiales de protección de la vida privada.

11.3. Cuando la protección de datos médicos pueda considerarse armónica con el principio de protección equivalente enunciado en dicho acuerdo, no debería existir límite para los flujos transfronterizos de datos médicos hacia un Estado que no haya ratificado el acuerdo pero que garantice una protección acorde con los principios de dicho acuerdo y de la presente recomendación.

11.4. A menos que la legislación interna lo establezca de otro modo, los flujos transfronterizos de datos médicos hacia un Estado que no garantice una protección acorde con dicho acuerdo y con la presente recomendación no deberían producirse por regla general, a menos que:

a. se hubieran tomado las medidas necesarias para respetar los principios del acuerdo y de la presente recomendación, incluidas las de naturaleza contractual, y que la persona interesada hubiera tenido la posibilidad de oponerse a la transferencia; o

b. la persona interesada hubiera dado su consentimiento.

11.5. Cuando los datos médicos se transfieran de un país a otro y salvo en caso de urgencia o transferencia aceptada por la persona interesada previa información, deberían tomarse las medidas apropiadas para garantizar su protección y en especial:

a. el responsable de la transferencia habría de indicar al destinatario las finalidades determinadas y legítimas para las cuales se recogen en principio los datos, así como las personas o entidades a las cuales puedan comunicarse;

b. salvo si la legislación interna lo establece de otra manera, el destinatario debería comprometerse con el responsable de la transferencia a respetar los fines determinados y legítimos reconocidos, así como a no poner los datos en conocimiento de personas o entidades distintas de las indicadas por el responsable de la transferencia.

12. Investigación científica

12.1. En la medida de lo posible, los datos médicos empleados con fines de investigación científica deberían ser anónimos. Las organizaciones profesionales y científicas, así como las autoridades públicas, deberían promover el desarrollo de técnicas o de procedimientos que garanticen el anonimato.

12.2. Sin embargo, si el anonimato convirtiera en imposible un proyecto de investigación científica y si este proyecto hubiera de llevarse a la práctica con un objetivo legítimo, la investigación podría realizarse con datos de carácter personal, con la condición de:

a. que la persona interesada dé su consentimiento previa información para la o las finalidades de investigación; o

b. que cuando la persona interesada sea legalmente incapaz o no se encuentre en condiciones de tomar determinaciones libremente, y cuando la legislación interna no le permita intervenir en su propio nombre, su representante legal, una autoridad o cualquier persona o instancia designada por la ley aporten su consentimiento en el marco de un proyecto de investigación vinculado a la condición médica o a una enfermedad de la persona interesada; o

c. que la comunicación de datos para fines de proyecto de investigación científica determinado por razones de interés público importantes haya sido autorizada por uno o varios organismos designados por la legislación interna, pero solamente:

i. si la persona interesada no se opone expresamente a la comunicación; y

ii. si se comprueba, pese a esfuerzos razonables, que no es factible establecer contacto con la persona interesada con miras a obtener su consentimiento; y

iii. si el interés del proyecto de investigación científica justifica esta autorización; o

d. que la investigación científica esté prevista en la ley y que represente una medida necesaria por motivos de salud pública.

12.3. A reserva de condiciones adicionales previstas por la legislación interna, los profesionales sanitarios facultados para llevar a cabo sus propias investigaciones médicas deberían poder hacer uso de los datos médicos en su poder siempre y cuando la persona interesada sea informada de tal facultad y siempre que no se oponga a ello.

12.4. Con respecto a cualquier investigación científica fundamentada en datos de carácter personal, los problemas consecuentes a incidentes originados por el respeto de las disposiciones del Acuerdo para proteger a las personas en cuanto respecta al tratamiento automatizado de datos de carácter personal, incluidos los de naturaleza ética y científica, deberían examinarse asimismo a la luz de otros instrumentos pertinentes.

12.5. Los datos de carácter personal empleados con fines de investigación científica no podrán publicarse en forma que permita identificar a las personas interesadas, a menos que estas últimas den su consentimiento con miras a la mencionada publicación y que la legislación interna lo autorice.

RECOMENDACIÓN Nº R (91) 15 DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS SOBRE COOPERACIÓN EUROPEA EN MATERIA DE ESTUDIOS EPIDEMIOLÓGICOS EN EL ÁMBITO DE LA SALUD MENTAL

(adoptada por el Comité de Ministros del 11 de octubre de 1991, durante la 463ª reunión de los Delegados de los Ministros)

El Comité de Ministros, en virtud del Artículo 15.b del Estatuto del Consejo de Europa,

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros y que esta meta puede alcanzarse, entre otros aspectos, mediante la adopción de un enfoque común en materia sanitaria y de protección social;

Una vez comprobado que los trastornos mentales constituyen un grave problema sanitario para las poblaciones de los Estados miembros, tanto en los planos humano como económico, tal como se deduce del informe "Futuro de la salud mental", establecido por la Conferencia de Ministros europeos responsables de Sanidad, celebrada en Estocolmo en 1985;

Consciente de que los trabajos de investigación en ciertos Estados miembros descubren la significativa importancia de necesidades pendientes de satisfacer en el ámbito de la salud mental;

Recordando la creciente demanda de cuidados sanitarios por trastornos mentales que afectan a un número cada vez mayor de personas de edad avanzada;

Habida cuenta de los importantes problemas de gestión y tratamiento relativos a enfermos mentales graves, tanto en el ámbito hospitalario como dentro de la colectividad;

Resaltando la existencia de importantes cambios en la organización de los cuidados y diferentes opiniones respecto a los enfoques que deben adoptarse;

Consciente de la primordial importancia que debe darse al análisis, control y evaluación de tales cambios;

Consciente de la necesidad, pese a determinados y prometedores avances científicos, de mejorar aún más la metodología actualmente vigente en el ámbito de la investigación epidemiológico-psiquiátrica;

Reconociendo que, pese a apreciables mejoras, la situación continúa siendo preocupante debido a la insuficiente comunicación entre los productores de datos de investigación (medios de investigación e institutos estadísticos gubernamentales) y los usuarios de estos datos (personas que toman decisiones profesionales sanitarios, medios de comunicación, público en general y los propios investigadores);

Convencido de la necesidad de mejorar los sistemas de información con el fin de que sean científicamente fiables y fácilmente utilizables por los llamados a tomar decisiones y profesionales sanitarios;

Atento al hecho de que el éxito de la investigación epidemiológica y de la evaluación dependen de la disponibilidad de los datos de carácter personal;

Consciente de que no siempre es posible para el individuo padecedor de trastornos mentales dar su consentimiento libre y fundamentado para la recogida de tales datos con fines de investigación;

Señalando, especialmente, la necesidad de encontrar otras salvaguardas apropiadas con el objeto de compensar esta incapacidad;

Resaltando igualmente, dentro de este contexto, lo dispuesto en el Artículo 6 del Acuerdo para proteger a las personas

en cuanto respecta al tratamiento automatizado de datos de carácter personal del 28 de enero de 1981, así como las disposiciones del apartado 3.4 del anexo a la Recomendación nº R (83) 10, relativa a protección de datos de carácter personal utilizados con finalidades de investigación científica y estadísticas.

Recomienda a los Gobiernos de los Estados miembros:

1. proceder de manera que los programas de actuación en materia de salud metal incluyan objetivos concretos y realistas para la investigación epidemiológica y de evaluación;

2. garantizar o incentivar una financiación adecuada para los estudios epidemiológicos en el ámbito de la salud mental;

3. promover:

- estudios sobre cuestiones jurídicas y éticas relativas a tratamientos psiquiátricos obligatorios y cuidados psiquiátricos voluntarios, que afecten en particular a la autonomía e integridad de los pacientes;

- uso de una investigación "longitudinal" sobre territorios determinados tomando en consideración que, en materia de salud mental, el estudio de los factores de riesgo, como también el efecto de los cuidados, requieren prolongados períodos de observación;

- estudios epidemiológicos relacionados con problemas de salud mental de personas de edad avanzada;

- evaluación de diferentes enfoques de cuidados destinados a disminuir la invalidez social y a mejorar la calidad de vida para los enfermos mentales gravemente afectados;

- estudios de relación coste-eficacia de diferentes maneras de concebir los cuidados, poniendo una especial atención en el papel del sector de cuidados sanitarios primarios en el contexto de los servicios de salud mental;

4. promover mejoras en los sistemas de información sanitaria de acuerdo con las recomendaciones de la Organización Mundial de la Salud, consistentes en:

- poner a punto y difundir métodos de medida e indicadores de resultados referidos a satisfacción del paciente, a la calidad de vida para sí mismo y su entorno y en cuanto al funcionamiento social, tomando en consideración la posibilidad de comparación cuando se empleen baremos de evaluación análogos y otros instrumentos de investigación;

- impulsar el establecimiento de una documentación común confeccionada por las comunidades investigadoras de los Estados miembros, así como la disposición de bases de datos ampliamente accesibles y que den cuenta de las investigaciones realizadas y en marcha;

- proseguir con la reflexión iniciada por los Estados miembros sobre protección de datos de carácter personal utilizados con fines de investigación, con miras a determinar si la particularidad de la enfermedad mental precisa normas éticas y garantías adicionales en lo referente a consentimiento de personas y confidencialidad de datos;

- poner a punto y reglamentar las técnicas de tratamiento de datos destinadas a garantizar la protección de las informaciones confidenciales, y todo ello permitiendo el constante desarrollo de investigaciones epidemiológicas y de evaluación;

- aportar al público información sobre los métodos y objetivos de investigación epidemiológica en sanidad mental, susceptible de desencadenar una actitud positiva ante este tipo de investigación, que despierte interés por sus resultados y disipe los temores referidos a un mal uso de las informaciones recopiladas;

- incentivar el mantenimiento y desarrollo de registros de casos psiquiátricos destinados a completar el sistema de datos estadísticos nacional;

5. promover cursos de formación en materia de metodología de la investigación epidemiológica, orientados sobre todo a estimular la coordinación entre países, así como alentar la inclusión de un módulo de investigación epidemiológico-psiquiátrica dentro de los cursos de formación sanitaria pública y epidemiológica, aparte de sensibilizar sobre epidemiología al conjunto de profesionales pertenecientes al ámbito de la sanidad mental.

MEMORIA DE 1997 - ANEXO III. INFORME DE ACTIVIDAD DE LA AUTORIDAD DE CONTROL COMÚN DEL CONVENIO DE SCHENGEN

PRÓLOGO

El periodo al que se refiere el 2º informe anual de la Autoridad de Control Común de Schengen (de marzo de 1997 a marzo de 1998) constituye un momento decisivo y de crucial importancia para la cooperación policial y para el Sistema de Información Schengen a nivel europeo: ampliación a nuevos países de las condiciones para el ejercicio de la libertad de circulación de los ciudadanos, refuerzo del sistema de seguridad y de información policial común e integración de Schengen en la Unión Europea.

1997 ha sido un año en que se ha reafirmado la independencia y se ha confirmado la importancia de la actividad de la Autoridad de Control Común (ACC) como instancia encargada de velar por los derechos y libertades de los ciudadanos, en particular en lo relativo a la protección de datos personales.

La ACC ha tratado temas fundamentales, contribuyendo positivamente a que el funcionamiento del Sistema de Información Schengen respete las normas y derechos previstos en el Convenio de Aplicación. De este modo, se ha realizado el análisis de las leyes de protección de datos de carácter personal de Italia y Grecia, se han emitido recomendaciones y dictámenes relativos a las condiciones de seguridad del tratamiento y transmisión de información personal, el tiempo de conservación de los datos, las descripciones de identidades usurpada o la transmisión de determinados datos a Interpol.

La ACC ha visto reconocida su importante labor por parte de las instancias ejecutivas de Schengen: se le ha garantizado un presupuesto mediante una línea presupuestaria autónoma; ha recibido con mayor regularidad la información indispensable para el ejercicio de sus cometidos; se le han solicitado dictámenes sobre diversos asuntos. Las sucesivas presidencias de Schengen (Portugal, Austria y Bélgica) han conferido una importancia cada vez mayor a la ACC.

Con vistas a cumplir nuestro plan de trabajo, deseamos dar este año un paso decisivo para la transparencia del funcionamiento del sistema y para la información de los ciudadanos. La ACC distribuyó su anterior informe anual en la conferencia de prensa de Lisboa, en abril de 1997, y lo transmitió a las instancias europeas y de Schengen; las comisiones nacionales lo presentaron a los respectivos Parlamentos, se han publicado varias ediciones del informe y figura en las páginas de Internet de varias Agencias de Protección de Datos. La ACC no ha dejado tampoco de alertar a las instancias competentes y a la opinión pública cuando ello ha sido necesario con respecto a problemas de seguridad ocurridos con motivo de una fuga de información de una de las Oficinas SIRENE. Al mismo tiempo, y en cooperación con las entidades nacionales competentes, la ACC decidió lanzar una campaña de información centrada en los derechos de los ciudadanos respecto del Sistema de Información Schengen.

En el marco de la evolución de los sistemas policiales de información europeos (Europol, Eurodac, Aduanero) y del refuerzo de las medidas de cooperación para luchar contra la delincuencia organizada, es importante perfeccionar los mecanismos de cooperación entre las Autoridades de Control Común encargadas en cada uno de estos sistemas de la protección de los valores fundamentales de las libertades y de los ciudadanos. La ACC procurará fomentar dicha colaboración, contando, como hasta ahora, con el apoyo vehemente de las agencias nacionales de protección de datos.

La integración de Schengen en la Unión Europea, prevista en el Tratado de Amsterdam, aportará un mayor valor a la transparencia de Schengen. El haber legislativo europeo se enriquecerá con los derechos de protección de datos de carácter personal que figuran en el Convenio de Schengen. El acervo de Schengen en la Unión Europea no dejará de incluir las recomendaciones más importantes de la ACC en este campo y el papel que se le reserve.

La ACC orientará sus trabajos y realizará los mayores esfuerzos con vistas a consolidar un espacio europeo común de libertad en seguridad.

26 de febrero de 1998

El Presidente

João Labescat

CAPÍTULO I. - INTRODUCCIÓN

En su primer informe de actividades, la Autoridad de Control Común recordaba las etapas recorridas por los cinco Estados signatarios del Acuerdo de Schengen desde 1985 hasta la firma del Convenio de Aplicación de dicho Acuerdo en 1990, y más tarde, en marzo de 1995, la puesta en aplicación de este instrumento. También exponía cómo durante este periodo se han sumado a los cinco Estados signatarios otros 10 Estados, deseosos a su vez de formar parte de este espacio de libre circulación de personas1.

La Autoridad de Control Común describía asimismo las medidas compensatorias previstas por el Convenio de Aplica-

ción del Acuerdo de Schengen para poder alcanzar su objetivo, a saber la supresión de los controles en las fronteras interiores de los Estados miembros, para crear de ese modo un gran espacio de libre circulación de personas, a la vez que se mantiene en el interior del mismo un nivel de seguridad al menos igual al que existía anteriormente. Más adelante se expone un breve resumen de dichas medidas.

Entre las medidas compensatorias de la supresión de los controles en las fronteras interiores que prevé el Convenio figuran la armonización de la política de expedición de visados, una política común con respecto a la 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 en las fronteras exteriores del territorio Schengen, así como un sistema informático Schengen (SIS).

Este sistema conecta al conjunto de los países que aplican el Convenio de Aplicación del Acuerdo de Schengen y permite a sus usuarios (servicios encargados de misiones policiales, embajadas y consulados, etc...) disponer inmediatamente de información útil para sus cometidos, introducida por cualquier Estado miembro que aplique el Convenio.

Se trata de información relativa a personas (buscadas para su detención con vistas a su extradición, no admitidas, desaparecidas, que deben ser objeto de vigilancia discreta,...) y a objetos (vehículos, armas, documentos, billetes de banco robados, sustraídos u ocultados).

La creación de un instrumento de este tipo ha ido acompañada por la de una Autoridad de Control Común para la protección de datos de carácter personal (ACC), encargada especialmente de velar por que se cumplan las disposiciones del Convenio con respecto a la unidad de apoyo técnico del SIS (artículo 115). A la ACC, compuesta por dos representantes de cada una de las autoridades de control de las Partes contratantes, se ha asignado asimismo una función de asesoramiento y armonización de las prácticas o de las doctrinas nacionales.

La ACC ha tenido que hacer grandes esfuerzos desde la puesta en aplicación del Convenio de Schengen para ver reconocidas sus competencias y su independencia frente a las instancias ejecutivas de Schengen.

Su primer informe de actividades así lo ha mostrado, en especial subrayando tanto las dificultades para obtener un presupuesto autónomo como las halladas por el grupo de expertos designados por la ACC para el control de la parte central del SIS (C.SIS) instalada en Estrasburgo.

En el momento de la aprobación del presente informe, más de un año después de haberse efectuado el control del C. SIS, la ACC sigue sin recibir respuesta alguna de las instancias ejecutivas de Schengen a las recomendaciones formuladas a raíz de dicho control, habiendo recibido únicamente la del Ministerio del Interior francés. Por lo que se refiere a las informaciones relativas al C.SIS, necesarias para el ejercicio de sus misiones, la ACC no ha recibido una parte de las mismas hasta febrero de 1998.

A pesar de los avances que se han producido, queda aún mucho por hacer. La visita de control de la ACC al C.SIS en 1996 ha mostrado el buen funcionamiento general del sistema, pero ha puesto de relieve diversos problemas, algunos de los cuales plantean verdaderas dificultades en términos de integridad.

Los problemas señalados por la ACC adquieren un significado muy particular a la vista del reciente aumento del número de Estados Schengen que aplican el Convenio, que a finales de 1997 han pasado de 7 a 10. En consecuencia, la cantidad de datos introducidos en el SIS también aumenta.

Los sistemas policiales de información evolucionan, y también el de Schengen. Dicha evolución debe ir acompañada por un aumento de las funciones de las autoridades de control independientes implicadas.

La integración de Schengen en la Unión Europea, prevista en el artículo 7 del protocolo del Tratado de Amsterdam por el que se integra el acervo de Schengen, representa mayor transparencia y mayores garantías para los derechos fundamentales de los ciudadanos. Los Parlamentos nacionales y las instancias europeas tomarán parte activa en la consecución de estos objetivos.

CAPÍTULO II: LA AUTORIDAD DE CONTROL COMÚN Y SUS COMETIDOS

Si bien el principal cometido de la ACC consiste en controlar la unidad de apoyo técnico del SIS, cometido éste que sólo la ACC está autorizada a cumplir (artículo 115.2), también tiene asignada una función de asesoramiento y armonización de las prácticas o las doctrinas nacionales.

El Convenio de Aplicación del Acuerdo de Schengen establece las funciones de la ACC con respecto al SIS en los siguientes artículos:

Artículo 106.3:

La ACC emitirá un dictamen en caso de desacuerdo entre dos Partes contratantes sobre la existencia de un error de hecho o de derecho en una descripción. En esta situación, la Parte contratante que no hubiera dado origen a la descripción estará obligada a someter el caso para dictamen a la ACC;

Artículo 115.3:

La ACC analizará las dificultades de aplicación o de interpretación que pudieran surgir con motivo de la explotación del SIS.

La ACC estudiará los problemas que se planteen durante el ejercicio de control independiente efectuado por las autoridades nacionales de control de las Partes contratantes.

La ACC estudiará los problemas que se planteen durante el ejercicio del derecho de acceso al sistema.

De manera más general, la ACC elaborará propuestas armonizadas con vistas a encontrar soluciones para los problemas existentes.

Artículo 115.4:

La ACC elaborará informes que remitirá a los organismos a los cuales las autoridades de control nacionales remiten sus informes.

Artículo 118.2:

La ACC recibirá comunicación de las medidas especiales adoptadas por cada Parte contratante con objeto de garantizar la protección de los datos durante la transmisión de datos a servicios situados fuera del territorio de las Partes contratantes.

Por lo que respecta a los intercambios de información fuera del SIS:

Artículo 126.3 f):

La ACC podrá, a instancias de una de las Partes contratantes, emitir un dictamen sobre las dificultades de aplicación y de interpretación del artículo 126, relativo al tratamiento de los datos transmitidos, fuera del SIS, en aplicación del Convenio.

Artículo 127.1:

La ACC podrá, en las condiciones y según las modalidades previstas en el artículo 126, emitir un dictamen en caso de transmisión de datos procedentes de un fichero no automatizado y de introducción de datos en un fichero de este tipo.

CAPÍTULO III : LAS ACTIVIDADES DE LA ACC DE MARZO 1997 A MARZO 1998

Entre marzo de 1997 y marzo de 1998, el pleno de la ACC se ha reunido en 10 ocasiones. Dichas reuniones se han celebrado en Bruselas, excepto la sesión anual celebrada por la ACC en Lisboa en abril de 1997, en la que participó el representante del Presidente del Comité Ejecutivo.

Además de estos plenos, la ACC ha mantenido cinco reuniones restringidas para preparar proyectos de "Dictamen" sobre problemas particulares, elaborar su informe anual y examinar las futuras modalidades del control del C.SIS.

Además, varios de los miembros de la ACC se han encontrado en tres ocasiones con representantes del Ministerio del Interior francés en su condición de responsable de la unidad de apoyo técnico del C.SIS.

Con motivo de uno de dichos encuentros estuvo presente la Troica de Schengen, en especial para hacer un balance del seguimiento de las recomendaciones emitidas por la ACC tras el control del C.SIS.

Ha de señalarse que a partir de la reunión de la ACC del 7 de marzo de 1997, de conformidad con la decisión adoptada por esta Autoridad en su reunión de los días 10 y 11 de febrero de 1997 en Estrasburgo, toman parte en las reuniones de la ACC como observadores Suecia, Dinamarca, Finlandia, Noruega e Islandia.

Durante estas reuniones se examinaron los siguientes asuntos:

1. FUNCIONAMIENTO DE LA ACC.

Composición de la ACC.

La ACC ha tomado nota de las leyes italiana y griega que regulan la protección de datos de carácter personal. Esta es una de las condiciones previas para la carga de datos de carácter personal en el SIS (art. 117) y por ende para la puesta en aplicación del Convenio en el territorio de los Estados miembros.

La ACC ha modificado su reglamento interior2 para poder atribuir el estatuto de miembros de la ACC a los representantes de las autoridades nacionales de control de los Estados que se han adherido al Convenio desde el momento en que, una vez cumplidas todas las demás condiciones, el Convenio se pone en aplicación en su territorio. En base a este criterio, en la reunión del 12 de diciembre de 1997 se constató que los representantes de las autoridades de

control de Italia, Austria y Grecia participarían en adelante en las reuniones de la ACC en calidad de miembros de la misma.

Elecciones del Presidente y del Vicepresidente.

La ACC ha elegido Presidente al Sr. J. Labescat (Portugal) el 12 de diciembre de 1997, y el 3 de febrero de 1998 ha elegido Vicepresidente al Sr. B. De Schutter (Bélgica).

Presupuesto autónomo de la ACC.

Las autoridades Schengen, tras largos debates de principio, han aprobado el presupuesto de la ACC para el año 1997.

La versión aprobada por el Comité Ejecutivo el 25 de abril de 1997 se modificó más tarde a la vista del aumento del número de países representados en sus reuniones. El presupuesto conferido a la ACC para 1997 ascendía a 2.839.950 BEF. El 12 de diciembre de 1997, la ACC ha procedido al cierre de cuentas de su presupuesto para 1997.

Las cuentas han mostrado un saldo de 992.179 BEF con respecto al presupuesto de 2.839.950 BEF que se le había acordado. El presupuesto se ha destinado a la realización del folleto sobre el derecho de acceso, la redacción, traducción e impresión del primer informe de actividades, la organización de la sesión anual de la ACC en Lisboa y la compra de equipamiento diverso.

El Grupo Central ha aprobado el 23 de febrero de 1998 el presupuesto para 1998, basado en los gastos del año anterior y en el programa de actividades de la ACC para el año 1998. Dicho presupuesto asciene a 3.239.950 BEF.

Secretaría de la ACC.

En varias ocasiones, la ACC ha solicitado un refuerzo de los medios logísticos a su disposición y una prioridad en las traducciones con respecto a los grupos de trabajo. Ha solicitado asimismo que se examine la posibilidad de disponer de una secretaría autónoma.

En efecto, con demasiada frecuencia la cantidad creciente de reuniones de los grupos de trabajo Schengen perjudica la preparación de sus propias reuniones. Por otra parte, la ACC ha constatado que el personal de la Secretaría General tenía como misión prioritaria la preparación de reuniones como las del Grupo Central o el Comité Ejecutivo.

Este problema se ha resuelto parcialmente atribuyendo un presupuesto a la ACC, que cubre sobre todo los gastos de traducción de su informe anual. El 23 de febrero de 1998, el Grupo Central ha expresado su acuerdo con el refuerzo del apoyo administrativo a su disposición.

La ACC se congratula de ello, pues considera que sólo podrá hacer frente a su aumento de trabajo con ayuda de una secretaría permanente, o al meno orientada prioritariamente hacia sus trabajos.

Considera asimismo que la secretaría actual, que se ha ocupado de sus actividades desde la redacción del Convenio, es la más apta para facilitarle dicho apoyo.

2 LOS ASUNTOS TRATADOS POR LA ACC.

Dictámenes de la ACC.

La ACC ha emitido diversos dictámenes, que se incluyen más adelante en el capítulo IV.

Control del C.SIS.

Se ha aprobado la versión definitiva del informe técnico confidencial sobre el control del C.SIS, efectuado en octubre de 1996, incluyendo las observaciones del Ministerio del Interior francés.

En diciembre de 1996 se transmitió al Presidente del Grupo Central una versión provisional de dicho informe, mientras que la versión definitiva se ha remitido el 22 de abril de 1997 a los Presidentes del Comité Ejecutivo y del Grupo Central para su difusión a los grupos técnicos competentes, a los que se ha encargado que verifiquen en qué medida pueden seguirse las recomendaciones emitidas por la ACC para hacer más seguro el sistema.

Casi dos años después de haberse realizado el control, las instancias oficiales de Schengen siguen sin comunicar a la ACC qué seguimiento tienen previsto dar a dichas recomendaciones.

Modalidades de los controles del C.SIS por parte de la ACC.

Durante todo el año se ha venido examinando el protocolo mencionado anteriormente por el que se especifican las modalidades según las cuales se realizarían en el futuro los controles del C.SIS.

Puesto que la mayoría de los miembros de la ACC han considerado en su reunión del 12 de diciembre de 1997 que no se tenía en cuenta el carácter independiente de su institución en el proyecto resultante de los diversos encuentros entre

representantes del Ministerio del Interior francés y de la ACC, se ha decidido que una comisión restringida prosiga el examen de esta delicada cuestión para proponer un nuevo proyecto que concilie las exigencias de seguridad planteadas por el Ministerio del Interior francés y la necesidad de que la ACC pueda ejercer sus controles con total independencia.

Un grupo restringido de miembros de la ACC ha elaborado el 2 de febrero de 1998 un nuevo proyecto para ser aprobado en el pleno del grupo del 6 de marzo de 1998. Este proyecto servirá de nueva base para los debates con los responsables implicados.

Seguridad de la oficinas SIRENE.

A raíz del descubrimiento de un tráfico de información confidencial procedente del SIS, en concreto de la Oficina SIRENE belga3 , la ACC, informada directamente de este hecho, aprobó un comunicado de prensa en su reunión del 12 de diciembre de 1997.

Dicho comunicado se dio a conocer ese mismo día a las agencias de prensa, y se remitió el 15 de diciembre de 1997 a los representantes del Comité Ejecutivo.

En su comunicado, la ACC señalaba su gran inquietud ante un acontecimiento que ponía de relieve de modo dramático la necesidad de mejorar continuamente las medidas de seguridad en el marco del SIS y del intercambio de información Schengen

La ACC ha solicitado de inmediato a las autoridades de control nacionales :

* que le informasen sobre la situación en materia de seguridad en sus SIS y sus oficinas SIRENE;
* que determinaran, en base a dichos informes, las medidas que deberían adoptarse para mejorar la seguridad;
* que evaluaran la necesidad de elaborar un informe anual sobre la situación en materia de seguridad;
* que volvieran a examinar este tema en su próxima reunión.

La ACC subrayó asimismo la importancia de que se le mantuviera en todo momento informada de las medidas de seguridad adoptadas por las instancias Schengen y las autoridades nacionales con objeto de garantizar la confidencialidad del Sistema de Información Schengen.

Desde esa fecha, varias autoridades de control nacionales han procedido a realizar verificaciones. Se están examinando los primeros informes nacionales.

Informe de actividades.

La ACC elaboró su primer informe de actividades: el 7 de marzo de 1997, los miembros examinaban un primer proyecto, aprobándose el 27 de marzo de 1997. El 3 de febrero de 1998 se ha aprobado la estructura del segundo informe de actividades de la ACC.

Un grupo restringido de redacción ha debatido un proyecto de texto el 25 de febrero de 1998, examinado por el conjunto de los miembros de la ACC en su reunión del 6 de marzo de 1998. Dicho proyecto se ha aprobado a continuación al término del procedimiento escrito.

Los días 22 y 23 de abril de 1997 se organizó en Lisboa una sesión anual de la ACC. En ella se presentó el informe de actividades de la ACC al representante del Grupo Central y a los periodistas que asistieron a la conferencia de prensa.

La conferencia de prensa contó con la presencia de diversos periodistas portugueses - televisión, radios, diarios de mayor difusión y la agencia de noticias portuguesa - y de algunos periodistas extranjeros, en particular de la Agencia EFE (España) y de la Agencia Reuters (G.B.). Además, la cobertura periodística de la reunión de la ACC y de la presentación del informe fue más amplia, con referencias en otras publicaciones.

Los asuntos a los que más atención prestaron los medios de comunicación fueron la definición de competencias de la ACC, su papel en el seno de las instancias Schengen, el funcionamiento del SIS en cuanto a tipos de datos contenidos y formas de acceso, así como datos generales sobre el Convenio de Aplicación del Acuerdo de Schengen.

Las autoridades de control nacionales han difundido este informe del mismo modo que lo hacen con sus informes nacionales, y en especial algunas de ellas lo han hecho a través de Internet. En algunos países se han celebrado conferencias de prensa para presentar el documento y dar a conocer mejor la ACC al conjunto de los ciudadanos.

Información de los ciudadanos.

Para cumplir su cometido de información en relación con los ciudadanos, la ACC decidió publicar un folleto explicativo destinado al público en general sobre los derechos de aquéllos ciudadanos descritos en el SIS. El 12 de diciembre de 1997, la ACC ha aprobado la versión definitiva del texto explicativo sobre el derecho de acceso de los ciudadanos a la información del SIS que les concierne, y ha seleccionado uno de los proyectos presentados por las empresas de comunicación convocadas.

Este texto, que se adjunta en anexo al presente informe, se difundirá en forma de folleto en los puntos de cruce autori-

zados de las fronteras exteriores de Schengen. Se informará al público de la existencia de dichos folletos por medio de carteles. La eficacia de esta iniciativa dependerá en gran medida de la difusión que se dé a estos documentos.

De este modo, la ACC espera el apoyo en este proyecto de las autoridades nacionales de control, las instancias Schengen y las autoridades competentes de los Estados.

Información a la ACC.

En abril de 1997, a petición de la ACC, el Grupo Central solicitó al C.SIS y a la Unidad de Gestión que pusieran a disposición de la ACC sus informes mensuales.

La ACC consideraba en efecto que necesitaba disponer de estos documentos para garantizar el cumplimiento de las normas de protección de datos de carácter personal. El Presidente del Grupo Central remitió una carta el 7 de mayo de 1997 al Presidente del Grupo de Trabajo Permanente y al jefe de la Delegación francesa, responsable del C.SIS, solicitándoles que llevasen a la práctica la decisión del Grupo Central. Los informes del C.SIS se han remitido a partir de entonces a la ACC con regularidad, mientras que los de la Unidad de Gestión sólo se le han transmitido a partir del 6 de marzo de 1998.

Relaciones entre la ACC y las instancias Schengen.

El 16 de junio de 1997 se celebró en Bruselas una reunión entre representantes de la ACC, del Grupo Central y del Ministerio del Interior francés, éste último como responsable del apoyo técnico C.SIS.

De este modo se informó a los representantes de la ACC de la situación en que se hallaban los trabajos relativos a la carga de datos reales en el SIS para Italia, Grecia y Austria. Se facilitaron asimismo detalles sobre la capacidad del SIS para acoger a estos tres nuevos países.

Se abordó también la cuestión de las consecuencias que se desprenderían del informe confidencial sobre el control del C.SIS, y los participantes aprobaron la propuesta del Ministerio del Interior francés de preparar, de común acuerdo con representantes de la ACC, un protocolo por el que se definieran las modalidades de los futuros controles de la ACC al C.SIS.

Se especificaron las modalidades de utilización del presupuesto de la ACC y se presentó oficialmente el dictamen de la ACC 97/1 relativo a la duplicación de una parte de las descripciones del SIS.

Se aceptó el principio de los encuentros periódicos entre representantes de la ACC y del Grupo Central, eventualmente, al margen de sus reuniones. Estas han dado paso a una mejor información entre estas autoridades.

De este modo, el 4 de marzo de 1998, invitada por la Presidencia belga, una delegación de la ACC ha participado por primera vez en una reunión del Grupo Central, precedida por una visita al C.SIS.

Este encuentro ha permitido un intercambio de información: la ACC ha presentado su programa de trabajo y ha recordado los cometidos que le encomienda el Convenio, a la vez que se le han proporcionado explicaciones técnicas sobre el desarrollo del SIS.

La ACC y el Grupo Central han acordado que en el futuro se informarán más y cooperarán más estrechamente. La ACC tendrá así la posibilidad de seguir algunas fases de los trabajos relativos al SIS, y podrá de ese modo asegurarse de que se tengan en cuenta sus recomendaciones, en especial sobre la seguridad del sistema.

CAPÍTULO IV : LOS DICTÁMENES EMITIDOS POR LA AUTORIDAD DE CONTROL COMÚN

Al ser examinados por la ACC, varios dictámenes han requerido complementos de información. Por este motivo, algunos dictámenes mencionados a continuación figuraban ya entre los trabajos en curso en el primer informe de actividades. Por otra parte, los dos primeros dictámenes que se exponen más adelante, aprobados en marzo de 1997, constaban asimismo en el anterior informe de actividades. A continuación se resumen dichos dictámenes, que se adjuntan completos en anexo.

1. Dictamen de 7 de marzo de 1997 relativo al proyecto piloto del Grupo de trabajo I "Policía y Seguridad" relativo a vehículos robados (SCH/Aut-cont (97) 22 rev.).

El Grupo Central transmitió a la ACC el 10 de febrero de 1997 una solicitud de dictamen procedente del Grupo de trabajo I "Policía y Seguridad", en relación con la participación de países no integrados en el SIS en un proyecto piloto en materia de robo de vehículos.

Tras haber constatado que en dicho proyecto se permitía el acceso de países no integrados en el SIS a consultar éste sistema por medio de sus funcionarios de enlace, la ACC solicitó información complementaria sobre el carácter de la información intercambiada y su modo de transmisión.

Una vez proporcionada dicha información, la ACC recordó en un dictamen emitido el 7 de marzo de 1997 que:

* la información relativa a la marca, tipo, color y características técnicas de un vehículo no constituyen de por sí datos de carácter personal, siempre y cuando dicha información no esté asociada a la matrícula, propietario o conductor del vehículo

* el intercambio de información policial sobre la base de los ficheros nacionales entre las Partes contratantes integradas en el SIS y otros Estados en los que aún no se aplica el Convenio de Schengen está regulado, a través de los mecanismos de cooperación bilateral o multilateral, por las legislaciones en materia de protección de datos y por el control de las respectivas autoridades nacionales.

Por lo que se refiere a la información directa o indirectamente nominativa registrada en el SIS, la ACC ha considerado que las autoridades de las Partes contratantes en cuyo territorio aún no se aplique el Convenio no tienen acceso ni pueden consultar directamente dichos datos, de conformidad con los artículos 101 y 126.1 del Convenio de Schengen.

Este dictamen se transmitió al Grupo de trabajo I, que lo ha tenido en cuenta a la hora de realizar su proyecto. Otros proyectos piloto deberán asimismo tener en cuenta este dictamen, como el que está preparándose sobre los estupefacientes.

2. Dictamen de 7 de marzo de 1997 relativo al proyecto de convenio de cooperación en materia de tramitación de expedientes por infracciones de tráfico y ejecución de las sanciones pecuniarias impuestas (SCH/Aut-cont (97) 19 rev.).

El 10 de febrero de 1997, el Grupo Central transmitió a la ACC una solicitud de dictamen procedente del Grupo de trabajo III "Cooperación judicial", en relación con un proyecto de convenio sobre las infracciones de tráfico.

El texto prevé por una parte el acceso a la información y a los datos que figuran en los registros de matriculación de las Partes contratantes, y por otro lado un sistema de notificación directa y de cooperación, así como la ejecución efectiva por cada Estado Parte de las decisiones que emanen de una autoridad de otra Parte contratante, a reserva de determinados casos en que se limita o excluye la aplicación de una sanción pecuniaria.

Este proyecto se basa en la declaración común de los Ministros y Secretarios de Estado de 19 de junio de 1990, según la cual las Partes contratantes se comprometen a iniciar o proseguir debates en diversos ámbitos, uno de los cuales es la persecución de las infracciones de tráfico y la ejecución recíproca de las multas.

Este proyecto constituye un instrumento jurídico internacional diferente pero complementario del Convenio de Schengen, y se hace referencia a su Título VI relativo a las normas sobre protección de datos aplicables en caso de transmisión de información no inscrita en el SIS.

Tras haber examinado las disposiciones sobre protección de datos previstas en el proyecto de convenio, la ACC emitió un dictamen el 27 de marzo de 1997 en el que solicitaba que se integrasen o explicitasen los siguientes principios:

* el derecho de toda persona a exigir la rectificación o supresión de los datos que contengan errores de hecho o de derecho que se refieran a ella.

* el principio de la cooperación entre las autoridades nacionales de control mencionadas en el artículo 128.1, con vistas a garantizar los derechos de acceso, rectificación o supresión.

* la competencia de la ACC para emitir dictámenes sobre los aspectos comunes en materia de protección de datos de carácter personal que resulten de la aplicación del mencionado convenio.

Este dictamen se transmitió al Grupo de trabajo III, que ha adaptado en consecuencia su proyecto de dictamen.

3. Dictamen 97/1, de 22 de mayo de 1997, relativo a la duplicación de una parte de las descripciones del SIS (SCH/Aut-cont (97) 38 rev.).

El artículo 102.2 estipula que los datos integrados en el SIS sólo podrán ser duplicados con fines técnicos, siempre que dicha duplicación sea necesaria para la consulta directa por las autoridades nacionales habilitadas.

A la vista de este artículo, la ACC inició, a petición de la Commission de la vie privée de Bélgica, un debate sobre la interpretación del concepto de duplicación de datos con fines técnicos y sobre el de consulta directa, en particular en relación con el modo de consulta automatizada contemplado en el artículo 92. La ACC evaluó asimismo las consecuencias de la duplicación en CD-Rom de todo un N.SIS o parte del mismo, es especial con fines de consulta por misiones diplomáticas y consulares.

El examen de las condiciones de aplicación del artículo 102.2 ha suscitado cuestiones relativas a la actualización de la información duplicada y a la seguridad de las transmisiones efectuadas a servicios situados fuera del territorio de las Partes contratantes.

Así pues, la ACC propuso una solución armonizada compatible con las disposiciones sobre protección de datos establecidas por el Convenio.

En su dictamen 97/1, la ACC recuerda que, sean cuales sean los medios adoptados por los Estados miembros para organizar la consulta de las descripciones a efectos del artículo 96 del Convenio por parte de sus representaciones diplomáticas y consulares, deben respetarse los principios que se exponen a continuación:

* Las técnicas y medios de duplicación deberán garantizar la identidad de los datos en tiempo real en relación con el tratamiento central SIS.

* Dicha técnicas y medios de duplicación deberán garantizar los niveles mínimos de protección exigidos en el artículo 118.1 del Convenio, y en concreto en las letras b), d) y f) de dicho artículo, así como ser conformes a lo dispuesto en el artículo 118.3 del Convenio.

* El programa que permita su utilización deberá permitir un registro que responda a lo dispuesto en el artículo 103 del Convenio.

Dichos registros deberán enviarse de vuelta al país de origen cada seis meses, y la instancia contemplada en el artículo 108.2 del Convenio con competencia central para la parte nacional del SIS deberá mantenerlos a disposición de la autoridad de control nacional contemplada en el artículo 114 del Convenio.

En caso de que se utilicen medios de duplicación que presenten riesgo de falta de identidad de los datos, la ACC recomienda encarecidamente que, tal y como está previsto en los artículo 92.2 y 116 del Convenio, la Parte contratante responsable :

* se comprometa, en caso de descripción del individuo en el soporte de duplicación utilizado, a hacer una verificación en tiempo real (red, teléfono, fax) para asegurarse de la confirmación de esta información;

* se comprometa, en caso de no descripción del individuo en el soporte de duplicación utilizado, a aceptar su responsabilidad si se produce la descripción de este mismo individuo en el espacio de tiempo que exista entre la fijación de los datos sobre el duplicador y el tiempo real. Sólo podrá quedar exenta de esta responsabilidad mediante prueba de una verificación en tiempo real en el momento de la solicitud de visado.

En el examen de esta cuestión, la ACC ha constatado que, contrariamente a lo dispuesto en el artículo 118.2, no ha recibido comunicación de las medidas particulares adoptadas por cada Parte contratante para garantizar la seguridad de los datos en su transmisión a servicios situados fuera de su territorio.

Por ello, el 6 de diciembre de 1996 la ACC solicitó al Grupo Central que le precisara cómo aplicaban los Estados miembros el artículo 118.2 del Convenio. En el momento de la redacción del presente informe, la ACC sigue a la espera de esta información, a partir de la cual verificará si las medidas aplicadas respetan la interpretación que ella ha realizado del Convenio.

4. Dictamen 98/1, de 3 de febrero de 1998, relativo a la conservación de expedientes tras la supresión de una descripción (SCH/Aut-cont (97) 55, 2ª rev.).

Se ha llamado la atención de la ACC sobre las dificultades que suscita, a la vista del artículo 102.1, la conservación de expedientes relativos a descripciones tras la supresión de éstas.

En efecto, el artículo 102.1 prohibe que las Partes contratantes utilicen los datos previstos en los artículos 95 a 100 para otros fines distintos de los enunciados para cada una de las descripciones contempladas en estos artículos.

Ahora bien, los servicios de policía nacionales de determinadas Partes Contratantes conservan expedientes relativos a descripciones del artículo 95 y ss. del Convenio, incluso tras su supresión, convirtiéndolos en expedientes penales.

Las autoridades policiales implicadas se basan para ello en las disposiciones de sus leyes nacionales (véase el punto 2.1.3. b) del Manual SIRENE) y en las disposiciones del Título VI del Convenio de Schengen.

La ACC ha considerado que se trataba de una cuestión muy importante respecto al principio de finalidad de los datos. En su dictamen de 3 de febrero de 1998, la ACC recuerda los principios y derechos fundamentales en la materia, en especial los principios siguientes :

a. Los datos del SIS sólo se podrán suministrar y utilizar para los fines enunciados en relación con cada una de las descripciones (art. 102.1 y art. 94.1). Cualquier excepción a este principio general deberá justificarse por la necesidad de prevenir una amenaza grave inminente para el orden y la seguridad públicos, por razones graves de seguridad del Estado o con vistas a prevenir un hecho delictivo grave (art. 102.3).

b. Toda utilización de los datos que no sea conforme con los apartados 1 a 4 del artículo 102 se considerará como una desviación de la finalidad (art. 102.5).

c. Los datos de carácter personal introducidos en el Sistema de Información Schengen a efectos de búsqueda de

personas sólo se conservarán, de conformidad con el art. 112 del Convenio, durante el tiempo necesario para los fines para los que se hubieren facilitado dichos datos.

d. En el marco de la interpretación complementaria del Convenio, estos principios son válidos para cualquier tipo de tratamiento de la información que esté relacionado con descripciones del Sistema de Información Schengen o se refiera a las mismas.

Por ello, la Autoridad de Control Común ha considerado que se debían adoptar las siguientes medidas :

a. en caso de supresión de una descripción a efectos de búsqueda de personas, cada Parte contratante Schengen, de conformidad con el artículo 112 del Convenio, deberá borrarla y destruir inmediatamente todos los expedientes relativos a la misma;

b. las instancias Schengen deberán proceder a una revisión del Manual SIRENE con el objeto de suprimir lo dispuesto en la letra b) del apartado 2.1.3, contrario al Convenio de Schengen.

5. Dictamen 98/2, de 3 de febrero de 1998, relativo a la usurpación de identidad y sus consecuencias a nivel del SIS para el titular legítimo de la identidad usurpada (SCH/Aut-cont (97) 42, 2ª rev.).

En caso de usurpación de identidad, en algunos países también se introduce en el SIS al autor de dicha usurpación con el nombre de la persona cuya identidad ha sido usurpada.

En otras palabras, el sistema contiene una descripción con una identidad que no corresponde ni de hecho ni de derecho a la identidad real de la persona buscada. La persona cuya identidad ha sido usurpada se halla de este modo descrita en el SIS sin haber sido informada de ello previamente.

Varios Estados subrayaron que en ese caso hace falta proceder de inmediato a la supresión de los datos relativos a la persona cuya identidad ha sido usurpada. Otros Estados consideraron que la descripción usurpada debía mantenerse aunque la persona cuya identidad se hubiera inscrito indebidamente en el SIS solicitara la supresión de dichos datos.

El argumento invocado a favor del mantenimiento de la descripción era la necesidad de buscar al impostor.

La ACC ha examinado los problemas planteados por la utilización indebida de alias de personas descritas en el SIS, a la luz de los principios sobre protección de datos de carácter personal previstos por el Convenio de Schengen. La ACC ha reafirmado los principios y los derechos fundamentales en materia de protección de datos, y en especial los siguientes:

a. Los datos sólo se podrán proporcionar y utilizar para los fines enunciados en relación con cada una de las descripciones (art. 102.1 y art. 94.1), principio que únicamente puede ser soslayado por la necesidad de prevenir una amenaza grave o un hecho delictivo grave (art. 102.3).

b Toda utilización de datos que no sea conforme con los apartados 1 a 4 del artículo 102 se considerará como una desviación de la finalidad (artículo 102.5).

c. El derecho de toda persona a exigir la rectificación o supresión de los datos que contengan errores de hecho o de derecho que se refieran a ella (artículo 110).

d. El derecho de toda persona a entablar una acción ante el órgano jurisdiccional o la autoridad competente en virtud del Derecho nacional, con vistas a garantizar el derecho de rectificación o supresión (artículo 111.1).

e. El derecho de toda persona a solicitar la verificación de los datos, en estrecha coordinación con la autoridad nacional de control (artículo 114.2).

La ACC, teniendo en cuenta de forma proporcionada y equilibrada los derechos de la persona cuya identidad ha sido usurpada, previstos por el Convenio de Schengen, así como la necesidad de detectar al impostor, ha emitido el siguiente dictamen:

1. Se aplicará el Derecho nacional al registro en el SIS de datos de una persona cuya identidad haya sido usurpada, sin perjuicio de las normas más exigentes previstas en el Convenio de Schengen (artículo 104.1).

2. A la Parte Contratante autora de la descripción corresponderá garantizar que los datos sean registrados solamente para los fines enunciados, manteniéndolos actuales y exactos (artículos 102.1, 106.1, 110, disposiciones sobre protección de datos del Convenio 108 del Consejo de Europa vinculante para los Estados Schengen, en particular las contempladas en su artículo 5).

3. A la Parte Contratante autora de la descripción corresponderá garantizar el ejercicio del derecho de rectificación o supresión de los datos registrados, a tenor de lo dispuesto en el artículo 106 del Convenio y con arreglo al procedimiento en él previsto.

4. El mantenimiento en el SIS de la descripción de personas cuya identidad haya sido usurpada deberá evaluarse según el principio de la proporcionalidad, teniendo en cuenta, por una parte, los derechos de la persona cuya identidad haya sido usurpada, y por otra, la necesidad de detectar al impostor.

5. A la espera de la entrada en funcionamiento del SIS II, será necesario estudiar y adoptar una solución adecuada, y a ser posible común, que permita indicar que se trata de una descripción de una identidad usurpada. La ACC manifiesta su voluntad de cooperar para hallar dicha solución.

6. Dictamen 98/3, relativo a la transmisión de datos del SIS sobre vehículos robados al banco de datos de Interpol "ASF4 - Vehículos robados" (SCH/Aut-cont (97) 50, 2ª rev.).

El proyecto en cuestión, presentado en una nota del Comité de Orientación SIS, contempla la transmisión a un banco de datos de Interpol de datos del SIS relativos a personas y a vehículos robados, y posteriormente los relativos a otras categorías de datos.

La ACC ha recordado varios principios del Convenio, así como su dictamen relativo al proyecto piloto Schengen sobre vehículos robados, y en referencia únicamente a los aspectos relacionados con la protección de datos de carácter personal, ha emitido el siguiente dictamen:

1. La información y datos de carácter personal registrados en el Sistema de Información Schengen no pueden transmitirse a Interpol en el marco del proyecto "ASF - vehículos robados" sin infringir las disposiciones del Convenio, en particular los artículos 101, 102, 118 y 126.

2. Los datos relativos a la marca, tipo, color y características técnicas de los vehículos no son datos de carácter personal en el sentido del Convenio.

3. La comunicación de datos no personales a Interpol en el marco del proyecto "ASF - vehículos robados" no infringe las disposiciones del Convenio en materia de protección de datos, siempre y cuando no exista ninguna relación posible con un dato que permita la identificación de una persona en relación con dicho vehículo.

4. El intercambio de información en el marco de la cooperación policial y a partir de los ficheros nacionales está regulado por la legislación nacional en cuestión, y en particular por la ley en materia de protección de datos.

7. Dictamen 98/4, de 3 de febrero de 1998, relativo a la interpretación del artículo 103 sobre el control de la admisibilidad de la consulta al SIS (SCH/Aut-cont (97) 70 rev.).

Se ha llamado la atención de la ACC sobre las dificultades surgidas para la aplicación del artículo 103 del Convenio, relativo al registro en cada N.SIS por parte de la autoridad gestora del fichero de una décima parte de las transmisiones de datos de carácter personal a efectos de control de la admisibilidad de la consulta.

Consciente de que el Sistema de Información Schengen (SIS) es un sistema de búsqueda automático que requiere una protección eficaz contra el acceso no autorizado de terceros, la ACC ha considerado que el registro de un promedio representativo de las consultas al sistema es un medio adecuado de lucha contra el acceso no autorizado de terceros.

La ACC ha realizado un estudio de las soluciones técnicas adoptadas por cada Parte contratante con ánimo de respetar el artículo 103.

La ACC constató que las Partes contratantes interpretaban de diferente modo la obligación que les impone el Convenio de registrar como promedio una décima parte de las transmisiones de datos de carácter personal en la parte nacional del Sistema de Información Schengen, a efectos de control de la admisibilidad de la consulta (artículo 103).

Para armonizar el procedimiento aplicado por las Partes contratantes, la ACC ha emitido un dictamen sobre la interpretación de este artículo.

La ACC considera que un registro conforme con el artículo 103 debe reunir los siguientes requisitos mínimos:

1. Deberá registrarse un promedio suficientemente representativo de todas las consultas, haya o no respuesta positiva. El requisito mínimo del 10% de registros también puede cumplirse mediante registros periódicos.

2. Un registro adecuado deberá contener los siguientes elementos fundamentales:

a. los datos biográficos transmitidos en relación con la persona objeto de la consulta;

b. la identificación del terminal, o de la autoridad que ha realizado la consulta, atendiendo a que se adopte cualquier medida útil para permitir la identificación del usuario;

c. lugar, fecha y hora de la consulta;

d. el motivo de la consulta; mencionando, por ejemplo, la base jurídica de la descripción.

3. Por otra parte, sería deseable que la consulta contuviese la siguiente información para el control de admisibilidad en un caso concreto: Referencia del expediente o número de asiento en el registro policial, en caso de llevarlo, a fin de volver a localizar el expediente que hubiese motivado la consulta.

Los datos deberán utilizarse exclusivamente para los fines previstos en el artículo 103.

Los datos registrados deberán borrarse en un plazo de 6 meses.

La ACC ha insistido en que se tenga en cuenta la obligación que resulta del artículo 103 de conformidad con el presente dictamen.

CAPÍTULO V : PROGRAMA DE ACCIÓN

El 3 de febrero de 1998 se ha aprobado el programa de acción propuesto por el Presidente de la ACC para el primer semestre de 1998.

El programa está orientado a conceder mayor importancia al papel de la ACC en el marco de Schengen, define las prioridades de su intervención en defensa de los principios de la protección de datos y recomienda una mayor cooperación entre las instancias Schengen.

La ACC proseguirá su misión de asesoramiento y de armonización de las prácticas o las doctrinas nacionales emitiendo dictámenes; se cerciorará de que los dictámenes emitidos sean objeto de la necesaria difusión por parte del Grupo Central, y de no ser así adoptará un método de publicación de los mismos.

Se prestará especial atención al seguimiento por parte de los órganos ejecutivos de Schengen de los dictámenes y recomendaciones de la ACC, en particular por lo que se refiere a la seguridad del C.SIS.

En efecto, si bien es cierto que las dos presidencias de Schengen durante 1997 han confiado el examen de estas recomendaciones a grupos técnicos, hay que reconocer que este asunto no ha recibido la prioridad que debería a juicio de la ACC.

La ACC desea que las instancias de Schengen le den a conocer en muy breve plazo qué curso tienen previsto reservar a sus recomendaciones. Este es el caso en particular de la solicitud de la ACC de que se le asigne una cuenta de usuario con fines de auditoría.

Esta solución le permitiría acceder directamente, sin capacidad de modificación, al sistema de explotación y a las bases de datos, y proceder así con mayor facilidad al control del C.SIS.

Por otra parte, la seguridad de las oficinas SIRENE será objeto de un control específico en todos los países, y se elaborará un informe final a partir de dicha base.

La ACC velará por que en los puntos de cruce autorizados de las fronteras exteriores del espacio Schengen esté disponible el folleto sobre el derecho de acceso y de información de los ciudadanos respecto de los datos del SIS que les conciernen, cuyo texto ha aprobado en diciembre de 1997.

La ACC reforzará sus contactos con los representantes de la Unión Europea, en la perspectiva de la incorporación del acervo de Schengen a la Unión Europea, en especial participando en la definición de su acervo. Este asunto adquirirá especial importancia en el marco del desarrollo de sistemas europeos de policía.

La ACC presentará al público y a la prensa su informe anual en la conferencia de prensa que organizará en Bruselas el día 28 de abril de 1998.

La ACC organizará en Lisboa el 30 de junio de 1998 un coloquio sobre los derechos de los ciudadanos respecto de los sistemas policiales de información, basándose en el modelo de Schengen.

La realización de este programa pretende contribuir a la reafirmación del papel de la ACC y a la eficacia de su intervención en defensa de los derechos y libertades de los ciudadanos, en el marco de la consolidación del espacio europeo.

ANEXO 1

Declaración de los países con estatuto de observadores

"Los países nórdicos, dado que disponen del estatuto de observadores en el seno de la ACC, comparten las preocupaciones expresadas en el informe anual por los Estados Schengen que son miembros de pleno derecho. Comparten asimismo los principales puntos de vista que figuran en dicho informe. Consideran muy importante que las instancias centrales y nacionales Schengen observen y respeten los dictámenes y opiniones formuladas.

La presencia de las comisiones nacionales de los países nórdicos en el seno de Schengen - en materia de protección de datos y de la vida privada - reviste una importancia considerable en el marco de los esfuerzos orientados a garanti - zar que la opinión pública acepte y apoye la realización de las actividades importantes previstas por el Convenio de Schengen. Los observadores nórdicos piensan que es posible que el presupuesto de la ACC deba aumentarse en el futuro. Consideran que deben incrementarse sin demora los recursos administrativos de la Secretaría, pero no excluyen la necesidad de disponer de una autoridad más formal".

ANEXO 2. PRO MEMORIA

I. LAS INSTANCIAS COMUNES PARA LA APLICACIÓN DEL CONVENIO

Para la aplicación del Convenio, las Partes contratantes han creado dos instancias:

* El Comité Ejecutivo, compuesto por un ministro responsable de la aplicación del Convenio en cada Parte contratante, tiene por misión general velar por la correcta aplicación del Convenio y dispone por otro lado de competencias espe - ciales (artículo 131).

* La Autoridad de Control Común (ACC), compuesta por dos representantes de cada autoridad nacional de control de las Partes contratantes, tiene por misión comprobar la correcta aplicación de las disposiciones del Convenio con respecto a la unidad de apoyo técnico del SIS (artículo 115). Dispone asimismo de competencias más generales en materia de protección de datos.

Además de estas dos instancias, la organización de Schengen está estructurada en torno a un Grupo Central, del que depende un Comité de Orientación SIS así como varios grupos de trabajo, de los cuales sólo uno está creado por el Convenio5.

Las instancias Schengen están asistidas por una secretaría, puesta a su disposición por el BENELUX, con sede en Bruselas.

II. OBJETIVO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN SCHENGEN

La totalidad del Título IV del Convenio está dedicada al Sistema de Información Schengen (SIS).

El artículo 93 del Convenio precisa que el SIS tiene por objeto preservar el orden y la seguridad públicos, incluida la seguridad del Estado, y la aplicación de las disposiciones del Convenio sobre la circulación de personas con la ayuda de la información transmitida por dicho sistema.

Información registrada

El artículo 94 enumera de forma limitada las categorías de datos que pueden introducirse en el sistema. Los artículos 95 a 100 especifican las finalidades que justifican la introducción de las descripciones.

Las categorías de datos hacen referencia a personas, objetos y vehículos.

* En el caso de personas, se podrán incluir los elementos relativos al estado civil y los alias, los rasgos físicos particu - lares, objetivos e inalterables, la indicación eventual de que las personas están armadas o que son violentas y la conducta que debe observarse en caso de localización.

Está prohibido mencionar información considerada como sensible y que revele el origen racial, las opiniones políticas, las convicciones religiosas u otras, así como la relativa a la salud o a la vida sexual. Las finalidades que justifican la descripción de una persona en el SIS son las siguientes:

a. Sea cual sea la nacionalidad de la persona:

- detención a efectos de extradición (artículo 95);
- búsqueda en caso de desaparición, búsqueda de menores o de personas que deban ser internadas por decisión de una autoridad competente (artículo 97);
- detención para comparecencia, incluidos los testigos, ante la justicia en el marco de un procedimiento penal o para ejecución de una pena privativa de libertad (artículo 98);
- vigilancia discreta y control específico para la represión de infracciones penales, la prevención de amenazas para la seguridad pública o la prevención de amenazas graves para la seguridad del Estado (artículo 99).

b. Para los extranjeros, es decir, toda persona que no sea nacional de los Estados miembros de las Comunidades Europeas (definición en el artículo 1, 6° párrafo):

- no admisión en el territorio como resultado de una decisión administrativa o judicial adoptada observando las normas de procedimiento previstas por la legislación nacional o en base a una amenaza contra el orden público y la seguridad

nacional o en base al incumplimiento de las legislaciones nacionales relativas a la entrada o a la residencia de extranjeros (artículo 96).

* En el caso de los objetos, sólo se podrán introducir los elementos, incluido el nombre de su propietario, que hagan referencia a vehículos, armas de fuego, documentos y billetes de banco robados, sustraídos u ocultados buscados con vistas a su incautación o como pruebas en un procedimiento penal (artículo 100).

* En el caso de los vehículos, podrán asimismo ser introducidos los datos relativos a los vehículos buscados a efectos de vigilancia discreta o de control específico (artículo 99 antes mencionado). Esta categoría permite la introducción de información relativa al conductor y los ocupantes de los vehículos vigilados.

Destinatarios de la información

Los artículos 92 y 101 del Convenio indican que las autoridades designadas por las Partes contratantes pueden acceder, por consulta automatizada o no:

- al conjunto de datos integrados en el SIS para controles fronterizos y comprobaciones u otros controles de policía y de aduanas dentro del país, de conformidad con el derecho nacional;

- únicamente a la categoría de las descripciones a efectos de no admisión para la expedición de visados, de permisos de residencia y la administración de extranjeros en el marco de lo dispuesto en el Convenio relativo a la circulación de personas.

Debe facilitarse al Comité Ejecutivo la lista de las autoridades que pueden consultar directamente los datos integrados en el SIS (artículo 101.4).

Arquitectura del Sistema de Información Schengen

Si bien varios de los artículos del Título IV prescriben el respeto de ciertas medidas de orden técnico, la descripción general del sistema figura en el artículo 92.

El Sistema de Información Schengen (SIS) está compuesto por una parte nacional (N.SIS) en cada una de las Partes contratantes y de una unidad de apoyo técnico (C.SIS) creada y mantenida en común, cuya responsabilidad asume la República Francesa.

La unidad de apoyo técnico, instalada en Estrasburgo, tiene como objeto hacer que todos los N.SIS sean materialmente idénticos. Para ello, el C.SIS contiene un fichero de datos que garantiza la identidad de los ficheros nacionales por la transmisión en línea de informaciones.

La transmisión de datos se efectúa de conformidad con los protocolos y procedimientos establecidos en común por las Partes contratantes para la unidad de apoyo técnico.

El artículo 118.4 describe las medidas de seguridad que deben adoptarse para la unidad de apoyo técnico. Estas medidas son idénticas a las requeridas para cada N.SIS (apartados 1 a 3 del artículo 118).

III. OFICINAS SIRENE

Las oficinas SIRENE (Suplemento de Información Requerido para la Entrada Nacional) son una creación de las Partes contratantes no prevista expresamente por el Convenio.

Encargadas de efectuar en cada Estado Schengen, sobre la base del SIS, intercambios de información complementaria, sirven asimismo de intermediarias durante las diversas consultas entre los Estados sobre la conducta a seguir en el caso de ejecución de una descripción.

Sus misiones y acciones están definidas de manera concreta en un manual común, "Manual SIRENE". Consisten, principalmente, en consultas previas a la creación de descripciones, intercambios de información y vigilancia de las descripciones múltiples y el establecimiento de prioridades.

IV. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Una ley y una autoridad nacional de control: condiciones previas a la aplicación del Convenio

Las Partes contratantes han establecido varias condiciones previas a la aplicación en su territorio del Convenio. En el Acta final se recuerda el carácter imperativo de su respeto.

Dentro de estas condiciones figura la obligación para cada Parte contratante de disponer, antes de cualquier transmisión de datos de carácter personal, de una autoridad nacional de control independiente (artículos 114 y 128) y de una ley de protección de datos.

Concretamente, por lo que respecta al tratamiento automatizado o no de datos transmitidos en aplicación del Convenio, el Convenio contiene las siguientes prescripciones:

a. Para el tratamiento automatizado de datos transmitidos en aplicación del Título IV relativo al SIS:

Artículo 117

Cada Parte contratante adoptará, a más tardar en el momento de la entrada en vigor del presente Convenio, las disposiciones nacionales necesarias para conseguir un nivel de protección de los datos de carácter personal que sea al menos igual al resultante de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas en lo referente al tratamiento automatizado de datos de carácter personal, y respetando la Recomendación R (87) 15 de 17 de septiembre de 1987 del Comité de Ministros del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

La transmisión de los datos de carácter personal no podrá realizarse hasta que las disposiciones de protección de datos de carácter personal hayan entrado en vigor en el territorio de las Partes contratantes afectadas por la transmisión.

b. En lo relativo al tratamiento automatizado de otros datos transmitidos en aplicación del Convenio, con la excepción de las solicitudes de asilo:

Artículo 126

La exigencia, en el momento de la entrada en vigor del Convenio, de un nivel de protección de datos de carácter personal que sea al menos igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 arriba mencionado y la transmisión de datos también supeditada a la eficacia de esta protección en el territorio de las Partes contratantes afectadas por la transmisión.

Artículo 129

Para la transmisión únicamente de los datos relativos a la cooperación policial, las Partes contratantes se comprometen a conseguir un nivel de protección de los datos de carácter personal que cumpla los principios de la Recomendación R (87) 15 de 17 de septiembre de 1987 del comité de Ministros del Consejo de Europa arriba mencionada.

c. Para los datos transmitidos en aplicación del Convenio procedentes de un fichero o integrados en un fichero, exceptuando aquellos relativos a las solicitudes de asilo, al SIS o a la asistencia judicial en materia penal:

Artículo 127:

Aplicación de lo dispuesto en el artículo 126 y, para la transmisión de datos relativos a la cooperación policial, nivel de protección de datos que cumpla los principios de la Recomendación R (87) arriba mencionada.

d. Finalmente, por lo que respecta a los datos transmitidos que figuran en los expedientes, únicamente se aplicarán, con una excepción, las disposiciones específicas de protección de datos del artículo 126.3 bajo el control, en su caso, de la autoridad nacional competente (artículo 128.2).

2. Campos de aplicación respectivos del Convenio y del derecho nacional

El Convenio establece, para la protección de datos de carácter personal, un reparto complejo entre el campo de aplicación de sus disposiciones y el de los derechos nacionales de las Partes contratantes.

Derechos de las personas respecto al SIS

La regla puede enunciarse de la siguiente forma: mientras que el Convenio no establezca disposiciones especiales, se aplicará el Derecho de cada Parte.

El Convenio precisa la naturaleza de los derechos que se reconocen a las personas y los límites eventuales que se aplican. Sin perjuicio del cumplimiento de tales disposiciones, los derechos de las personas se ejercen cumpliendo el derecho nacional de cada Parte contratante.

a. Derecho de acceso y de comunicación (artículo 109)

Toda persona puede acceder a la información que se refiera a ella introducida en el SIS. Para ello, la persona deberá presentar una solicitud ante los organismos competentes en cada Parte contratante.

Si está previsto por el derecho nacional, el autor de la solicitud podrá recibir la información referente a él. Sin embargo, en aplicación del "principio de propiedad de datos", la comunicación estará supeditada al hecho de que el Estado ante el que se presenta la solicitud que no es el autor de la introducción de los datos dé previamente al Estado descriptor la ocasión de adoptar una postura.

No se facilitará información a la persona en cuestión si dicha información pudiera ser perjudicial para la ejecución de la descripción o si se considera necesaria para la protección de los derechos y libertades de terceros. Se denegará en todos los casos si la persona está descrita a efectos de vigilancia discreta.

b. Derecho de rectificación (artículo 110)

Toda persona podrá, en los datos que se refieran a ella, hacer rectificar datos que contengan errores de hecho o hacer suprimir datos que contengan errores de derecho. En la práctica, el ejercicio de tal derecho se facilita ampliamente mediante la comunicación de la información que figura en el sistema.

c. Derecho de emprender acciones a efectos de rectificación, supresión, información o indemnización (artículo 111)

En el territorio de cada Parte contratante, toda persona podrá hacer valer sus derechos ante el órgano jurisdiccional o la autoridad competente. Las decisiones definitivas serán ejecutadas por la Parte contratante afectada.

d. Derecho de solicitar la comprobación de datos (artículo 114.2)

Toda persona tendrá derecho a solicitar a las autoridades de control que comprueben los datos referentes a ella integrados en el SIS, así como el uso que se haga de dichos datos. Si los datos hubieran sido introducidos por otro Estado, el control se realizará en estrecha colaboración con la autoridad de control del Estado descriptor.

Si bien aún no se ha elaborado una recopilación exhaustiva de las solicitudes presentadas ante los Estados Schengen para el ejercicio de los derechos antes mencionados, de la información de la que dispone la ACC se desprende que, para cada Estado, el número de dichas solicitudes oscila entre una y cuarenta para los dos años transcurridos.

El control del Sistema de Información Schengen

El Convenio cita los principios de protección de datos que, sin perjuicio del derecho nacional de cada Parte contratante, se aplican en el tratamiento de datos integrados en el SIS (artículo 104). Para el control de su respeto, el Convenio distingue entre la Autoridad de Control Común y las autoridades nacionales de control (artículos 114 y 115).

Los principios enumerados por el Convenio son los siguientes :

a. Principio de finalidad de la introducción de los datos, y salvo excepciones enumeradas de forma limitada, de su utilización: extradición, no admisión, personas desaparecidas, testigos, personas citadas o condenadas, objetos robados, personas y vehículos bajo vigilancia discreta o control específico (artículos 94 a 100 y 102 antes mencionados).

b. Prohibición de tratar datos sensibles y enumeración limitada de los datos introducidos (artículo 94 antes mencionado).

c. Definición de los destinatarios: acceso limitado a las autoridades nacionales competentes en ámbitos específicos y únicamente para el cumplimiento de sus misiones (artículo 101 antes mencionado).

d. Prohibición de copiar las descripciones de otra Parte contratante en un fichero nacional y limitación de las duplicaciones con fines técnicos (artículo 102).

e. Obligación de registro de la décima parte de las transmisiones de datos a efectos de control de la admisibilidad. (artículo 103).

f. Establecimiento de un periodo de conservación de datos (artículos 112 y 113).

g. Obligación de conservar los datos suprimidos durante un año en la unidad de apoyo técnico para el control posterior de su exactitud y de la licitud de su integración (artículo 113.2).

Respecto al control del sistema, el Convenio precisa que cada Parte contratante debe encomendar a una autoridad nacional que controle de manera independiente y con arreglo a lo dispuesto por el derecho nacional (artículo 114), el fichero de la parte nacional del sistema de información (N.SIS). Estas autoridades deberán comprobar que se respetan las disposiciones de protección de datos previstas por el Convenio y las que se añadan, en su caso, por el derecho nacional.

En cambio, el control de la unidad de apoyo técnico (C.SIS) corresponde a la Autoridad de Control Común, que deberá actuar según lo dispuesto en el Convenio de Schengen, el Convenio del Consejo de Europea sobre la protección de datos, la Recomendación del Consejo de Europa para los datos en el sector de la policía y de conformidad con el derecho francés.

Intercambios de información fuera del SIS

El Título VI (Artículo 126 y siguientes) del Convenio, titulado "protección de datos de carácter personal", se dedica a las normas aplicables a los intercambios de informaciones que no se hayan de introducir en el SIS pero que intervienen

para la aplicación del Convenio (ver punto 2.1. b y c).

Los principios establecidos (finalidad, límite de destinatarios, exactitud de los datos, etc.) se aplican sin prejuicio de las disposiciones del derecho nacional de protección de datos que rige principalmente el ejercicio de los derechos de las personas implicadas.

El control del respeto de las normas citadas por el Convenio incumbe a las autoridades nacionales.

La ACC posee un papel residual: puede, a petición de las Partes contratantes, emitir un dictamen sobre la dificultad de aplicación e interpretación que plantean dichas normas.

ANEXO 3. DICTÁMENES DE LA ACC

Autoridad de Control Común

Bruselas, 7 de marzo de 1997
SCH/Aut-cont (97) 22 rev.
Traducción: orig. PT

DICTAMEN DE 7 DE MARZO DE 1997 RELATIVO AL PROYECTO PILOTO "VEHÍCULOS ROBADOS"

Se ha solicitado a la ACC que se pronuncie sobre un proyecto piloto relativo a vehículos robados. Se pretende saber si resulta posible que los países no integrados en el SIS puedan acceder a datos introducidos en el Sistema de Información Schengen y, en concreto, a los relativos a vehículos robados.

La solicitud de dictamen no venía acompañada de datos relativos al proyecto como entidades participantes, sistema de coordinación nacional e internacional, condiciones de acceso a la información, así como su utilización y su análisis futuro.

Mientras tanto ha sido posible recabar las siguientes informaciones:

El proyecto piloto está destinado a mejorar la coordinación policial europea en la lucha contra el tráfico de vehículos robados, en concreto la identificación de las redes internacionales de tráfico, sus rutas y los métodos utilizados.

En las acciones a desarrollar de forma coordinada en las distintas fronteras y zonas previamente definidas se ven implicadas las fuerzas policiales que, en los distintos Estados, tienen competencia en materia de controles fronterizos, fiscalización vial, aduanera, fiscal y penal.

En el proyecto participan los siguientes Estados:

Las Partes Contratantes del Convenio de Aplicación que tienen descripciones y acceso al Sistema de Información Schengen (Alemania, Bélgica, España, Francia, Luxemburgo, Países Bajos, Portugal).

Las Partes Contratantes del Convenio o de los Acuerdos de cooperación con los Estados Schengen en los que, por distintas razones, el Convenio aún no se aplica y que ni introducen descripciones en el sistema, ni tienen acceso al SIS (Austria, Grecia, Italia, Dinamarca, Finlandia, Noruega y Suecia).

Pronunciándose sólo sobre las cuestiones relativas a la protección de datos de carácter personal,

LA ACC

Considerando que:

a. el acceso a los datos introducidos en el Sistema de Información Schengen, así como los derechos a consultar directamente, están exclusivamente reservados a las entidades competentes indicadas en una lista comunicada al Comité Ejecutivo, en la que se define el tipo de descripción a la que tiene acceso cada autoridad (el derecho de consulta y acceso a determinado tipo de descripciones corresponde a la competencia nacional de cada entidad - primer y tercer apartados del artículo 101 del Convenio);

b. los usuarios sólo podrán utilizar los datos a los efectos previstos en cada una de las descripciones (finalidad de utilización - primer apartado del artículo 102 del Convenio);

c. el derecho nacional se aplica a los datos introducidos en la parte nacional del SIS, sin perjuicio de la aplicación de normas más rigurosas por el Convenio (primer apartado del artículo 104);

d. la transmisión de datos personales en aplicación del Convenio sólo podrá realizarse a las Partes Contratantes que garanticen, a nivel nacional, un régimen de protección de datos personales al menos igual a los principios del Convenio nº 108, de 28 de enero de 1981, del Consejo de Europa (primer y segundo apartados del artículo 126 del Convenio);

e. las informaciones relativas a la marca, tipo, color, características técnicas de un vehículo no constituyen, por si, datos personales, siempre y cuando estas informaciones no estén asociadas a la matrícula, al propietario o al conductor del vehículo en causa (lo que, por ejemplo, permitiría identificar a un vehículo recurriendo a un constructor sin conocer al titular registrado);

f. a nivel de cada uno de los países implicados en el proyecto resulta posible, gracias a los mecanismos de cooperación policial -bilateral o internacional-, el acceso de las autoridades policiales de otro Estado a las bases de datos nacionales de vehículos robados, a partir del momento en que la legislación nacional de protección de datos de carácter personal no lo impida o lo permita;

g. la facilitación de información a las autoridades competentes de cada uno de los países participantes en el proyecto por parte del país autor de la descripción no supone una violación de las normas de protección de datos de carácter personal previstas en el Convenio, siempre que no se comuniquen otros datos o elementos.

h. el intercambio de información de tipo policial relativa a vehículos robados, sobre la base de los ficheros nacionales, de las Partes Contratantes del SIS a los demás países en los que aún no se aplica el Convenio de Schengen está regulado por las legislaciones nacionales en materia de protección de datos de carácter personal, bajo el control de las respectivas autoridades nacionales.

Emite el siguiente

DICTAMEN

1. Las autoridades de las Partes Contratantes en las que no se aplica el Convenio no podrán acceder ni consultar directamente las informaciones y datos personales incluidos en el Sistema de Información Schengen, según lo dispuesto en los artículos 101, 126.1 y 126.2 del Convenio.

2. Los datos del vehículo relativos a marca, tipo, color y características técnicas no son, en cuanto tales, datos personales a efectos del Convenio de Schengen.

3. La comunicación realizada en el ámbito del proyecto a las autoridades competentes de los países parte en el mismo por el país autor de una descripción no supone una violación de las normas de protección de datos de carácter personal consagradas en el Convenio, siempre que no se transmita ningún otro tipo de datos.

4. El intercambio de información realizada en el ámbito de la cooperación policial y sobre la base de los ficheros nacionales está regulada por la legislación nacional respectiva, en concreto la relativa a protección de datos de carácter personal, siempre que dicha legislación no lo impida.

Autoridad de Control Común

Bruselas, 7 de marzo de 1997
SCH/Aut-cont (97) 19 rev.
Traducción: Orig. PT
DOCUMENTO FINAL

DICTAMEN DE 7 DE MARZO DE 1997 SOBRE EL CONVENIO DE COOPERACIÓN EN MATERIA DE TRAMITACIÓN DE EXPEDIENTES POR INFRACCIONES DE TRÁFICO Y EJECUCIÓN DE LAS SANCIONES PECUNIARIAS IMPUESTAS

El Grupo Central solicitó el dictamen de la ACC respecto al Convenio sobre cooperación en materia de infracciones de tráfico (doc. SCH/III (96) 25, 4ª rev.).

Dicho Convenio consagra:

1. El principio de cooperación entre las Partes contratantes por lo que respecta a la tramitación de expedientes por infracciones de tráfico, y su respectiva ejecución, materializado por la posibilidad de acceso del servicio nacional encargado de los registros de tráfico de cada uno de los países, tomando como base una matrícula, a los registros de tráfico de los demás Estados, en relación con los datos del vehículo (tipo y marca), así como con la identificación del propietario del vehículo (nombre y dirección) en el momento de la comisión de la infracción.

2. La comunicación directa de la información a las autoridades competentes de los Estados que solicitan la información, así como el nombre y la dirección de la autoridad requerida.

3. La notificación directa de los presuntos autores de infracciones, por parte de la autoridad requirente, con comunicación de la información que permite la reacción o la presentación de un recurso a las personas o entidades implicadas.

4. La colaboración de las autoridades con vistas a obtener la reacción del interesado.

5. Un sistema que pretende limitar los importes de las sanciones pecuniarias al importe previsto por la ley del Estado en el que éstas se ejecutan.

6. La misión general del Comité Ejecutivo de Schengen de velar por la aplicación del referido Convenio.

7. La aplicación a la transmisión de datos de carácter personal de los artículos 126 a 128 del Convenio de Aplicación de Schengen.

Centrando el análisis en el aspecto referente a la protección de datos de carácter personal, la ACC considera que:

a. El Convenio sobre infracciones de tráfico se basa en dos aspectos esenciales: por una parte, el acceso a la información y datos que figuran en los registros de tráfico de las demás Partes contratantes, en los límites de la finalidad prevista y en el ámbito de las competencias de las autoridades nacionales respectivas. Y por otra parte, un sistema que permite la notificación directa, la cooperación y la efectiva ejecución de una decisión de una autoridad de una Parte contratante por una autoridad de otro Estado, en determinadas condiciones que limitan la aplicación de una sanción pecuniaria, incluso la excluyen (si la legislación nacional no tipifica la infracción en cuestión).

b. Sólo pueden transmitirse los datos a las Partes contratantes que cuentan con una Autoridad de control nacional independiente y con una legislación nacional sobre protección de datos y que garantizan un nivel de protección de datos de carácter personal al menos igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (de conformidad con los apartado 1 y 2 del artículo 126, y del apartado 1 del artículo 128 del Convenio).

c. Los datos de carácter personal se limitan al nombre y dirección del propietario del vehículos y presunto autor de la infracción.

d. Los principios enunciados en los artículos 126 a 128 del Convenio se aplican a la transmisión y utilización de los datos, lo que implica que los datos únicamente se utilizan para los fines para los que han sido transmitidos, a saber, la identificación y ejecución de una infracción vial con vistas a la ejecución de una sanción pecuniaria (principio de la finalidad). Asimismo, los datos transmitidos no se pueden poner en relación con sistemas de información nacional en materia de infracciones viales.

e. Queda garantizado el derecho del titular de los datos a ser informado del hecho de que éstos han sido transmitidos, así como el principio de la notificación previa a la ejecución de la sanción pecuniaria, con garantía de defensa y reacción, incluyendo por tanto la posibilidad de oponerse a las decisiones fundadas sobre un error de hecho o de derecho (artículos 4 y 6 del Proyecto de convenio).

No obstante, la Autoridad de Control Común considera conveniente que también se incluyan o expliciten en el mencionado convenio los siguientes principios:

1. El derecho de cualquier persona a poder exigir la rectificación o supresión de datos que le conciernan, que contengan errores de hecho o de derecho.

2. El principio de la cooperación entre las autoridades nacionales de control, contempladas en el artículo 128.1, con vistas a garantizar los derechos de acceso, rectificación o supresión.

3. La competencia de la ACC para emitir un dictamen en cuanto a los aspectos comunes en materia de protección de datos de carácter personal, que resulten de la aplicación del mencionado convenio, principio que debe constar en su artículo 16.

Autoridad de Control Común

Bruselas, 26 de mayo de 1997
SCH/Aut-cont (97) 38 rev
Traducción ; orig. FR

DICTAMEN Nº 01/97 DE 22 DE MAYO DE 1997 RELATIVO A LA DUPLICACIÓN DE UNA PARTE DE LAS DESCRIPCIONES DEL SIS

Asunto: **Utilización de soportes técnicos de duplicación para la consulta de las descripciones a efectos del artículo 96 del Convenio de Aplicación del Acuerdo de Schengen por parte de Representaciones diplomáticas y Oficinas consulares de algunos Estados Schengen en el extranjero.**

Con motivo de la reunión del 22 de mayo de 1997, la Autoridad de Control Común (en lo sucesivo ACC) ha decidido, en base a los artículos 115.3 y 126 f) del Convenio de Aplicación del Acuerdo de Schengen (en lo sucesivo CAS), emitir el siguiente dictamen al Grupo Central relativo al problema mencionado más arriba :

Constatando que las Representaciones diplomáticas y Oficinas consulares de algunas de las Parte contratantes (p. ej. Bélgica, España, los Países Bajos y Francia) utilizan diversos medios técnicos para facilitar la consulta in situ de las descripciones previstas en el artículo 96 CAS,

- que dichas consultas se realizan para la expedición de un visado de entrada en territorio Schengen de conformidad con los artículos 92.1 in fine y 101.2 CAS,

- que, por múltiples razones, las Representaciones diplomáticas y Oficinas consulares de algunas de las Partes contratantes no disponen aún de un sistema de consulta directa al SIS,

la ACC ha procedido a verificar su compatibilidad con el modelo inicial del SIS tal y como se halla desarrollado en el CAS.

En efecto, varias disposiciones del CAS imponen condiciones estrictas en lo que se refiere a los procedimientos de utilización del SIS:

a. en varias partes del artículo 92 CAS se contempla "un procedimiento de consulta directa" (art. 92.1 CAS) basado en una "transmisión rápida y eficaz" de los datos (art. 92.2 CAS).

El artículo 92.3 CAS precisa además que la unidad de apoyo técnico, llamada más comúnmente C.SIS, incluye un fichero de datos que garantiza la identidad de los ficheros de datos de los diferentes N.SIS "mediante la transmisión en línea de informaciones".

Por otra parte, el artículo 101.2 CAS, que habilita a diversas autoridades a acceder a las descripciones a efectos del artículo 96 CAS, evoca asimismo el modo "de consulta directa" precisamente por parte de las autoridades competentes para la expedición de visados y de las autoridades centrales competentes para el examen de las solicitudes de visado.

Por último, se menciona de nuevo el proceso de consulta directa en los artículos 101.4 y 102.2 CAS. El artículo 106.2 CAS contempla por su parte la posibilidad de que cada Parte contratante deba corregir o suprimir, es decir, modificar o actualizar los datos "sin demora".

De estas disposiciones del Título IV CAS se desprende que el tipo de tratamiento de la información que quisieron desarrollar los autores del CAS se refiere a un sistema de consulta automatizada de datos que permita el tratamiento de datos en tiempo real.

b. El CAS prevé una serie de disposiciones de seguridad

El artículo 118.1 CAS exige a cada una de las Partes contratantes un conjunto de garantías para proteger los datos de carácter personal integrados en el SIS.

De dichas disposiciones, la ACC destaca las siguientes:

- **las medidas *adecuadas*** "para impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados por una persona no autorizada (control de los soportes de datos)" (art. 118.1.b CAS);

- **las medidas adecuadas** *"para garantizar la posibilidad de verificar y comprobar a qué autoridades pueden ser remitidos datos de carácter personal a través de las instalaciones de transmisión de datos (control de la transmisión)"* (art. 118.1.f CAS);

- **las medidas adecuadas** *"para impedir que, en el momento de la transmisión de datos de carácter personal y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control de transporte)"* (artículo 118.1.h CAS).

c. Por otra parte, hay previstos requisitos para controlar el registro.

El artículo 103 CAS recomienda que cada Parte contratante registre una décima parte de las transmisiones de datos de carácter personal para controlar la admisibilidad de la consulta.

En enero de 1994, a raíz de una pregunta de la Autoridad de Control Común provisional (véase la nota SCH/Aut-cont (94) 33 del 10 de enero de 1994), el representante del Comité de Orientación precisó que dicho artículo se ha interpretado en el sentido de registrar al menos una décima parte de las respuestas positivas (véase la nota SCH/OR.SIS (95) 116 del 16 de junio de 1995).

POR ESTE MOTIVO, la ACC considera que la utilización de cualquier tipo de medios de duplicación (CD Rom, disquete, etc.) para la consulta de descripciones a efectos del artículo 96 CAS por parte de las Representaciones diplomáticas y Oficinas consulares de algunos Estados Schengen en el extranjero está sujeta a las tres condiciones siguientes:

1. Las técnicas y medios de duplicación deberán garantizar la identidad de los datos en tiempo real en relación con el tratamiento central SIS. Cualquier diferencia de tiempo, por mínima que sea, deberá ajustarse a las condiciones

previstas en el apartado 4.

2. Dicha técnicas y medios de duplicación deberán garantizar los niveles mínimos de protección exigidos en el artículo 118.1 CAS, y más en concreto en las letras b), d), f) y h) de dicho artículo, así como ser conformes a lo dispuesto en el artículo 118.3 CAS.

3. El programa que permita su utilización deberá permitir un registro que responda a lo dispuesto en el artículo 103 CAS.

Dichos registros deberán enviarse al país cada seis meses, y la instancia contemplada en el artículo 108.2 CAS con competencia central para la parte nacional del SIS deberá mantenerlos a disposición de la autoridad de control nacional contemplada en el artículo 114 CAS;

4. En caso de que se utilicen medios de duplicación que presenten riesgo de falta de identidad de datos, la ACC recomienda encarecidamente que, tal y como está previsto en los artículo 92.2 y 116 CAS, la Parte contratante responsable:

- se comprometa, en caso de descripción del individuo en el soporte de duplicación utilizado, a hacer una verificación en tiempo real (red, teléfono, fax) para asegurarse de la confirmación de esta información;

- se comprometa, en caso de no descripción del individuo en el soporte de duplicación utilizado, a aceptar su responsabilidad si se produce la descripción de este mismo individuo en el espacio de tiempo que exista entre la fijación de los datos sobre el duplicador y el tiempo real. Sólo podrá quedar exento de esta responsabilidad mediante prueba de una verificación en tiempo real en el momento de la solicitud de visado.

Autoridad de Control Común

Bruselas, 3 de febrero de 1998
SCH/Aut-cont (97) 55, 2ª rev.
Traducción: Orig. DE

DICTAMEN Nº 98/1 DE 3 DE FEBRERO DE 1998 RELATIVO A LA CONSERVACIÓN DE LOS EXPEDIENTES TRAS LA SUPRESIÓN DE UNA DESCRIPCIÓN

Asunto: Conservación de los expedientes tras la supresión de una descripción

En su reunión del 3 de febrero de 1998, la Autoridad de Control Común (en lo sucesivo "ACC") ha adoptado el siguiente dictamen, sobre la base del artículo 115.3 de Convenio de Aplicación de Schengen (CAS):

Consciente de que los servicios de policía nacionales de determinadas Partes contratantes siguen conservando expedientes de las descripciones del artículo 95 y siguientes del CAS incluso tras su supresión, y abren expedientes criminales, y

Conscientes de que las autoridades policiales en cuestión se amparan para ello en la legislación nacional en materia de protección de datos (véase letra b) del apartado 2.1.3 del Manual SIRENE), aplicándose asimismo las disposiciones del Título VI del Convenio de Aplicación de Schengen,

la ACC ha procedido al examen de esta práctica y, a este respecto, quiere hacer hincapié sobre todo en los siguientes requisitos en materia de protección de datos.

La ACC confirma los principios y derechos fundamentales en materia de protección de datos contemplados en el Convenio de Aplicación de Schengen, concretamente:

a. Los datos sólo se podrán suministrar y utilizar con los fines enunciados para cada una de las descripciones (art. 102. 1 y art. 94.1). Cualquier excepción a este principio general deberá justificarse por la necesidad de prevenir una amenaza grave inminente para el orden y la seguridad públicos, por razones graves de seguridad del Estado o con vistas a prevenir un hecho delictivo grave (art. 102.3).

b. Toda utilización de los datos que no sea conforme con los apartados 1 a 4 del artículo 102 se considerará como una desviación de la finalidad (art. 102.5).

c. Los datos de carácter personal introducidos en el Sistema de Información de Schengen a efectos de la búsqueda de personas sólo se conservarán, de conformidad con el art. 112 CAS, durante el tiempo necesario para los fines para los que se hubieren facilitado dichos datos.

d. En el marco de la interpretación complementaria del Convenio, estos principios son válidos para cualquier tipo de tratamiento de la información que esté relacionado con descripciones del Sistema de Información Schengen o se refiera a las mismas.

La Autoridad de Control Común considera, por tanto, que se deben adoptar las siguientes medidas:

a. en caso de supresión de una descripción a efectos de búsqueda de personas, cada Parte contratante Schengen, de conformidad con el artículo 112 CAS, debe borrarla y destruir inmediatamente todos los expedientes relativos a la misma;

b. las instancias Schengen deben proceder a una revisión del Manual SIRENE con el objeto de suprimir lo dispuesto en la letra b) del apartado 2.1.3, contrario al Convenio de Schengen.

Autoridad de Control Común

Bruselas, 3 de febrero de 1998
SCH/Aut-cont (97) 42, 2ª rev.
Traducción: Orig. PT

DICTAMEN Nº 98/2 DE 3 DE FEBRERO DE 1998 RELATIVO A LA DESCRIPCIÓN EN EL SIS DE PERSONAS CUYA IDENTIDAD HA SIDO USURPADA

La ACC ha examinado los problemas planteados por la utilización indebida de alias de personas descritas en el SIS (véanse notas SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 y SCH/Aut-cont (97) 42), a la luz de los principios de protección de datos de carácter personal previstos por el Convenio de Schengen.

La descripción del titular legítimo cuya identidad ha sido usurpada se mantiene en el SIS en la mayoría de los Estados. Actualmente, no parece posible precisar en el SIS, al menos mediante texto libre, que se trata de una usurpación de identidad.

La ACC reafirma los principios y los derechos fundamentales en materia de protección de datos, concretamente los siguientes:

a. Los datos sólo pueden proporcionarse y utilizarse para los fines enunciados en relación con cada una de las descripciones (arts. 102.1 y 94.1), principio general que únicamente puede ser soslayado por la necesidad de prevenir una amenaza grave o un hecho delictivo grave (art. 102.3).

b. Toda utilización de datos que no sea conforme con los apartados 1 a 4 del artículo 102 se considerará como una desviación de la finalidad (apartado 5 del mismo artículo 102).

c. El derecho de toda persona a exigir la rectificación o supresión de los datos que contengan errores de hecho o de derecho que se refieran a ella (artículo 110).

d. El derecho de entablar una acción ante el órgano jurisdiccional o la autoridad competente en virtud del Derecho nacional, con vistas a garantizar el derecho de rectificación o supresión (artículo 111.1).

e. El derecho a solicitar a la autoridad nacional de control que compruebe los datos (artículo 114.2).

La ACC, teniendo en cuenta de forma proporcionada y equilibrada los derechos de la persona cuya identidad ha sido usurpada, previstos por el Convenio de Schengen, así como la necesidad de detectar al usurpador, emite el siguiente dictamen:

1. Al registro en el SIS, por una Parte Contratante, de datos de una persona cuya identidad ha sido usurpada se aplica el Derecho nacional, salvo que existan condiciones más exigentes previstas en el Convenio de Schengen, de conformidad con su artículo 104.1.

2. Incumbe a la Parte Contratante autora de la descripción garantizar que los datos sean registrados para los fines enunciados, manteniéndolos actuales y exactos (artículo 102.1, artículo 106.1, artículo 110, normas de protección de datos del Convenio 108 del Consejo de Europa a que los Estados Schengen están obligados, en particular las contempladas en el artículo 5).

3. Incumbe a la Parte Contratante autora de la descripción garantizar el ejercicio del derecho de rectificación y supresión de los datos registrados, a tenor de lo dispuesto en el artículo 106 del Convenio y con arreglo al procedimiento en él previsto.

4. El mantenimiento en el SIS de la descripción de personas cuya identidad ha sido usurpada debe evaluarse según el principio de la proporcionalidad, teniendo en cuenta, por una parte, los derechos de la persona cuya identidad ha sido usurpada y, por otra, la necesidad de detectar al usurpador.

5. En espera de la entrada en funcionamiento del SIS II, es necesario estudiar y adoptar una solución adecuada y, si es posible, común, que permita indicar que se trata de una descripción de una identidad usurpada. La ACC manifiesta su

voluntad de cooperar para encontrar dicha solución.

Autoridad de Control Común

Bruselas, 3 de diciembre de 1997
SCH/Aut-cont (97) 50, 2ª rev.
Traducción: Orig. FR
Aprobado el 3 de febrero de 1998

DICTAMEN 98/3 DE 3 DE FEBRERO DE 1998 SOBRE LAS POSIBLES RELACIONES ENTRE EL SIS Y EL SISTEMA EN PROYECTO "ASF - VEHÍCULOS ROBADOS" DE INTERPOL

Se ha sometido a la ACC una nota de la Delegación alemana del Grupo OR.SIS (documento SCH/OR.SIS (97) 81) de 30 de abril de 1997, que presenta el proyecto "ASF-vehículos robados" (Automated Search Facility) con vistas a una toma de postura en el marco de Schengen respecto a Interpol.

Dicho proyecto lleva a la ACC a preguntarse si los datos del SIS relativos a personas y a vehículos robados pueden transmitirse a Interpol.

La mencionada nota ofrece una descripción sucinta del proyecto: "Según la información disponible, solamente cuatro países (Suecia, Luxemburgo, Rusia y Eslovaquia) participan actualmente en el proyecto "Vehículos robados".

Hoy en día se dispone de registros de aprox. 80.000 vehículos robados. (...) en relación a los ficheros sobre vehículos robados y personas que ya se hallan en uso (...)".

En la mencionada nota también se contempla una ampliación de este proyecto a otras categorías de datos (obras de arte robadas, tarjetas de crédito, documentos y pasaportes falsificados, embarcaciones/aparatos de vuelo robados).

Ante la importancia que estos proyectos pueden adquirir en el futuro, la ACC ha decidido emitir un dictamen sobre este proyecto concreto respondiendo a la pregunta de si los datos del SIS relativos a personas y vehículos robados pueden transmitirse a Interpol en el marco del proyecto ASF.

En referencia únicamente a los aspectos relacionados con la protección de datos de carácter personal,

la ACC,

Considerando que:

a. en virtud del artículo 101.4 del Convenio, únicamente las autoridades competentes están autorizadas a consultar directamente los datos integrados en el SIS. A este respecto, cada Parte contratante comunica al Comité Ejecutivo la lista de dichas autoridades, indicando, para cada autoridad, los datos que puede consultar y para qué misión;

b. en virtud del artículo 102.1 del Convenio, las Partes contratantes sólo podrán utilizar los datos con los fines previstos para cada categoría de descripción;

en virtud del artículo 102.2 del Convenio, está prohibida la duplicación de los datos (excepto con fines técnicos, necesaria para la consulta directa por las autoridades competentes);

en virtud del artículo 102.4 del Convenio, los datos no podrán ser utilizados con fines administrativos;

por último, en virtud del artículo 102.5 del Convenio, toda utilización de datos que no sea conforme con los mencionados apartados de este mismo artículo se considerará como una desviación de la finalidad;

c. en virtud del artículo 104.1 del Convenio, el Derecho nacional se aplicará a los datos integrados en la parte nacional del SIS, salvo que existan condiciones más exigentes en el Convenio;

d. en virtud de los apartados 1 y 2 del artículo 126 del Convenio, la transmisión de datos de carácter personal prevista en el Convenio únicamente podrá realizarse hacia las Partes contratantes que hayan adoptado las disposiciones nacionales que sean necesarias para conseguir un nivel de protección de estos datos que sea al menos igual al que se desprende de los principios del Convenio nº 108 del Consejo de Europa de 28 de enero de 1981;

e. en virtud de la letra d) del artículo 118, cada Parte contratante se compromete a adoptar, en lo referente a la parte nacional del SIS, las medidas adecuadas para impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos;

f. los datos relativos a la marca, tipo, color y características técnicas de los vehículos no son datos de carácter personal, siempre y cuando no haya ningún nexo posible con un dato que permita la identificación de una persona en relación

con este vehículo, como por ejemplo, el número de matrícula o el número de bastidor, que puedan conducir a la identi - ficación del propietario del vehículo o de su conductor;

g. las autoridades policiales de los países que participan en el proyecto ASF pueden intercambiar información (en este caso, datos de carácter personal) procedente de bases de datos nacionales, en la medida en que, a través de meca - nismos de cooperación policial, bilateral o multilateral, este intercambio esté autorizado o no esté prohibido por la legislación nacional en materia de protección de datos;

h. debe tenerse en cuenta el dictamen de 7 de marzo de 1997 que la ACC emitió respecto al proyecto piloto relativo a los vehículos robados (véase documento SCH/Aut-cont (97) 22 rev.). En dicho dictamen, se trataba de determinar si los países que no están aún integrados en el Sistema de Información Schengen podían acceder a los datos relativos a vehículos robados registrados en el SIS,

emite el siguiente DICTAMEN:

1. La información y datos de carácter personal registrados en el Sistema de Información Schengen no pueden transmi - tirse a Interpol en el marco del proyecto "ASF - vehículos robados" sin infringir las disposiciones del Convenio, en particular los artículos 101, 102, 118 y 126.

2. Los datos relativos a la marca, tipo, color y características técnicas de los vehículos no son datos de carácter personal en el sentido del Convenio.

3. La comunicación de datos no personales a Interpol en el marco del proyecto "ASF - vehículos robados" no infringe las disposiciones del Convenio en materia de protección de datos, siempre y cuando no exista ninguna relación posible con un dato que permita la identificación de una persona en relación con dicho vehículo.

4. El intercambio de información en el marco de la cooperación policial y a partir de los ficheros nacionales está regu - lado por la legislación nacional en cuestión y concretamente por la ley en materia de protección de datos.

Autoridad de Control Común

Bruselas, 3 de febrero de 1998
SCH/Aut-cont (97) 70 rev.
Traducción: orig. DE

DICTAMEN Nº 98/4 DE 3 DE FEBRERO DE 1998 RELATIVO AL REGISTRO DE CONSULTAS PREVISTO POR EL ARTÍCULO 103 DEL CONVENIO

La Autoridad de Control Común,

Visto el artículo 115 del Convenio de Aplicación de Schengen,

Consciente de que el Sistema de Información Schengen (SIS) es un sistema de búsqueda automático que requiere una protección eficaz contra el acceso no autorizado de terceros,

Consciente de que el registro de un promedio representativo de las consultas del Sistema constituye un medio adecuado de lucha contra el acceso no autorizado,

Consciente de que el artículo 103 del Convenio de Schengen obliga a cada Parte contratante a velar por que una décima parte, como promedio, de las transmisiones de datos de carácter personal sea registrada en la parte nacional del Sistema de Información de Schengen por la autoridad gestora del fichero, a efectos de control de la admisibilidad de la consulta,

Considera que un registro conforme con el artículo 103 debe reunir los siguientes requisitos mínimos:

1. Debe registrarse un promedio suficientemente representativo de todas las consultas, independientemente de si tienen como resultado una respuesta positiva o no. El requisito mínimo del 10% de registros también puede cumplirse realizándolos de forma periódica.

2. Un registro conforme deberá contener los siguientes elementos fundamentales:

a. los datos biográficos transmitidos en relación con la persona objeto de la consulta;

b. la identificación del terminal, o de la autoridad que ha realizado la consulta, atendiendo a que se adopte cualquier medida de utilidad para permitir la identificación del usuario;

c. lugar, fecha y hora de la consulta;

d. el motivo de la consulta; mencionando, por ejemplo, el fundamento jurídico de una descripción.

3. Por otra parte, sería deseable que a efectos de un control de admisibilidad en el caso concreto, la consulta contuviese la siguiente información.

Referencia del expediente o número de asiento en el registro policial, caso de llevarlo, a fin de volver a localizar el expediente que hubiese motivado la consulta;

4. Los datos deben utilizarse exclusivamente para los fines previstos en el artículo 103.

5. Los datos registrados deberán borrarse en un plazo de 6 meses.

La ACC insiste en que se tenga en cuenta la obligación que resulta del artículo 103 de conformidad con el presente dictamen.

ANEXO 4. INFORMACIÓN DE LOS CIUDADANOS

EL DERECHO DE ACCESO Y DE INFORMACIÓN DE LOS CIUDADANOS RESPECTO DE LOS DATOS QUE LES CONCIERNEN INTRODUCIDOS EN EL SISTEMA DE INFORMACIÓN DE SCHENGEN.

El Acuerdo de Schengen y su Convenio de Aplicación han dado origen a un espacio de libre circulación de personas, suprimiendo los controles en las fronteras interiores de los Estados miembros e instaurando el principio de control único a la entrada en territorio Schengen. Por motivos de seguridad, se ha puesto de manifiesto la necesidad de aplicar medidas compensatorias, entre las que destaca el Sistema de Información Schengen (SIS).

El SIS es una base de datos común al conjunto de los Estados miembros del espacio Schengen que centraliza dos grandes categorías de información: la información relativa a las personas buscadas o sometidas a vigilancia y la información sobre los vehículos u objetos buscados.

En el Sistema de Información Schengen puede, por ejemplo, introducirse información relativa a:

* las personas buscadas o vigiladas por los servicios de policía,
* las personas desaparecidas o a las que debe protegerse, en particular los menores,
* las personas no nacionales de un Estado miembro del espacio Schengen a quienes se prohibe la entrada en el territorio Schengen,
* las personas cuya identidad es utilizada fraudulentamente por otras personas como identidad falsa.

El control del SIS lo efectúa una autoridad independiente: la Autoridad de Control Común Schengen (ACC).

La ACC está integrada por miembros de las Autoridades de Protección de Datos personales de los Estados miembros del espacio Schengen. Esta autoridad, además de ejercer el control técnico de la base de datos central instalada en Estrasburgo, tiene como misión principal comprobar que los Estados miembros respetan los derechos reconocidos a las personas en el Convenio de Schengen.

Los derechos de los ciudadanos respecto al SIS.

El SIS le afecta a Ud. directamente, sea o no nacional de un Estado miembro del espacio Schengen.
Por esta razón, el Convenio de Schengen le reconoce derechos específicos en este ámbito.
Así pues, dispone Ud. de:

* el derecho de acceso a la información registrada en el SIS relacionada con Ud.;
* el derecho de rectificación en caso de que los datos se hayan registrado basándose en un error de hecho o de derecho;
* el derecho a emprender una acción ante los Tribunales o las instancias competentes para obtener la rectificación o supresión de la información errónea, o una indemnización;
* el derecho a solicitar la comprobación de los datos registrados y la utilización que de ellos se hace.

Si Ud. piensa que su nombre figura en el SIS, no dude en ejercer sus derechos. Las Autoridades Nacionales de Protección de Datos de los Estados miembros del espacio Schengen están a su disposición para ofrecerle toda la información necesaria para el ejercicio de estos derechos.

La verificación de sus datos personales incluidos en el SIS (pertinencia de su inscripción en este fichero y de la información registrada relacionada con Ud.) se efectuará según el Derecho nacional aplicable en el país que Ud. elija para ejercer sus derechos. A petición suya, la Autoridad Nacional de Protección de Datos competente le comunicará cada una de las leyes nacionales aplicables; las direcciones de contacto de estas Autoridades las podrá encontrar en este folleto. Se le informará posteriormente de los resultados obtenidos, o del curso dado a su petición.

MEMORIA DE 1997 - ANEXO IV - RECOMENDACIONES A USUARIOS DE INTERNET

(Este documento se encuentra accesible a través de la base de datos "PUBLICACIONES")