AGENCIA
DE
PROTECCIÓN DE DATOS

MEMORIA
1998

MEMORIA DE 1998 - FUNCIONAMIENTO DE LA AGENCIA

1. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

De conformidad con lo establecido en el artículo 36 h) de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal, una de las funciones de la Agencia de Protección de Datos, consiste en informar con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley; por su parte, el artículo 5 en sus apartado a) y b), concreta este precepto estableciendo que la Agencia informará preceptivamente los proyectos de disposiciones generales de desarrollo de la Ley Orgánica, así como cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica. El número de informes en este ámbito efectuado por la Agencia, sobre Proyectos de disposiciones, ha sido de 22, cifra ligeramente superior a los efectuados en el año anterior (20).

Dentro de los mismos, merecen destacarse:

* El informe sobre el nuevo texto del 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.

* El informe solicitado por el Instituto Nacional de Estadística para una Instrucción sobre la cesión de datos personales obrantes en los Padrones Municipales solicitada por distintas Administraciones Públicas con la finalidad, de poder cumplir, más satisfactoriamente, las competencias que tienen atribuidas.

* Informe sobre el proyecto de Reforma del Reglamento Hipotecario.

* El informe acerca del Plan para la formación de una Base de Datos Nacional del Catastro en relación a su inclusión en los Anteproyectos de Ley de Presupuestos Generales del Estado y de Medidas Fiscales.

* Informe sobre el Proyecto de Real Decreto por el que se aprueba el Reglamento por el que desarrolla el Título III de la Ley General de Telecomunicaciones.

* También merecen especial mención los informes relativos al proyecto de reforma de la Ley Orgánica 5/92 para adaptarla a la Directiva 95/46.

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 artículo 37 de la LO 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, y en los artículos 18 a 22 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia de Protección de Datos, se configura como órgano colegiado de asesoramiento del Director del Ente Público, cuyos cometidos se centran en emitir informe en todas las cuestiones que le someta el Director de la Agencia y formular propuestas en temas relacionados con las materias de competencia de ésta.
* En su composición, está integrada por los siguientes miembros:
* Presidente:
* D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos.
* Vocales:
* D. Carlos Navarrete Merino, Diputado propuesto por Congreso de los Diputados
* Dª. Rosa Vindel López, Senadora propuesta por el Senado
* D. Álvaro de la Cruz Gil, Vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias.
* D. Eloy Benito Ruano, Vocal propuesto por la Real Academia de Historia
* D. Antonio Pérez Prados, Vocal propuesto por el Consejo de Universidades.
* Dª. Nuria Díaz Anduiza, Vocal propuesto por el Consejo de Consumidores y Usuarios.
* Dª. Elena Gómez del Pozuelo, Vocal del sector de ficheros privados propuesta por el Consejo Superior de Cámaras de Comercio, Industria y Navegación.
* Secretaria:
* Dª. Sofía Perea Muñoz, Secretaria General de la Agencia de Protección de Datos.
* 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:
* Toma de posesión de los nuevos Vocales del Consejo Consultivo como consecuencia de su renovación por expiración del mandato del anterior Consejo.
* Planes de actuación de la Inspección de Datos y del Registro General de Protección de Datos a lo largo de 1998.
* Reunión en España de Autoridades de Protección de Datos XX Conferencia Internacional de Autoridades de Protección de Datos en Santiago de Compostela en septiembre de 1998, organizada por la Agencia de Protección de Datos.
* Convocatoria de la segunda edición del Premio Protección de Datos Personales, así como fallo del mismo.

* Transposición de la Directiva 95/46 CE y consiguiente reforma legislativa de la Ley Orgánica 5/ 92.
* Resultado de las inspecciones a las policías locales.
* Límites a la cesión de datos entre Administraciones en base al Padrón Municipal de Habitantes.
* Medidas a adoptar para una mayor publicidad y conocimiento de la ley y concienciación de la obligación de cumplirla.
* Códigos Tipo: Perspectivas de futuro.
* Inscripción de Ayuntamientos en el Registro General de Protección de Datos.

3 EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

3.1. INTRODUCCIÓN

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

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

La Ley ha desechado el establecimiento de la autorización previa a la inscripción constitutiva en un registro con la pretensión de evitar una perniciosa burocratización, por lo tanto, la inscripción en el Registro General de Protección de Datos es declarativa. Por otra parte, la consulta es pública y gratuita y serán objeto de inscripción en el mismo, tanto los ficheros automatizados de los que sean titulares las Administraciones Públicas, como los ficheros automatizados de titularidad privada, así 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 fichero, deberá efectuar una notificación para su inscripción en el Registro, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos.

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

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

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

3.2. LÍNEAS DE ACTUACIÓN

A lo largo del quinto 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 fluída, ya que el tiempo medio de respuesta desde que una notificación tiene entrada en el Registro hasta que se emite la correspondiente resolución de inscripción al responsable del fichero no supera los tres días de media. Dentro de las actividades propias del Registro se ha tramitado la inscripción de 3.253 nuevos ficheros, se han modificado 5.704 inscripciones y se han suprimido 1.234.

Las actuaciones puntuales del registro durante el año 1998, se han centrado en las siguientes grandes líneas de actuación:

3.2.1. NOTIFICACIÓN DE INSCRIPCIÓN Y ADAPTACIÓN A LA DIRECTIVA 95/46/CE

La Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, dispone en la sección IX del capítulo II las obligaciones relacionadas con la notificación de tratamientos.

En el artículo 18 se establecen los principios de la obligación de notificación a la autoridad de control. En este artículo se determina que los Estados miembros podrán disponer la simplificación o la omisión de la notificación en determinados casos y condiciones.

El artículo 19 de la Directiva establece la información que, como mínimo, debe figurar en la notificación, coincidiendo en todos los apartados con la prevista en el artículo 18 de la LORTAD. Además, en este artículo se determina que serán los Estados miembros los que precisarán los procedimientos por los que se notificará a la autoridad de control.

En el artículo 20 se determina que los Estados miembros precisarán los tratamientos que pueden suponer riesgos específicos para los derechos y libertades de los interesados y dispone que la autoridad de control los examine antes del comienzo de los mismos. En la ley española no está prevista la autorización previa en este tipo de tratamientos.

En el artículo 21 se expone el principio de publicidad de los tratamientos, y se determina que los Estados miembros establezcan que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18. Este aspecto coincide plenamente con lo dispuesto en la ley española en relación con el Registro General de Protección de Datos.

En este punto sería interesante hacer algunas consideraciones en relación con el concepto utilizado por la Directiva de *tratamiento* y el utilizado por la ley española de *fichero*.

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

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

Idéntica similitud de conceptos puede encontrarse en los modelos que al efecto se publicaron en la Resolución de 22 de junio de 1994, en el B.O.E. nº 149 de 23 de junio de 1994. Así, se puede observar que la denominación del cuestionario aparece como "MODELO DE NOTIFICACIÓN DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL" *Creación, Modificación y Supresión de ficheros.*

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

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

Por lo tanto, y en el escenario de la declaración de ficheros, a los efectos de publicidad de los mismos, se puede considerar que el concepto al que se refiere la Directiva en su artículo 21 de *Publicidad de los tratamientos,* es equiparable al concepto utilizado por la Ley española en su artículo 36.j) *Velar por la publicidad de la existencia de los ficheros automatizados.*

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

Además, se realizaron los siguientes análisis y estudios en relación con la obligación de notificación de tratamientos de datos personales al Registro General de Protección de Datos con la finalidad de determinar la adecuación de los modelos de notificación de ficheros actuales al contenido de las notificaciones de tratamientos de datos personales contemplados en la Directiva:

- Estudio del impacto de la Directiva en la notificación de ficheros de titularidad pública en el Registro General de Protección de Datos.
- Planificación, estudio, desarrollo e implantación de los sistemas de información necesarios para implantar las nuevas medidas legales.
- Posibilidad de instrumentalizar la notificación directa de ficheros vía Internet. Estudio de su legalidad y de los recursos tecnológicos necesarios.
- Estudio y planificación de la incidencia del Proyecto del Reglamento sobre seguridad en la notificación de tratamientos al Registro General de Protección de Datos

Como resultado de estos estudios se ha manifestado la necesidad de definir nuevos modelos de notificación de ficheros lo que implica el desarrollo de nuevas aplicaciones así como la adecuación de las actuales a las nuevas necesidades funcionales y legales. En el apartado 4 de este Capítulo se detallan con más precisión las nuevas necesidades.

3.2.2. INSCRIPCIONES SECTORIALES

El Director de la Agencia ha mantenido diversas reuniones con responsables de determinados sectores para el análisis de su situación específica en relación con la protección de datos personales, y concienciarles sobre las obligaciones y responsabilidades en esta materia, así como de la conveniencia de realizar códigos tipo.

Se pueden resaltar por su interés, las mantenidas con el Consejo General de Colegios Notariales y otros colectivos profesionales así como con los sectores de seguros, banca y marketing.

3.2.3. INSCRIPCIONES DE FICHEROS PÚBLICOS

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

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

- Revisión de la inscripción actual,
- Determinación de sistemas informáticos con datos personales que no han sido inscritos,
- Inscripción masiva de ficheros (Colegios, Hospitales, ...)
- Propuesta de elaboración y distribución de normas y recomendaciones para los usuarios y responsables de sistemas que utilicen ficheros con datos personales.

3.2.4. TRANSFERENCIAS INTERNACIONALES

Se ha analizado el impacto de la Directiva Europea de Protección de Datos en el concepto actual de Transferencia Internacional de Datos, así como las disposiciones que se deberían transponer a la ley española en lo relativo a las Transferencias Internacionales.

Las conclusiones que se han obtenido se detallan en el apartado de esta memoria sobre Transferencias Internacionales.

3.3. NOTIFICACIÓN DE FICHEROS: DERECHO NACIONAL APLICABLE (Artículo 4 y 18 Directiva 95/46/CE)

Con la entrada en vigor de la Directiva 95/46/CE en octubre de 1998, se han producido una serie de consultas y dudas de los responsables de ficheros en relación con la territorialidad de los mismos y su declaración a efectos de inscripción.

Es evidente que, los sistemas de tratamiento de datos deben estar al servicio del hombre; y por tanto, deben cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales y, en particular, la intimidad. La libre circulación de mercancías, personas, servicios y capitales, hace necesaria la libre circulación de datos personales y precisamente el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de datos.

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

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

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

El establecimiento, en territorio español, de una actividad que conlleve un tratamiento de datos, deberá cumplir las obligaciones impuestas por el Derecho español1.

El avance de las tecnologías implica, en estos momentos, la posibilidad de realizar tratamiento de datos2, sin que sea determinante la ubicación de los soportes informáticos (ficheros); por lo tanto, podrían quedar sin contenido los derechos de los ciudadanos ante un uso indebido en el tratamiento de sus datos.

Los procedimientos de notificación tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características y una de las funciones más importantes de la autoridad de control es contribuir a la transparencia de los tratamientos de datos efectuados en un estado miembro.

Por todo lo anterior, se considera necesaria la notificación a efectos de inscripción, en el Registro General de Protección de Datos, de los tratamientos de datos que se efectúen en un establecimiento en España que implique el ejercicio

efectivo y real de una actividad, con la finalidad de conseguir los siguientes objetivos:

- Transparencia de los tratamientos de datos.

- Identificación del responsable o representante en su caso.

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

- Garantizar al máximo los derechos de los ciudadanos ante un tratamiento de datos, que se verían seriamente mermados si tiene que ejercer sus derechos ante el responsable del fichero en otro país.

Las entidades domiciliadas en otro Estado miembro que traten datos en España, deberán cumplir, en los mismos términos que las entidades españolas, todos los preceptos de notificación que exija la Ley Orgánica 5/1992. Por lo tanto, tendrán que notificar la declaración de ficheros.

Será indiferente donde se encuentren ubicados los ficheros en los que se almacenan los datos. Únicamente, a efectos de inscripción, tendrán que declarar, en su caso, las transferencias internacionales que efectúen, así como la ubicación del fichero.

Las entidades domiciliadas en otro Estado miembro que pretenda tratar datos en España, vendrán obligadas a designar, con carácter previo al comienzo de sus actividad de tratamiento de datos personales en España, un representante o encargado del tratamiento (persona física o entidad establecida en España), para que les represente a los efectos del cumplimiento de las obligaciones de notificación al Registro General de Protección de Datos y de información en la recogida de datos y facilite los derechos de acceso, rectificación y cancelación a los ciudadanos.

Las entidades domiciliadas en terceros países que traten datos en España, deberán designar un representante establecido en España, que deberá comprometerse a aplicar y cumplir las disposiciones vigentes en protección de datos.

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

Los derechos de acceso, rectificación y cancelación serán facilitados por el representante establecido en España, para lo que deberá notificar, a efectos de inscripción, la dirección del establecimiento en España3, con la finalidad que el Registro General de Protección de Datos pueda proporcionar dicha dirección a los afectados cuando éstos la soliciten.

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

3.4. LA NECESIDAD DE ADECUAR EL SISTEMA DE INFORMACIÓN DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS PARA AFRONTAR EL "EFECTO 2000" Y LA ADAPTACIÓN A LA DIRECTIVA 95/46/CE

En la puesta en marcha del Registro General de Protección de Datos se desarrolló un sistema informático que permitiera inscribir, modificar, suprimir y consultar los asientos registrales de los ficheros automatizados con datos de carácter personal inscritos en el mismo.

La rápida evolución de los equipos informáticos hacia entornos Windows y el abandono de entornos DOS, así como el problema derivado de que esta aplicación sólo permite la introducción de fechas anteriores al año 2000, hace necesaria la modificación de este sistema de notificación de ficheros.

Por otra parte, la adecuación a la Directiva 95/46/CE conllevará la necesidad de modificar las aplicaciones del sistema de información del Registro para adaptarlo a las nuevas disposiciones legales.

Estos cambios legales obligarán a la modificación del contenido de la notificación de ficheros con datos personales.

Por otro lado, como la Agencia dispone de una página Web en Internet, que entre otra información incluye los modelos de formularios de declaración de ficheros, y siendo frecuente que los responsables de los mismos que consultan estas páginas, soliciten la declaración de ficheros a través de Internet, es por lo que se ha determinado la conveniencia de esta nueva forma de declarar ficheros.

Todo ello conllevará, a lo largo del próximo año, la necesidad de efectuar modificaciones de los modelos normalizados en soporte papel y magnético a través de los que deben efectuarse las correspondientes inscripciones en el Registro, tanto en su entorno tecnológico como en el contenido de las notificaciones de datos, siendo necesario:

- Modificación de los modelos de declaración de ficheros en soporte magnético, adaptándolos a los nuevos entornos Windows y eliminación del "Efecto 2000".
- Facilitar la declaración de ficheros vía Internet.

- Modificación de la estructura de la base de datos del Registro y de las aplicaciones de forma que permita la adaptación a los cambios que surjan de la transposición de la Directiva 95/46/CE.

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

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

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

El objetivo de este catálogo es dar publicidad de la existencia de los ficheros 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.

La primera publicación en soporte papel, correspondiente al año 1995, 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, para la publicación del catálogo correspondiente a 1997, se optó por continuar utilizando el soporte en CD-ROM, y se completó con la publicación del mismo en la red Internet. Asimismo, el ciudadano también puede pedir la información en soporte papel.

Los datos publicados en el soporte CD-ROM para el Catálogo 1998, 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.

- Finalidad y usos del fichero.

En la publicación en CD-ROM del Catálogo de ficheros 1998, se mantienen los criterios y facilidades de consulta 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, 1996 y 1997.

* 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.

* Utilización y control de datos laborales automatizados. Premio protección de datos 1997.
* Recomendaciones para usuarios de Internet.

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

Asimismo, se han publicado los modelos de declaración de ficheros en la página Web de la Agencia, facilitando de esta forma la obtención de los impresos establecidos como modelos normalizados en la Resolución de 22 de junio de 1994 publicada en el B.O.E. nº 149 de 23 de junio de 1994.

La publicación en Internet se incluye como una opción mas dentro de la Web institucional de la Agencia, donde se puede encontrar en primer lugar, información con carácter general. También se facilitan las instrucciones necesarias para inscribir nuevos ficheros en el Registro, pudiendo obtenerse el modelo normalizado de inscripción tanto de ficheros de titularidad pública, como de titularidad privada y el catálogo de ficheros propiamente dicho.

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.

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

Además, para los ficheros de titularidad pública se ha establecido una consulta que reproduce la estructura 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.

Del análisis de las estadísticas de acceso a la página web se observa un número creciente de accesos a la misma, con una media cercana a 20.000 accesos mensuales a las páginas.

De éstas, aproximadamente, el 20% corresponden a accesos a la información del Registro General de Protección de Datos, tanto a los apartados en que se indica la forma de realizar la declaración de ficheros, como a la consulta del Catálogo de ficheros o a los modelos de formularios para la declaración de los mismos. De ellos el 70%, acceden a la herramienta de consulta del catálogo de ficheros, bien sea a través de las pantallas de consulta general o a través de la consulta de búsqueda jerarquizada para los ficheros de titularidad pública. Otro 15% accede a los formularios de inscripción de ficheros.

El número de detallado de accesos, distribuido por meses, se recoge en el siguiente cuadro:

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
TOTAL ACCESOS PAGINA WEB AGENCIA	17.561	16.250	16.759	16.173	18.234	16.425	14.882	12.732	17.582	32.571	20.683	16.879
REGISTRO GENERAL PROTECCION DE DATOS	334	316	367	373	426	442	388	263	368	861	427	359
NORMAS INSCRIPCION FICHEROS	90	87	90	86	132	113	97	78	128	233	117	86
USO DE LA INFORMACION CONTENIDA	43	48	38	42	65	58	46	42	61	119	48	40
CONSULTA DE FICHEROS	2.171	2.123	2.176	2.364	2.771	2.562	1.901	1.548	2.077	4.303	2.065	2.054
FORMULARIOS	180	275	200	199	231	267	226	204	353	521	350	259
FORMULARIOS DE TITULARIDAD PRIVADA	103	123	104	130	156	174	154	108	180	342	230	174
FORMULARIOS DE TITULARIDAD PUBLICA	53	52	44	40	60	37	40	40	67	101	93	67

3.6. FICHEROS DE TITULARIDAD PRIVADA

3.6.1. EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN

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

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

3.6.1.1. Inscripción de ficheros

** Cifras generales.*

A lo largo de 1998 se han tramitado 2.296 solicitudes de inscripción de ficheros de titularidad privada, de las que se han derivado al final del ejercicio 2.281 ficheros, lo que supone un 1,1 % de las 203.138 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 1998 con las 1.760 altas de 1997, 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 en relación con los primeros años de inscripción. Este resultado es lógico 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.

En el último año se ha producido un aumento en la inscripción respecto al año anterior, originado en parte por el progresivo aumento del conocimiento de la Ley, que tienen los responsables de ficheros, debido a las campañas de información que la propia Agencia de Protección de Datos realiza y en parte a la coyuntura económica favorable a la creación de nuevas empresas.

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

Por otra parte, el número de entidades que ha solicitado inscribir ficheros en 1998 es de 1.150, lo que supone una media de inscripción de prácticamente dos ficheros por empresa, cifra que coincide con la relativa a 1997, 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 61,5% de las operaciones de alta de ficheros privados del año 1998 se ha notificado en soporte magnético, con lo que la tendencia a utilizar este tipo de sistema sigue siendo superior al modelo del cuestionario en soporte papel, al igual que en años anteriores (en 1997 el porcentaje de operaciones de alta por disquete fue del 57, 6%, en 1996 fue del 53,6%, en 1995 fue del 76,2% y en 1994 fue del 56,1%). La tendencia a utilizar como modelo de notificación el soporte magnético más que el soporte papel, es una característica que se mantiene a lo largo del tiempo.

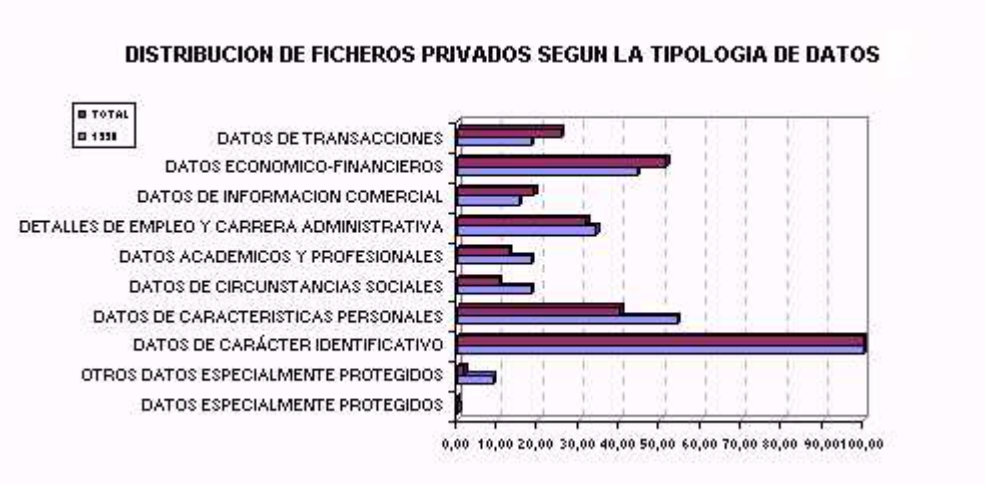
En cuanto a este punto, la evolución de la tecnología con la aparición de nuevos sistemas operativos, así como el efecto 2000, han provocado la obsolescencia de la aplicación actual, lo que hace necesario un nuevo modelo que permita realizar las notificaciones en soporte magnético y a través de Internet. Esta aplicación estará operativa en el año 1999 solucionando los problemas anteriormente citados.

* Tipos de datos.

En cuanto a la tipología de datos declarados en los ficheros privados inscritos en el ejercicio de 1998, aparte de los datos de carácter identificativo que aparecen lógicamente en el 100% de la inscripción, predominan los datos de características personales (54,2% de la inscripción) y los económico-financieros (44,4% de la inscripción), seguidos de los datos de detalles de empleo (34,3%), los de circunstancias sociales (18,3%), los académicos y profesionales (18, 3%), los de transacciones (18,2%) y los de información comercial (15,3%). En una escala inferior (9%) se encuentran las declaraciones de ficheros que contienen datos de salud, vida sexual y origen racial, encuadrados bajo la denominación de "otros datos especialmente protegidos". Por último los "datos especialmente protegidos" de ideología, creencias y religión afectan a un 0,4% de la inscripción del ejercicio.

Si analizamos los datos sobre tipología de todos los ficheros que se encuentran inscritos en el Registro, se obtienen resultados similares (el 51,3% han declarado datos económico financieros, el 40,2% datos de características personales, el 31,7% datos de características de empleo, el 25,5% datos de transacciones, el 19% datos de información comercial, el 12,7% datos académicos y profesionales, el 10,3% datos de circunstancias sociales, el 1,7% otros datos especialmente protegidos y el 0,15% datos especialmente protegidos).

En la gráfica siguiente se comparan los datos sobre tipología en la inscripción total de ficheros con los relativos al año 1998 observándose una tendencia similar, excepto en la declaración de ficheros que contienen datos de salud, vida sexual y origen racial, significativamente más alta este año por las razones que se analizan en el siguiente apartado.



** Datos especialmente protegidos.*

Respecto a los datos especialmente protegidos relativos al apartado 1 del artículo 7 (ideología, creencias o religión), se han inscrito seis ficheros que declaran datos de ideología, un fichero con datos de creencias y cuatro ficheros con datos de religión. Los ficheros que declaran datos de ideología son los que contienen información relativa a la afiliación sindical de los empleados de las empresas, información que 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.

Los ficheros que declaran datos de religión tienen como finalidad la gestión automatizada de la declaración del Impuesto sobre la Renta de las Personas Físicas, y señalan 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. Asimismo, contempla datos de religión un fichero inscrito por Cruz Roja Española cuya finalidad es la atención social a inmigrantes para la tramitación de la solicitud de asilo o refugio y para la regularización de su situación documental en España. Se declaró también un fichero con datos de ideología, creencias y religión correspondiente a un archivo que contiene información sobre investigación histórica relativa a la Guerra Carlista.

En relación a los datos de salud, origen racial y vida sexual enumerados en el artículo 7.3 de la Ley, se observa un incremento en la declaración de ficheros que contienen este tipo de datos. Se han inscrito 202 ficheros que declaran datos de salud, correspondiendo una parte considerable de los mismos a ficheros cuya finalidad es la gestión de recursos humanos de empresas que mantienen políticas de prevención de riesgos laborales y vigilancia de la salud de sus trabajadores. También incluyen datos de salud los ficheros de entidades del sector asegurador que ofrecen seguros de vida y salud o que gestionan pólizas de asistencia sanitaria o decesos.

Así mismo, responsables del sector sanitario, como hospitales, clínicas y médicos declaran 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 tratan este tipo de datos con la finalidad de realizar ensayos clínicos. También declaran datos de salud asociaciones y entidades cuya actividad es la prestación de servicios sociales.

Mención aparte merecen los ficheros que contienen datos de salud con la finalidad de la atención farmacéutica y seguimiento del uso de medicamentos, cuya inscripción se ha derivado del proyecto TOMCOR (Treatment Out Maintenance Coronary) y que ha influido decisivamente en el aumento de este tipo de datos en la inscripción de 1998.

Prácticamente un tercio de la inscripción total de ficheros con datos de salud declarada durante el año 1998 proviene de responsables del sector farmacéutico adscritos a este proyecto. TOMCOR es un proyecto de investigación cuya finalidad consiste en realizar un seguimiento de productos farmacéuticos en enfermos coronarios. El proyecto está financiado por la Asociación Red Española de Atención Primaria (REAP), asociación sin ánimo de lucro, que se dedica a fomentar y financiar proyectos de investigación en las áreas de Farmacia y Medicina. Para la ejecución del proyecto la REAP ha dotado de una aplicación informática a un grupo de oficinas farmacéuticas colaboradoras con el proyecto. Estas farmacias envían a la REAP periódicamente la información sobre los medicamentos que se suministran a los pacientes donde se centraliza la información del colectivo en estudio. En estos ficheros, se declaran los datos de salud amparándose en el consentimiento expreso del afectado.

Por otra parte, existen dos ficheros notificados en 1998 que declaran datos de origen racial, uno de los cuales refleja como finalidad la atención social a inmigrantes y el otro contiene datos demográficos y analíticos de personas participantes en ensayos clínicos. Dado lo sensible de estos datos, se requirió a los responsables para que justificaran y

aclararan la necesidad del tratamiento automatizado de estos datos. En el primero de los casos, nos informaron que su finalidad era la de atención social a la inmigración con el objeto de tramitar la solicitud de asilo o refugio y la consiguiente regularización de su situación en España. En el segundo de los casos, la finalidad del fichero declarado es la creación de una base de datos de voluntarios para investigación científica, el responsable del fichero justificó el tratamiento del dato de *origen racial*, en razón a la necesidad descrita en los protocolos de investigación dado que hay distintos polimorfismos genéticos en las distintas razas, lo que conlleva un distinto comportamiento del organismo tras la toma de determinados fármacos, pudiendo influir también en los resultados, el régimen dietético y otros hábitos de ciertas culturas. Se han inscrito también seis ficheros que consignan el tipo de datos relativos a *vida sexual* amparándose en las finalidades de investigaciones científicas y médicas e historial clínico.

No se procedió a la inscripción en un caso que se notificaban *otros datos especialmente protegidos* de vida sexual en un fichero del sector asegurador, cuya finalidad era el control y la gestión de la cartera de seguros. Se requirió al responsable del fichero para que aclarara la necesidad del tratamiento de este dato comunicándose la decisión de no grabar ni tratar este tipo de datos, dado que podría suponer un acto de discriminación.

Por imperativo legal 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. En todo caso, los responsables de los ficheros que declaran cualquier tipo de dato especialmente protegido son requeridos para que justifiquen y aclaren la necesidad del tratamiento de los mismos y su adecuación a los usos y fines legítimos de los ficheros.

** Finalidades y usos*

En cuanto a los usos declarados en los ficheros inscritos en 1998 destacan aquellos que declaran como finalidad del tratamiento *la gestión contable, fiscal y administrativa* (33%), *la gestión de clientes* (30%), *obtención de estadísticas diversas* (28%), *gestión de cobros y pagos* (25,6%), *publicidad propia* (22,7%), *gestión de personal* (21,2%), *seguridad y control interno* (13,6%), *históricos de relaciones comerciales* (13,5%), *prospecciones de mercado* (10,2%), *encuestas de opinión* (6,8%), *selección de personal* (6,1%) *y publicidad para terceros* (5,7%). Estas cifras ponen de manifiesto el aumento continuado de creación de ficheros cuya finalidad declarada es la contabilidad, gestión de cobros y pagos, gestión de clientes, fiscalidad, gestión de personal y nóminas. Estas cifras son lógicas ya que la mayoría de las entidades están informatizando la gestión interna de la empresa.

Hay finalidades como la *solvencia patrimonial y el crédito* que presentan un descenso considerable respecto a años anteriores debido a la consolidación del sector.

En cuanto a las finalidades y usos referidos a la inscripción total de ficheros predominan aquellos que han declarado como finalidad la gestión contable, fiscal y administrativa (65,6%), la gestión de cobros y pagos (43,2)%, la gestión de clientes (31,6%), la obtención de estadísticas diversas (26,8%), la gestión de personal (26,1%), históricos de relaciones comerciales (15,7%), publicidad propia (9,6%), asesorías y servicios relacionados (6,6%), seguridad y control interno (5%) y prospecciones de mercado (3,4%). Si comparamos la inscripción por finalidades de los ficheros notificados durante el año 1998 con la inscripción total por finalidades en la base de datos, se observa un aumento significativo en la finalidad de selección de personal, debido en su mayor parte a las declaraciones de inscripción de ficheros por parte de las empresas de trabajo temporal. También experimenta un aumento significativo la finalidad de seguridad y control interno, debido a la tendencia actual de utilizar este tipo de servicios, que implica la declaración de ficheros realizados desde este sector. También ha influido la declaración del sector de Actividades Recreativas tales como Salas de Bingo o Casinos, que declaran los ficheros de acceso, amparándose en el Reglamento de Casinos y Juegos de las distintas Comunidades Autónomas.

Mención aparte merece el aumento que presentan en el año 1998 las declaraciones de inscripción de ficheros con finalidades de encuestas de opinión, prospección de mercado, publicidad propia y publicidad para terceros. Este aumento puede estar basado en el desarrollo de nuevas técnicas en el ámbito del tratamiento de la información como, *datawarehouse*, *data mining*, *data mart*, *sistemas de ayuda a la decisión (DSS)*, etc., relacionadas con los sistemas de ayuda a la dirección y que pretenden ofrecer soluciones en los procesos de negocio para la toma de decisiones en general y en el ámbito del marketing en particular. Estas técnicas surgen por la necesidad de hacer más operativa la enorme cantidad de información almacenada en distintas bases de datos.

El desarrollo de las nuevas tecnologías de la información, aplicadas al marketing, están comenzando a introducirse en nuestro país, lo que exigirá analizar su incidencia en la intimidad.

Desde la perspectiva de la Agencia de Protección de Datos, es importante en primer lugar, que el ciudadano tenga conocimiento de la existencia de estas nuevas técnicas a la hora de proporcionar sus datos y el consentimiento para su utilización en los principios que especialmente protege la LORTAD, sobre todo el principio de finalidad que podría resultar conculcado con el uso de estas técnicas.

La Agencia de Protección de Datos ha tomado conciencia de su irrupción en el marcado español y permanece vigilante ante el mal uso potencial en el que se podría incurrir en el tratamiento de datos de carácter personal.

A continuación, se definen brevemente en concreto las técnicas en las que se basan estos tratamientos automatizados:

- *datawarehouse*: con este nombre se aglutinan una serie de diseños de bases de datos que tienen en común que son una agrupación de un gran volumen de datos. Estos datos provienen de diversas áreas funcionales de la empresa y pueden guardar datos históricos y/o acumulados para facilitar una determinada consulta. Pueden tener un grado mayor o menor de desfase con respecto a los sistemas on-line. Estos diseños de datos pueden realizarse una vez que el usuario conoce el tipo de consulta que va a realizar o puede que se realice sin conocer lo que se va a pedir, con lo cual se convierte en un gran almacén de datos para su posterior consulta.

- *data mining:* se basa en el uso de los algoritmos estadísticos de análisis multivariante para descubrir sutiles relaciones, o relaciones ocultas entre elementos que constituyen la información de las bases datos, así como la generación de modelos predictivos basados en ellos. En lo relativo al marketing, las técnicas de *data mining* derivan en un marketing inteligente aplicado al cliente individual que tiene como finalidad esencial el adquirir una visión integral del mismo en todas sus facetas (económica, de relación con la entidad, perfil socioeconómico, historia detallada, entorno, etc.) y desde un gran número de perspectivas. En particular, la técnica de *redes neuronales*, puede identificar los patrones de comportamiento de los clientes a partir de complejas interacciones entre variables de cuya información se dispone en las bases de datos, permitiendo extraer la información de las mismas de forma dirigida, construir muestras y analizarlas, y finalizado el proceso, extender los resultados a toda la base de datos en tiempos muy cortos. Una vez identificados perfiles y patrones de comportamiento, se puede realizar publicidad dirigida y marketing inteligente en general.

- data mart: diccionario de datos al que acceden los usuarios finales y contiene información correspondiente a una sola área o un solo tema funcional de una empresa.

- *sistemas DSS* (Decision Support Solutions): término general que describe aplicaciones para el análisis de grandes cantidades de datos y la realización de gran variedad de cálculo y proyecciones.

* Origen y procedencia de los datos

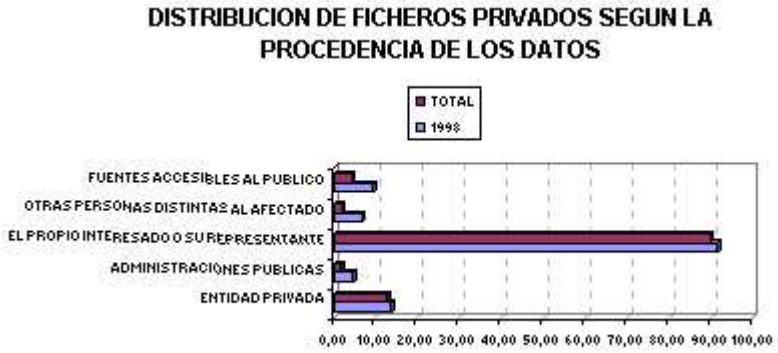
En cuanto a la procedencia de los datos declarados en los ficheros inscritos en 1998, destacan aquellos que declaran que los datos grabados en sus ficheros provienen del propio interesado o su representante legal (91,5% de los ficheros declarados), seguido de aquellos que declaran el origen a través de entidades privadas (13,6%), fuentes accesibles al público (9,3%), otras personas distintas del afectado o su representante legal (6,8%) y administraciones públicas (4,7%).

En la mayoría de los casos es el propio interesado el que aporta la información, lo cual concuerda con la elevada cifra de ficheros inscritos cuya finalidad declarada puede estar amparada en la existencia de una relación contractual que implica necesariamente que el dato lo aporte el propio interesado; tal sería el caso de la gestión de la contabilidad, fiscalidad, gestión de personal y nóminas constatados en el apartado anterior.

Por otra parte, la cifra referente a la procedencia de los datos de las *administraciones públicas* 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.

Si analizamos la información de todos los ficheros inscritos en relación a este apartado, nos encontramos que el (90% de ficheros declaran como procedencia de sus datos el propio interesado o su representante legal. El 12,6% que proceden de entidades privadas, el 4,4% que proceden de fuentes accesibles al público, 2% de otras personas distintas del afectado o su representante y 1,7% que su origen estaría en las Administraciones Públicas). Se observa en los años 1997 y 1998 un aumento significativo de los ficheros que declaran como origen de sus datos la procedencia de fuentes accesibles al público, de Administraciones Públicas y de otras personas distintas del afectado, originado posiblemente por la utilización creciente de las bases de datos accesibles al público en Internet. Así mismo, se puede observar, que para el resto de apartados de procedencia de los datos, las cifras que se recogen del año 1998 son bastante coinci - dentes con las cifras de las inscripciones que configuran el Registro.

El gráfico siguiente presenta las cifras de inscripción total en el Registro en relación con la procedencia de los datos y las compara con las relativas al año 1998.



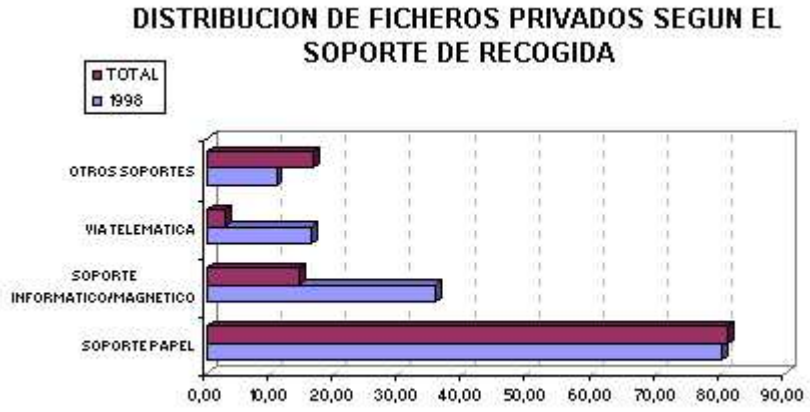
** Soporte utilizado en la recogida de los datos*

El 80% de los ficheros que se han notificado al Registro durante el año 1998, declaran que el soporte utilizado en la recogida de los datos ha sido a través de cuestionarios y métodos convencionales.

Los datos que se han grabado o recogido directamente en soportes tecnológicos (directamente desde el teclado del ordenador o a través de medios telemáticos) alcanzan la cifra del 35,6% los primeros y el 16,2% los segundos.

Si analizamos todos los datos de los ficheros que constan inscritos en el registro y comparamos con las cifras de este año, destaca el aumento durante los años 1997 y 1998 de las nuevas tecnologías en la recogida de los datos. Esto es debido sobre todo a la fuerte incidencia de nuevos medios de acceso a la información, como es el caso de la red Internet, lo que también está en consonancia con los datos reflejados en el apartado anterior.

El gráfico siguiente presenta las cifras de inscripción total según el soporte de recogida de los datos y las compara con las relativas al año 1998.



** Procedimiento de recogida.*

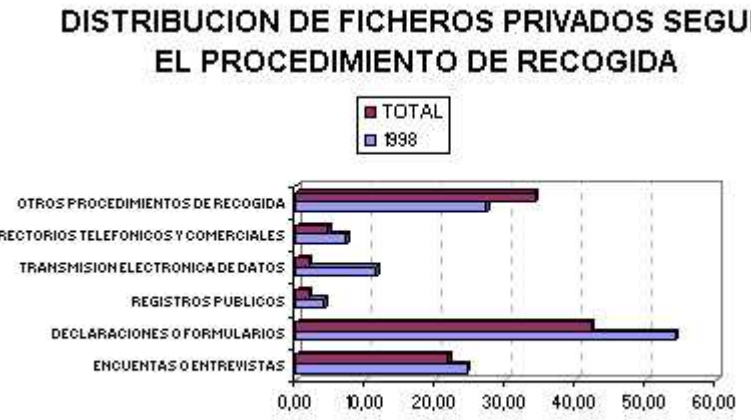
En cuanto al procedimiento de recogida de los datos de los ficheros inscritos en 1998 predominan aquellos que consignan como medio de recogida las *declaraciones o formularios* (54,2%) seguido de *encuestas o entrevistas* (24, 4%), *transmisión electrónica de datos* (11,3%), *directorios telefónicos y comerciales* (7,2%) y *registros públicos* (4%) y *otros procedimientos de recogida* (27,6%). 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 cuando se consigna *el propio interesado*, ya que los datos de los ficheros de contabilidad, fiscalidad, gestión de personal y nóminas, que son los predominantes, suelen recogerse inicialmente en formularios en papel o mediante entrevista directa con el afectado. En relación a la comparación con los datos totales del Registro se puede resaltar

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

El apartado *"otros procedimientos de recogida"* engloba distintos procedimientos de obtención de información que no están normalizados en el modelo de notificación de ficheros. En este apartado se contemplan distintas formas de obtención de datos, en la mayoría de los casos facilitados por el propio interesado, pero a través de nuevos medios de captación de la información, como los cupones respuesta y testigos de compra, catálogos y cuestionarios, campañas publicitarias, "buzoneo", recogida de currículos, encuestas telefónicas, fax, sistemas audiotext. Alguno de estos procedimientos a su vez implica la utilización de las nuevas tecnologías como medios de transporte.

Si analizamos los datos de procedimiento de recogida referidos a la inscripción total el 42,1% del total de ficheros declaran que los datos se han recogido con procedimientos que implican rellenar declaraciones o formularios. El 34,1% no especifica los procedimientos de recogida. El 21,7% a través de encuestas o entrevistas, 4,5% de directorios telefónicos, comerciales, catálogos y memorias, 1,9% de registros públicos y 1,8% de transmisión electrónica de datos y compararlos con los relativos a 1998, 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, datos que están en línea con las cifras de los apartados anteriores.

El gráfico siguiente presenta las cifras de inscripción total según el procedimiento de recogida de los datos y las compara con las relativas al año 1998.



** Cesiones de datos.*

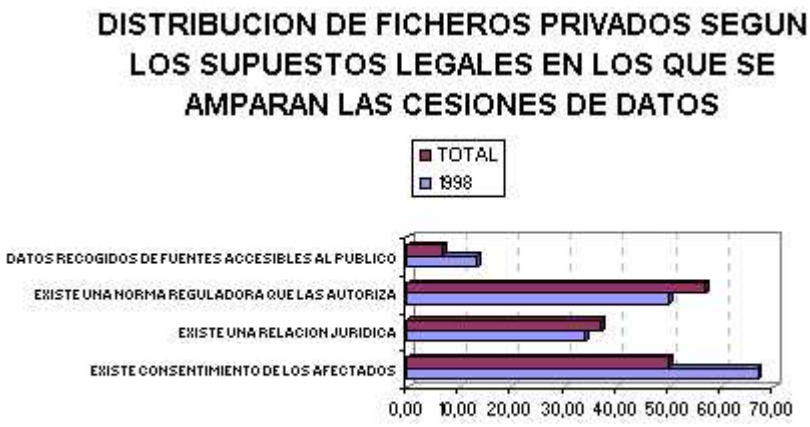
En cuanto a las cesiones de datos, en 1998 se han inscrito 649 ficheros que declaran este apartado, lo que supone un 28,4% del total de ficheros inscritos en el ejercicio. El mayor porcentaje de cesiones se justifican por la existencia del consentimiento de los afectados (66,8% del total de ficheros inscritos con cesiones en el ejercicio), seguido por la existencia de una norma reguladora que las autoriza (49,7%), la existencia de una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros (33,7%) y los que realizan la cesión amparándose en que los datos cedidos fueron recogidos de fuentes accesibles al público (13,2%).

El consentimiento de los afectados como justificación de la cesión se refleja en ficheros de gestión de clientes, históricos de relaciones comerciales y publicidad a los propios clientes. 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 consonancia 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, envíos de publicidad, prospección de mercados y fines relacionados con este sector de actividad.

En cuanto a las cifras referentes a la inscripción total de ficheros y relativas a los supuestos legales en los que se amparan las cesiones de datos, el 56,7% del total de ficheros inscritos con cesiones las justifican por la existencia de una norma reguladora que las autoriza, el 49,8% se basan en el consentimiento de los afectados, el 36,9% las justifican por la existencia de una relación jurídica que implica 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 de cesiones declaradas en el total de la inscripción con las cifras de ficheros que declaran cesiones durante el año 1998, distribuyendo los ficheros entre los supuestos legales en los que se amparan. En este gráfico se observa un aumento de cesiones amparadas en fuentes accesibles al público durante el año 1998, lo que está en consonancia con el aumento de la inscripción de ficheros que declaran finalidades relacionadas con la publicidad y el marketing durante ese año. También se observa un aumento de las cesiones declaradas con consenti - miento del afectado motivado por el mayor conocimiento y cumplimiento de la LORTAD por parte de los responsables en lo referente a cesiones de datos.



** Inscripción de ficheros privados por ámbito geográfico.*

En cuanto a la distribución geográfica de las cifras de inscripción de ficheros más representativas durante el año 1998 por Comunidades Autónomas, se observa que la Comunidad de Madrid ha inscrito el 41% del total de ficheros del ejercicio, seguida de Cataluña con una inscripción del 27,3% del total, Andalucía el 6%, Comunidad Valenciana el 4, 5%, País Vasco el 4%, Aragón el 3,7%, Extremadura el 3,6% y Principado de Asturias con el 2,6%.

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 de estas dos comunidades son muy semejantes en los dos últimos años e indican una posible evolución paralela en el tiempo.

El gráfico siguiente muestra las cifras de inscripción de ficheros durante el año 1998 por Comunidades Autónomas.

Si comparamos las cifras de inscripción de ficheros por Comunidades Autónomas con la inscripción total del Registro y la declarada en 1998, se observa un cierto paralelismo, excepto en el aumento de inscripción en los últimos años en Madrid (aumento que se ha acentuado desde 1996) y Extremadura y Principado de Asturias y la disminución en la declaración de Comunidades como la Valenciana, Gallega y Castilla-León debido al elevado número de notificaciones

presentadas en los años anteriores.

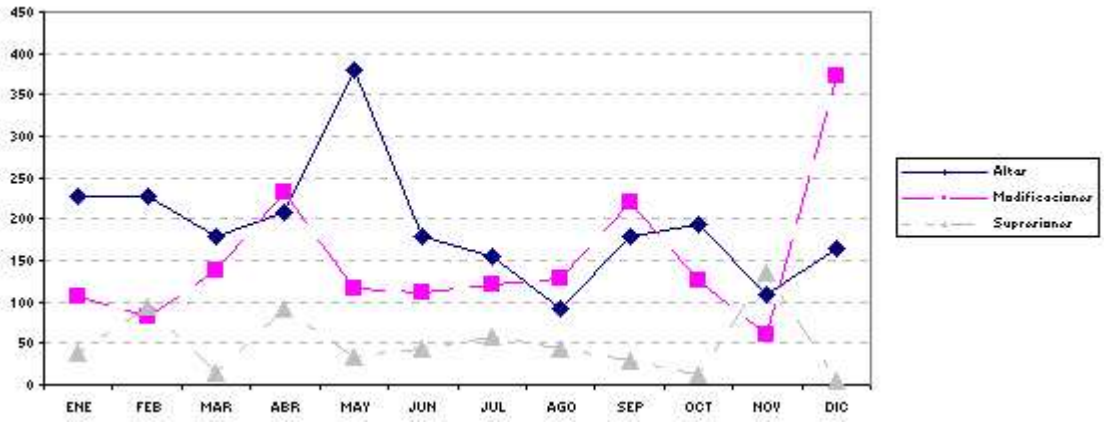
** Distribución temporal de la inscripción.*

En cuanto a la distribución temporal de la inscripción en 1998, se observa que la mayoría de los meses presentan cifras similares, salvo Agosto que contempla la cifra más baja y Mayo que contempla la más alta. Puede constatarse que las épocas de mayor inscripción son el segundo y último trimestres del año, seguido del primer trimestre que también presenta cifras altas. En el tercer trimestre se nota una bajada acentuada en la inscripción. 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 requerimientos que realiza la propia Agencia demandando información a determinados sectores.

Resumen de operaciones realizadas durante 1998 sobre ficheros de titularidad privada inscritos en el RGPD
(A solicitud del responsable del fichero)

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
ALTAS	228	227	178	208	381	178	156	93	180	194	108	165	2.296
MODIFICACIONES	106	82	137	232	117	112	122	129	221	126	60	373	1.817
SUPRESIONES	39	95	14	93	33	44	57	43	30	12	136	4	600
TOTAL	373	404	329	533	531	334	335	265	431	332	304	542	4.713



** Inscripción por Sectores Económicos.*

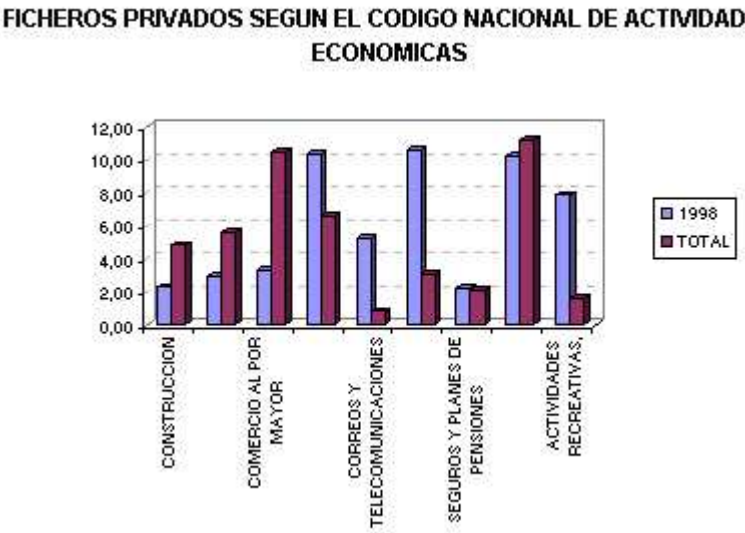
En cuanto a la inscripción de ficheros en el año 1998 por sectores económicos de actividad, predomina el sector de la *intermediación financiera* con un 10,6% del total de ficheros inscritos en el ejercicio. Le siguen el *comercio al por menor* con un 10,3%, *otras actividades empresariales* (que incluye las actividades jurídicas, de contabilidad, auditoría, asesoría fiscal, estudios de mercado, encuestas de opinión y asesoramiento sobre dirección y gestión empresarial) con un 10,3%, las *actividades recreativas, culturales* y *deportivas* con un 8%, *telecomunicaciones* con un 5,3%, las actividades de *edición*, *artes gráficas* y *reproducción de soportes grabados* con un 4,5%, *el comercio al por mayor* e *intermediarios del comercio* con un 3,2%, la *industria de productos alimenticios* y *bebidas* con un 3,1% y las actividades de *venta, reparación* y *mantenimiento de vehículos de motor* , con un 3% .

Estos datos se resumen en el gráfico siguiente:

En cuanto a la inscripción total de ficheros en el Registro General de Protección de Datos por sectores económicos de actividad, predominan los sectores encuadrados en el título de *otras actividades empresariales* con un 11,2 % del total de ficheros inscritos y el *comercio al por mayor e intermediarios* del comercio con un 10,5%.

Le sigue el *comercio al por meno*r con un 6,5%, las actividades de venta, reparación y mantenimiento de vehículos de motor con un 5,6%, la construcción con un 4,8%, la intermediación financiera con un 3%, la industria de productos alimenticios y bebidas con un 2,9%, los seguros y planes de pensiones con un 2%, las actividades de edición, artes gráficas y reproducción de soportes grabados con un 1,9% y las actividades recreativas, culturales y deportivas con un 1,6%. Estos datos se reflejan en el siguiente gráfico.

Si comparamos las cifras de inscripción por Sectores Económicos para la inscripción total y la de 1998, se observa un aumento de la inscripción en el último año en los sectores de intermediación financiera, actividades recreativas, culturales y deportivas, telecomunicaciones y actividades de edición, artes gráficas y reproducción de soportes grabados. 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 inscripción en los sectores de las telecomunicaciones debido a la liberalización de mercado y la edición y reproducción de soportes grabados puede deberse al desarrollo continuo de estas ramas de actividad en la actualidad derivado del aumento de uso de la red Internet, de los soportes ópticos y de otros avances de las nuevas tecnologías de la información y la comunicación. La gráfica siguiente presenta la comparativa de las cifras de inscripción de ficheros por Sectores Económicos para la inscripción total y la de 1998.



3.6.1.2. Modificación de inscripción de ficheros

Se han modificado, a solicitud del responsable, mediante recepción de notificación en tal sentido (en soporte papel o en disquete), un total de 1.816 inscripciones de 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 (70%), mientras que el 30% restante solicitó la modificación a efectos de inscripción en soporte magnético.

Las cifras de modificaciones de los dos últimos años son inferiores a las 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 declarantes a medida que aumenta su difusión y su puesta en práctica. No obstante, la cifra de modificaciones realizadas durante 1998 supera a la de 1997, hecho que está en línea con el ya citado aumento de las notificaciones de altas que se ha produ-

cido en este ejercicio.

El porcentaje más alto de modificaciones son aquellas que están relacionadas con los cambio que se producen en las entidades. Estos cambios suelen estar relacionados con los avances tecnológicos y la actualización de los sistemas de información, cambios de denominación social o forma jurídica.

El siguiente gráfico refleja la evolución de las operaciones solicitadas por los responsables para modificar la inscripción de sus ficheros.

En cuanto a las cifras de modificaciones relativas a la inscripción total de ficheros en el Registro General de Protección de Datos, se han modificado hasta la fecha 15.818 inscripciones de ficheros, lo que supone el 7,8% del total de los ficheros inscritos en el Registro General de Protección de Datos. El 84,6% de las modificaciones se han solicitado en soporte papel, y el 15,4% restante, en soporte magnético.

Se observa que, el apartado que ha sufrido mayores modificaciones como consecuencia de errores producidos en la notificación de ficheros, ha sido el de cesiones, quizá se deba a la dificultad que supone la interpretación de los supuestos legales que amparan las cesiones de datos a terceros o por las dificultades que en la práctica supone 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 el modelo de los formularios, o bien por la dificultad de plasmar en la notificación la procedencia real de los datos que originan los ficheros automatizados. En el apartado de responsable se producen errores materiales en relación al Código de Identificación Fiscal y en el Código Nacional de Actividad Económica (CNAE).

La Agencia de Protección de Datos es consciente de estas deficiencias que no se aprecian en una primera lectura de la Ley. La experiencia obtenida de los primeros años de aplicación de la LORTAD obliga a la Agencia, en primer lugar, a corregir estos comportamientos, y, en su caso a sancionar las conductas que conculquen los principios de la LORTAD.

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

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

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

Otro 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 la denominación de la razón social. En estos casos, además de producirse 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 informarles de las exigencias legales que en estos casos debe cumplir el responsable del fichero, en particular, sobre la comunicación de la identidad del nuevo responsable a los afectados.

3.6.1.3. Supresión de ficheros

El artículo 24 apartado 3 de la Ley Orgánica 5/1992 y el artículo 8 apartado 2 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley en relación a la 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, dispone que se deberá comunicar la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

Durante el año 1998 se han realizado 600 operaciones de supresión de inscripción de ficheros a petición de sus responsables, lo que supone un 0,3% del total de los ficheros de titularidad privada inscritos 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 (75%), mientras que el 15% 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 de supresiones referidas al total de la inscripción de ficheros en el Registro General de Protección de Datos, se han suprimido hasta la fecha 3.522 inscripciones de ficheros a petición de los responsables, lo que supone un 1,7% de la inscripción total. En cuanto a la evolución en el tiempo, el 17% de las supresiones se han realizado durante el año 1998, el 44,6% se han realizado en 1997, el 5,6% se realizaron en 1996, el 26% se han realizaron en 1995 y el 6,8% restante se realizó en 1994.

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

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

- En primer lugar, se producen casos de **bajas, disoluciones o ceses de actividad de las empresas**, que conllevan una destrucción física de los ficheros con datos personales. En estos casos, se solicita al responsable que garantice las medidas de destrucción y aclaren las circunstancias por las que se ha tomado la decisión de destruir el fichero. Además, se anota, a efectos de información 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 de la Ley. Además, en el caso de la absorción, se comprueba la inscripción anterior de la empresa absorbente y en los asientos de supresión se reflejan los códigos de inscripción de los nuevos ficheros que van a contener la información de los suprimidos. En el caso de la fusión de empresas, es 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 supresiones de inscripción con el fin de subsanar un error en la interpretación de la norma, en relación con el encargo a terceros, de la gestión de los servicios de tratamiento informático. En este caso, surge la figura definida en la Directiva 95/46/CE, como "encargado del tratamiento" 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 actualizar los apartados de ubicación de los ficheros y sistemas de tratamiento.

3.6.2. 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 1998 se han realizado un número de operaciones de oficio que han afectado a un total de 2.323 inscripciones de ficheros, lo que supone más de un 1% del total de ficheros inscritos en el Registro. El 76,7% de las operaciones de oficio corresponden a modificaciones de los asientos y un 23,2% a cancelaciones o supresiones de inscripciones debidas a la depuración de inscripciones duplicadas.

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

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

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

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

3.6.2.1. Depuración de inscripciones duplicadas

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

El procedimiento establecido para realizar esta depuración ha consistido en seleccionar 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 537 inscripciones de

ficheros duplicados durante el año 1998.

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

Existen responsables de ficheros que debido a la distribución geográfica de su actividad, tienen distintas delegaciones en el territorio nacional y en cada una de ellas tienen ubicados ficheros, que en lo único que se diferencian, es en el colectivo de personas que se almacenan en los mismos. Tal es el caso de las grandes superficies, las empresas de grandes dimensiones y en general las empresas con numerosas sucursales en distintas provincias de España. En estos casos, el responsable de los ficheros es único y la dirección de acceso, rectificación y cancelación también suele ser única y centralizada. Sin embargo un mismo fichero presenta distintas ubicaciones físicas, en general tantas como sucursales o centros de actividad distintos posea el responsable. Debido a estas circunstancias, existen inscripciones de ficheros del mismo responsable y con el mismo nombre, pero con ubicación física distinta, que inicialmente pueden confundirse con ficheros duplicados. En estos casos, se ha subsanado de oficio y de forma normalizada la denominación del nombre y descripción de los ficheros incluyendo, adicionalmente a la denominación, el nombre de la localidad o bien el nombre de la sucursal o delegación donde se ubican. Este proceso de depuración se ha realizado en 735 inscripciones de ficheros.

3.6.2.3. Depuración de denominaciones de responsables

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

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

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

Si añadimos las circunstancias anteriores a la declaración errónea del Código Nacional de Actividad Económica, se obtiene como resultado que un porcentaje alto de notificaciones de todo tipo enviadas al Registro General de Protección de Datos implican asientos registrales de oficio o, en caso de duda, requerimientos de subsanación al responsable.

3.6.2.4. Depuración denominación de provincias

Como consecuencia de la publicación en el B.O.E de la Ley 2/1998, de 3 de marzo, sobre el cambio de denominación de las provincias de La Coruña y Orense, pasando a denominarse A Coruña y Ourense, respectivamente se procede a realizar la modificación de oficio en la inscripción de los ficheros, de las denominaciones de localidad y provincia de los apartados de responsable (tanto público como privado), acceso, ubicación y declarante, afectando las modificaciones al siguiente número de ficheros:

LOCALIDAD	RESPONSABLE PRIVADO	RESPONSABLE PUBLICO	ACCESO	UBICACION	DECLARANTE
A CORUÑA					
T O T A L	**2.011**	**36**	**852**	**1.256**	**2.311**
OURENSE					
T O T A L	**10**	**9**	**3**	**270**	**628**

PROVINCIA	RESPONSABLE PRIVADO	RESPONSABLE PUBLICO	ACCESO	UBICACION	DECLARANTE
A CORUÑA					
T O T A L	**5.888**	**582**	**1.769**	**3.061**	**6.527**
OURENSE					
T O T A L	**1.057**	**146**	**179**	**333**	**1.141**

3.6.2.5. Cesiones de datos

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

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

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

3.6.3. OTRO TIPO DE ACTIVIDADES

3.6.3.1. Análisis de la inscripción privada por sectores de actividad.

Entre las actividades del Registro General de Protección de Datos, se encuentra la de realizar análisis de la inscripción por sectores de actividad cuando lo requiere una situación concreta, como puede ser una petición de la Dirección, una petición de la Inspección, el control del propio sector u otra causa similar. Dentro de este tipo de actividades destacan, durante el año 1998, las siguientes:

* Notarías

Ante el contraste entre la creciente informatización de las actividades notariales y la escasa inscripción en el Registro General de Protección de Datos de ficheros cuyo responsables sean los notarios, se procedió al análisis de los ficheros inscritos relacionados con este sector de actividad. Como resultado se obtuvo un reducido número de inscripciones cuyos titulares son los notarios, determinados Colegios Notariales Provinciales y el Consejo General del Notariado.

Ante esta situación, el Director de la Agencia mantuvo diferentes reuniones con el Consejo General del Notariado con la finalidad de concienciar e informar a los notarios. Se procedió a informar de una forma organizada, uniforme y coordinada, objetivo que pudo conseguirse a través del Consejo General del Notariado, con lo que se prevé el aumento de la declaración de los ficheros automatizados de este sector en el próximo año.

** Hospitales*

Dentro de la rúbrica de análisis de inscripciones sectoriales se ha estudiado la inscripción de los ficheros de centros hospitalarios tanto públicos como privados. La inscripción de este sector se ha analizado a partir del Catálogo Nacional de Hospitales, catálogo que contiene datos sobre el nombre, finalidad asistencial, dependencia patrimonial, dependencia funcional, conciertos con el Servicio Nacional de Salud (SNS), acreditación docente, datos geográficos, pertenencia a complejos hospitalarios, etc.

Aunque la información del Catálogo es amplia, la labor de identificación de los Hospitales inscritos en el Registro General de Protección de Datos no ha sido sencilla, dado que en muchas ocasiones las denominaciones del responsable inscritas en la base de datos del Registro General no coinciden con las denominaciones sociales que aparecen en el Catálogo y además en el propio Catálogo no consta el Código de Identificación Fiscal de los Centros Hospitalarios. Por otra parte, hay centros hospitalarios que, aún teniendo denominaciones distintas y encontrándose en locali-

dades distintas, tienen un mismo CIF, tratándose casi siempre de instituciones religiosas, Cruz Roja, etc.

Una vez realizado el análisis del Catálogo Nacional de Hospitales, 144 centros de titularidad privada han inscrito sus ficheros automatizados de datos de carácter personal en el Registro General de Protección de Datos.

Una prioridad del Director de la Agencia, es el tratar de concienciar, a través de las organizaciones Empresariales, de las obligaciones derivadas para éstos centros del cumplimiento de la LORTAD, con carácter previo a la iniciación en su caso, de las correspondientes actuaciones inspectoras.

** Empresas de Trabajo Temporal*

En los últimos años ha experimentado un auge importante el sector de las empresas de trabajo temporal. Dado que los ficheros de estas empresas contienen información personal relevante se ha analizado la inscripción de este sector en el Registro General de protección de Datos.

Como resultado del análisis se obtuvo un número considerable de empresas que han inscrito sus ficheros, y una vez analizada la inscripción se requirió a los responsables con deficiencias en la misma para que realizasen las pertinentes subsanaciones y aclaraciones. Finalmente, se detectó la necesidad de una coordinación con las empresas del sector para unificar criterios, informar a todos sus componentes de la obligatoriedad de la inscripción y realizar la misma de una forma uniforme.

** Sector de Investigación y Seguridad*

En el marco de los análisis realizados a petición de la Inspección de Datos se estudió el estado de inscripción de los ficheros privados cuyos responsables pertenecen al sector de Servicios de Investigación y Seguridad. También se analizó la inscripción de ficheros cuya finalidad incluye las investigaciones privadas a personas.

DESCRIPCIÓN CNAE	Nº DE FICHEROS
Servicios de Investigación y Seguridad	21
Investigación	27
Vigilancia, protección y seguridad	231

Del análisis referido se derivó que existen inscritos en el Registro General de Protección de Datos 279 ficheros cuyo responsable pertenece al sector de actividad de Servicios de Investigación y Seguridad, de entre los cuales la mayoría corresponden al subsector de Vigilancia, Protección y Seguridad (que comprende la custodia por vigilantes jurados de edificios de apartamentos, oficinas, almacenes, fábricas, solares en construcción, etc., servicios de vehículos blindados, actividades de guardaespaldas, control mediante dispositivos de seguridad, etc.) y una minoría al subsector de la Investigación propiamente dicha (que comprende los servicios de investigación y las actividades de los detectives privados). Esta información fue remitida a la Inspección a los efectos oportunos.

** Solvencia Patrimonial y Crédito*

En el marco de los análisis realizados a petición de la Inspección de Datos también se estudió la inscripción de ficheros con fines de cumplimiento o incumplimiento de obligaciones dinerarias y con fines de información sobre solvencia patrimonial y crédito.

La instrucción 1/95 de 1 de marzo de la Agencia de Protección de Datos, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito, exigía dentro del año siguiente a su publicación, que los sistemas que almacenan o procesan información relativa al incumplimiento de obligaciones dinerarias implantaran medidas de seguridad que se han de acreditar por la presentación de un informe de auditoría. Con la finalidad de detectar los ficheros que podrían estar incluidos en el ámbito de aplicación de la Instrucción, se analizaron 3.271 ficheros inscritos con finalidad de "información sobre la solvencia patrimonial y el crédito", estando incluidos en este colectivo, tanto ficheros con finalidad de control interno de impagados, como ficheros comunes alimentados por más de un responsable relativos al cumplimiento o incumplimiento de obligaciones dinerarias. Para la delimitación de este tipo de ficheros se analizaron las inscripciones por los sectores de actividad asociados al artículo 28 de la Ley.

La información fue remitida a la Inspección de Datos para la tramitación relativa al cumplimiento de la Instrucción 1/95, sobre la prestación de servicios sobre solvencia patrimonial y crédito, y en especial para el control de la remisión del informe de auditoría que prescribe la norma cuarta de la citada instrucción.

3.1.3.2 Requerimientos

Entre las actividades del Registro General de Protección de Datos se encuentra la de realizar requerimientos a los responsables de los ficheros, bien cuando lo requiere una situación concreta, o los resultados de un análisis de ficheros,

o una petición de la Dirección o de la Inspección u otra causa similar. Dentro de este tipo de actividades destacan, durante el año 1998, las siguientes:

* Datos de origen racial y vida sexual

Debido a que se detectó en la base de datos del Registro General la existencia de ficheros que declaraban otros datos especialmente protegidos de origen racial o vida sexual (artículo 7.3 de la Ley 5/1992), se procedió a realizar un estudio que permitiera analizar dichas inscripciones para conocer los sectores de actividad, usos y fines y determinar si dichos datos eran adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se habían obtenido, así como para poder detectar posibles errores de interpretación en la cumplimentación de los modelos de notificación.

Como consecuencia del análisis anterior, se requirió a 87 responsables de ficheros que habían notificado en su día la inclusión de otros datos especialmente protegidos de origen racial, para que aclararan las circunstancias de la presencia de este tipo de datos en sus ficheros o procedieran a subsanar los errores correspondientes. La gran mayoría de las respuestas recibidas notificaron que había existido un error en la declaración y comunicaron que sus ficheros no contenían otros datos especialmente protegidos, procediéndose a suprimir este tipo de datos de la inscripción.

Se recibieron 3 respuestas justificando el uso de este tipo de datos por las siguientes causas:

Origen Racial: Una empresa cuya actividad se incluía en el código nacional de actividades económicas como: «Otras actividades artísticas y de espectáculos», tenía declarada en el Registro General de Protección de Datos una base de datos de nombre "Actores". En este fichero se declaraban en el apartado de estructura y descripción de los tipos de datos de carácter personal incluidos en el fichero, el Origen Racial. El responsable del fichero justificó la necesidad de incluir en la Base de Datos el origen racial del actor, para facilitar la selección en castings para publicidad, teatro, televisión, etc., en los casos que se solicitan personas de razas y/o etnias determinadas.

Vida Sexual: Una sociedad del sector de la distribución de películas, declara en su fichero de *gestión de clientes*, la utilización de datos de vida sexual. Requerido el responsable del fichero para que aclarase las circunstancias en las que se recaba este tipo de dato, así como la finalidad del tratamiento del mismo, justifica su uso, dado que su actividad está relacionada con la venta de películas con temática sexual de contenido pornográfico y la finalidad es ofrecer a sus clientes información especializada, ante la solicitud de los mismos.

Un responsable del sector de actividades médicas declara en su fichero el uso de datos de salud y vida sexual con la finalidad de gestionar informatizadamente el *Historial Clínico* de sus pacientes. Ante el requerimiento de la Agencia, motivó la necesidad de utilizar este tipo de datos, dado que su especialización médica es la ginecología.

Por imperativo legal 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. En todo caso, los responsables de los ficheros que declaran cualquier tipo de dato especialmente protegido son requeridos para que justifiquen y aclaren la necesidad del tratamiento de los mismos y su adecuación a los usos y fines legítimos de los ficheros.

** Transferencias de carácter dinerario*

Como consecuencia del análisis de los ficheros que declaraban transferencias internacionales se estudiaron las inscripciones de aquellos responsables que habían declarado transferencias de datos a países que no proporcionan un nivel de protección equiparable al que presta la LORTAD y que se declaraban amparándose en el supuesto legal de que se refieren a *transferencias dinerarias* , conforme su legislación específica , según lo dispuesto en el articulo 33 d).

Como consecuencia del análisis anterior, se requirió a aquellos responsables de ficheros que habían justificado la transferencia por su carácter dinerario y que de la naturaleza y finalidad del fichero podría desprenderse que no se adecuaban a este tipo de transferencia. Una parte de las respuestas recibidas informaron que había existido un error en la declaración y comunicaron que la información de sus ficheros no se transfería; otra parte solicitó la supresión de sus ficheros, bien por no contener datos personales o bien por que los ficheros ya no existían. Otro grupo de responsables solicitó la preceptiva autorización del Director para realizar la transferencia internacional de datos, dado que dicha transferencia no se podía amparar en ninguna legislación específica.

** Clubes de Fútbol o Sociedades Deportivas.*

Como continuación a los requerimientos realizados a Clubes de Fútbol y Sociedades Deportivas se procedió a iniciar nuevos expedientes sancionadores a cinco entidades que no habían procedido a notificar sus ficheros de socios a los efectos de inscripción. De las cinco entidades, tres de ellas procedieron a notificar sus ficheros durante el trámite de los correspondientes expedientes. Las dos restantes resultaron sancionadas y notificaron sus ficheros para su inscripción a finales del año 1998.

3.7. FICHEROS DE TITULARIDAD PÚBLICA

3.7.1. EXPEDIENTES DE INSCRIPCIÓN, MODIFICACIÓN Y SUPRESIÓN DE FICHEROS

Durante el año 1998, el número de movimientos registrales efectuados sobre ficheros de titularidad pública ha ascendido a 3.145. De las operaciones realizadas a instancia de parte, 947 han sido nuevas inscripciones, 408 modificaciones y 91 cancelaciones de inscripción. Asimismo, se realizaron 1.699 operaciones de oficio, debido a la necesidad de normalización y adecuación de los datos consignados en la notificación de ficheros, en relación con las disposiciones de regulación de los mismos que se publican en los boletines oficiales.
De las inscripciones realizadas en el año, 677, es decir, el 71% 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 57% aún no ha formalizado la inscripción de sus ficheros. Las actuaciones de la Agencia que se han realizado ante esta situación se detallan en el párrafo "Actuaciones relacionadas con la Administración Local". Por tanto, el número de inscripciones a pesar de ser el más elevado respecto a otras Administraciones, sólo supone un crecimiento aproximado del 2% respecto al año anterior. La mayor parte de estas inscripciones pertenece a Ayuntamientos, con poblaciones inferiores a 1.000 habitantes, emplazados en el ámbito territorial de la provincia de Barcelona.
La inscripción de ficheros automatizados de datos personales de la Administración General del Estado, sí parece encontrarse estabilizada, al haber declarado prácticamente todos sus ficheros en años anteriores. El incremento de ficheros en 1998, respecto a las cifras finales de 1997, no supera el 3%. En cambio, ha alcanzando un crecimiento mayor, cercano al 19%, en la Administración Autonómica, que ha continuado formalizando la inscripción de ficheros, contribuyendo a que este porcentaje sea mayor, el hecho del requerimiento solicitado por la Agencia, a todas las Comunidades Autónomas para que procedieran a la revisión y regularización de la inscripción de sus ficheros.
Este año ha descendido considerablemente la inscripción de ficheros en el apartado de Otras Personas Jurídico-Públicas, que apenas ha aumentado en un 4%. En este grupo se encuentra el colectivo de Universidades, al que en el año anterior se dedicó una especial atención, requiriendo a todas aquellas que se encontraban creadas antes de 1997, y cuya inscripción se ha completado en 1998, con la notificación de 18 nuevos ficheros.
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 (28,3%), gestión de estadísticas internas (27%), gestión tributaria y de recaudación (22,65%), gestión económica con terceros (20,1%), seguidos de la gestión de la función estadística pública (17,6%), gestión del padrón (15%) y gestión de personal (14,2%), indicando que la mayor parte de ficheros pertenecientes a la Administración Pública y Organismos de titularidad pública corresponden a gestión administrativa.
Hay que resaltar el hecho de que no se ha producido ninguna inscripción de ficheros conteniendo *datos especialmente protegidos* regulados en el artículo 7 de la Ley Orgánica 5/92, referidos a ideología, religión o creencias.
Sin embargo, si se han producido inscripciones de ficheros conteniendo *otros datos especialmente protegidos* de salud, origen racial o vida sexual, ascendiendo en 1998 a 29 los ficheros declarados con esta tipología, correspondiendo 3 de ellos a ficheros de gestión y/o investigación sanitaria del Hospital Provincial de Huesca, del Instituto de Salud de Navarra y el Registro de Donantes y Tejidos del Ministerio de Sanidad y Consumo. El resto, y, por tanto, la mayoría de los ficheros que durante este año han sido notificados al Registro, con este tipo de datos en su estructura, corresponden al Sistema de Información sobre los Usuarios de Servicios Sociales (SIUSS), también denominado "Ficha Social", aplicación informática desarrollada por el Ministerio de Trabajo y Asuntos Sociales, que se continúa implantando en las Corporaciones Locales del ámbito territorial de las Comunidades Autónomas que han suscrito el oportuno convenio con el Ministerio.
Mediante este sistema de información se recogen en soporte informático los datos de los usuarios de los servicios sociales generales que demandan asistencia o sobre los que se realiza algún proceso de intervención social a través de las Corporaciones Locales, poniendo el Ministerio, a disposición de las Comunidades Autónomas que lo convengan, un 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, perfiles de usuarios, siempre tratando de mejorar la adecuación de los recursos existentes a las necesidades y demandas planteadas por los ciudadanos.
Desde la creación del Registro General de Protección de Datos ya se aproxima a 300 el número de ficheros inscritos en el mismo para dar soporte a este sistema de información.
También en la categoría de ficheros con datos especialmente protegidos amparados en el artículo 7 de la Ley, se encuentran aquellos que contienen información sobre infracciones penales y/o administrativas. En el año 1998, se ha llevado a cabo la inscripción de 43 ficheros, pertenecientes en general, a las Policías Locales. Estos ficheros se han declarado debido a los requerimientos que se habían realizado el año anterior, a las Policías Locales de diversos Ayuntamientos.

3.7.2. 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 1998, ha dado lugar a 1.697 subsanaciones de la inscripción de ficheros de titularidad pública. No obstante, y debido a que las declaraciones de ficheros han evolucionado mejorando la consignación de los datos requeridos en las notificaciones, ha descendido el número de este tipo de operaciones en una tercera parte respecto al año anterior.

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-1998, cerrada a 30 de abril.

3.7.2.1. Actuaciones relacionadas con la Administración General del Estado

Las disposiciones generales 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 1998 se han publicado en el Boletín, las siguientes disposiciones de carácter general que regulan nuevos ficheros o modifican alguno de los existentes en la Administración General del Estado y/o sus Organismos Autónomos:

* Orden 11/1998, de 15 de enero de 1998, del Ministerio de Defensa, por la que se amplía la Orden 75/1994, de 26 de julio de 1994, que regula los ficheros automatizados de datos de carácter personal, (BOE nº 23, de 27 de enero de 1998)
* Orden de 9 de julio de 1998, del Ministerio de Medio Ambiente, por la que se crean los ficheros automatizados de datos de carácter personal del Ministerio, (BOE nº 175, de 23 de julio de 1998).
* Orden de 10 de julio de 1998, del Ministerio del Interior, por la que se modifica la Orden de 4 de julio de 1997, relativa a ficheros automatizados de los Registros Generales Delegados de Sustancias Químicas Catalogadas, (BOE nº 174, de 22 de julio de 1998).
* Resolución de 7 de mayo de 1998, del Consejo Superior de Deportes, por la que se modifican algunos ficheros del Organismo. (BOE nº 119, de 19 de mayo de 1998)

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

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

En el caso de las relacionadas anteriormente, se han recibido las notificaciones de inscripción del Ministerio de Defensa y de algunos centros directivos del Ministerio de Medio Ambiente.

Para el resto de centros directivos del Ministerio de Medio Ambiente, de los que no se ha recibido notificación de inscripción de los ficheros creados por esta Orden, y para el Ministerio del Interior y el Consejo Superior de Deportes, en el mes de octubre, se procedió a requerir formalmente la notificación de inscripción de los ficheros a los que hacen referencia las disposiciones generales que se han relacionado anteriormente.

Al finalizar el ejercicio, aún quedaban por notificar algunos de los ficheros anteriormente reseñados. No obstante se espera que en el primer trimestre de 1999, se formalice dicha notificación.

3.7.2.2. Actuaciones relacionadas con la Administración de las Comunidades Autónomas.

Desde la inscripción inicial de los ficheros de Comunidades Autónomas, a raíz de la creación de la Agencia se han ido produciendo reestructuraciones orgánicas en estas Administraciones que no siempre han tenido reflejo en el Registro General de Protección de Datos.

Este hecho, puede dar lugar a que una de las funciones más importantes encomendadas al Registro, que es velar por la publicidad de los ficheros en él inscritos, facilitando al ciudadano las direcciones de los responsable de ficheros, no se pueda cumplir convenientemente.

Por este motivo, en el mes de agosto el Director de la Agencia se dirigió al Consejero encargado de la coordinación entre Departamentos de cada Comunidad Autónoma, informándole de los siguientes puntos:

* La obligación de cada responsable de ficheros automatizados de inscribir y mantener actualizada la inscripción en el Registro de estos ficheros.
* La importancia de la revisión de la actual inscripción, debido al impulso del uso de las nuevas tecnologías en la Administración y la posibilidad de haberse creado nuevos ficheros automatizados.
* Necesidad del análisis de las normas legales que establecen la creación de Registros Nacionales, con objeto de mantener la eficiencia y coordinación de medios estatales, que a su vez, se actualizan a partir de ficheros de las Comunidades Autónomas.

Hasta finales de 1998, se han ido recibiendo contestaciones de las Comunidades Autónomas del Principado de Asturias, Canarias, Castilla La Mancha, Cataluña, Galicia, Comunidad Foral de Navarra, País Vasco y Comunidad Valenciana, indicando que están procediendo a realizar las tareas que se solicitaban, y en algunos casos, inscribiendo nuevos ficheros.

Durante el año 1998, se ha recibido la notificación de inscripción de 179 nuevos ficheros pertenecientes a Comunidades Autónomas, y se ha tenido conocimiento de la publicación en los Diarios Oficiales respectivos, de las siguientes disposiciones de carácter general de creación, modificación o supresión de ficheros. Algunas de ellas aunque se publicaron en el año 1997, se recogen de nuevo en esta memoria, dado que los responsables notificaron sus ficheros en 1998 y por lo tanto los correspondientes asientos registrales también se realizaron en este año.

* Orden de 22 de mayo de 1998, de la Consejería de Trabajo e Industria, de regulación del fichero automatizado de datos de carácter personal del Servicio Andaluz de Colocación para su inscripción en el Registro General de Protección de Datos de la Agencia de Protección de Datos (BOJA nº 67, de 18 de julio de 1998)
* Resolución de 23 de diciembre de 1997, de la Consejería de Cooperación, del Principado de Asturias, por la que se crean ficheros automatizados de datos de carácter personal (BOPA nº 8, de 12 de enero de 1998)
* Resolución de 4 de noviembre de 1998, de la Consejería de Cultura del Principado de Asturias, por la que se modifica

el fichero automatizado "Actividades Culturales" y se suprime el de "Proveedores", (BOPA 270 de 21 de noviembre de 1998). Esta disposición al cierre del ejercicio 1998 no había sido notificada.
* Resolución de 23 de diciembre de 1997, del Instituto de Fomento Regional del Principado de Asturias, por la que se regula el fichero automatizado de datos de empresas asturianas (BOPA nº 8, de 12 de enero de 1998)
* Resolución de 23 de febrero de 1998, de la Consejería de Economía del Principado de Asturias, completando la Resolución de 31 de octubre de 1997 por la que se regulan los ficheros automatizados de la Consejería de Economía sobre datos de carácter personal destinados a la gestión del sistema tributario, (BOPA nº 53, de 5 de marzo de 1998)
* Resolución de 23 de febrero de 1998, de la Consejería de Economía, del Principado de Asturias, completando la de 31 de octubre de 1997, por la que se regulan los ficheros automatizados de la Consejería de Economía sobre datos de carácter personal, excluidos los de gestión del sistema tributario, (BOPA nº 53, de 5 de marzo de 1998)
* Resolución de 23 de diciembre de 1997 de la Consejería de Cooperación, del Principado de Asturias, por la que se modifican los ficheros de tratamiento automatizado de datos de carácter personal regulados por Resolución de 28 de julio de 1994, de la extinta Consejería de Interior y Administraciones Públicas (BOPA nº 8 de 12 de julio de 1998)
* Resolución de 3 de diciembre de 1997, de la Consejería de Economía, del Principado de Asturias, por la que se rectifican errores de la Resolución de 31 de octubre de 1997, por la que se regulan los ficheros automatizados de dicha Consejería con datos de carácter personal destinados a la gestión del sistema tributario (BOPA 293 de 20 de diciembre de 1997)
* Resolución de 20 de marzo de 1998 de la Consejería de Economía, del Principado de Asturias, por la que se dispone rectificación de error padecido en la Resolución de 23 de febrero de 1998 de la Consejería de Economía, por la que se regulan los ficheros automatizados de la Consejería de Economía sobre datos de carácter personal destinados a la gestión del sistema tributario (BOPA nº 79, de 4 de abril de 1998)
* Orden de 16 de julio de 1997, de la Consejería de Empleo y Asuntos Sociales de la Comunidad Autónoma 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).
* Orden de 14 de diciembre de 1998, de la Consejería de Administraciones Públicas de la Junta de Comunidades de Castilla La Mancha, por la que se regula el registro de documentos en la Administración de la Junta de Comunidades, (DOCM nº 63, de 24 de diciembre de 1998). Esta disposición al cierre del ejercicio 1998 no había sido notificada.
* Orden de 26 de noviembre de 1998, de la Consejería de Bienestar Social, por la que se modifican, suprimen y crean ficheros automatizados de carácter personal dependientes de la Consejería de Bienestar Social de la Comunidad Autónoma de Castilla La Mancha (DOCM 56, de 28 de noviembre de 1998). Esta disposición al cierre del ejercicio 1998 no había sido notificada.
* Orden de 30 de octubre de 1998, de la Consejería de Educación y Cultura, por la que se convocan becas para la elaboración de tesis doctorales y obtención del grado de doctor de la Comunidad Autónoma de Castilla La Mancha (DOCM nº 54, de 20 de noviembre de 1998)
* Resolución de 19 de septiembre de 1997 por la que se modifica la de 10 de febrero de 1997 de la Secretaría General Técnica de la Comunidad Autónoma de Castilla La Mancha, por la que se crea el Registro de Licitadores de la Consejería de Obras Públicas, y se establecen normas sobre custodia de documentación (DOCM 44 de 21 de septiembre de 1997)
* Resolución de 10 de febrero de 1997 de la Secretaría General Técnica por la que se crea el Registro de Licitadores de la Consejería de Obras Públicas y se establecen normas sobre custodia de documentación, de la Comunidad Autónoma de Castilla La Mancha. (DOCM 8 de 21 de febrero de 1997)
* Resolución de 3 de abril de 1997 de corrección de errores a la de 10 de febrero de 1997 por la que se crea el Registro de Licitadores de la Consejería de Obras Públicas, de la Comunidad Autónoma de Castilla La Mancha, y se establecen normas sobre custodia de documentación (DOCM 15 de 11 de abril de 1997)
* Decreto 223/98, de 30 de julio, por el que se actualizan los ficheros automatizados que contienen datos de carácter personal y gestionados por el Departamento de la Presidencia de la Generalidad de Cataluña (DOGC nº 2699, de 10 de agosto de 1998)
* Decreto 44/97 de 3 de marzo, de modificación del Decreto 335/94, de 16 de noviembre, por el que se regulan los ficheros automatizados que contienen datos de carácter personal gestionados por el Departamento de Enseñanza de la Generalidad de Cataluña (DOGC 2594, de 9 de marzo de 1998)
* Resolución de 3 de marzo de 1998, del Instituto Gallego de Promoción Económica de la Consejería de Economía y Hacienda de la Junta de Galicia, por la que se crea el fichero de datos de carácter personal del Centro de Innovación y Servicios Tecnológicos de la Madera (DOGA nº 55, de 23 de marzo de 1998)
* Resolución de 9 de marzo de 1998, de la Consejería de Economía y Hacienda de la Junta de Galicia, por la que se modifica la de 29 de julio de 1994 reguladora de los ficheros automatizados con datos de carácter personal existentes en el Instituto Gallego de Promoción Económica (DOGA nº 55, de 23 de marzo de 1998)
* Orden Foral 121, de 3 de septiembre de 1998, del Consejero de Salud de la Comunidad Foral de Navarra, por la que se suprime el fichero informatizado con datos de carácter personal denominado Salud Laboral y se crean los ficheros Incapacidad Laboral, Accidentes de Trabajo, Enfermedades Profesionales y Trabajadores Expuestos a Riesgos Laborales (BON nº 112, de 18 de septiembre de 1998)
* Orden de 17 de noviembre de 1997 del Vicepresidente del Gobierno del País Vasco y Consejero de Hacienda y Administración Pública por la que se regulan los ficheros automatizados de carácter personal de la Vicepresidencia del Gobierno, del Departamento de Hacienda y Organismos Autónomos adscritos al mismo (BOPV 239 de 15 de diciembre de 1997)
* Decreto 74/92, de 31 de marzo de 1998, por el que se establece la estructura orgánica del Departamento de Justicia del Gobierno Vasco, (BOPV nº 82, de 4 de mayo de 1998), que implica el cambio del nombre de responsable de los ficheros de este Departamento.
* Orden de 23 de octubre de 1998, de la Consejería de Economía, Hacienda y Administración Pública de la Generalidad Valenciana, por la que se crea el fichero automatizado de datos de carácter personal denominado HUMAN1 de la Consejería de Bienestar Social, (DOGV nº 3376, de 19 de noviembre de 1998)
* Orden de 5 de noviembre de 1998, de la Consejería de Presidencia, por la que se crea el Fichero de datos y se regula

el Registro de Méritos de Determinación Autonómica de la Comunidad Valenciana de los funcionarios de administración local con habilitación de carácter nacional. (DOGV3390 de 10 de diciembre de 1998). Esta disposición al cierre del ejercicio 1998 aún no había sido notificada.
* Acuerdo de la Excelentísima Asamblea sobre la propuesta de aprobación de fichero informático con datos de carácter personal "PMH001", de la Ciudad Autónoma de Melilla. (B.O. Ciudad de Melilla 3590 de 27/8/98)

3.7.2.3. Actuaciones relacionadas con los Órganos de Protección de Datos correspondientes a las Comunidades Autónomas.

El artículo 40 de la LORTAD, dispone que las funciones de la Agencia de Protección de Datos reguladas en su artículo 36, a excepción de las mencionadas en los apartados j), k), y l) y en los apartados f) y g) en lo que se refiere a transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas por los órganos correspondientes de cada Comunidad, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por la propia Comunidad Autónoma.
A su vez el apartado 2 del mismo artículo habilita a las Comunidades Autónomas a crear y mantener sus propios registros de ficheros públicos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos. En el Registro General de Protección de Datos serán objeto de inscripción los ficheros automatizados que sean titulares las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros que se puedan crear de conformidad con el artículo 40.2 de la Ley.

Comunidad Valenciana

Durante 1998, se ha publicado el Decreto 96/98, de 6 de julio, del Gobierno Valenciano, por el que se regulan la organización de la función informática, la utilización de los sistemas de información y el Registro de Ficheros Informatizados en el ámbito de la Administración de la Generalidad Valenciana, a través del Diario Oficial de la Generalidad Valenciana nº 3291, de 22 de julio de 1998.
Este Decreto prevé la creación del Registro de Ficheros Informatizados en el ámbito de la Generalidad Valenciana, mediante un desarrollo reglamentario del mismo, que por el momento no ha sido publicado.
Durante 1998, se han mantenido reuniones entre representantes de la Generalidad Valenciana y la Agencia de Protección de Datos con el fin de establecer los mecanismos de comunicación y coordinación entre ambos Órganos.
Es de señalar que es un mero registro administrativo y no se trata en ningún caso de una Agencia de Protección de Datos autonómica.

Comunidad de Madrid

Desde la creación de la Agencia de Protección de Datos de la Comunidad de Madrid, se ha mantenido una estrecha relación entre dicha Agencia y este Registro, con comunicaciones y reuniones periódicas.
Es un compromiso de la Agencia Autonómica, el hacer llegar al Registro General de Protección de Datos la notificación para su inscripción de todos los ficheros de la Comunidad Autónoma, con el fin de facilitar a los responsables de los ficheros la doble obligación de inscripción de los mismos en la Agencia de Protección de Datos y en la Agencia de Protección de Datos de la Comunidad de Madrid.
La Agencia de Madrid está realizando la adecuación de su Sistema Informático para ajustarse a los requerimientos establecidos por la Resolución de 23 de junio de 1994, de la Agencia de Protección de Datos.
Durante 1998, se han realizado diferentes pruebas en este sentido con la actualización de la inscripción de los ficheros pertenecientes a los diferentes centros directivos de esta Comunidad, esperándose la actualización definitiva a principios del próximo año.
No obstante, en el Registro General de Protección de Datos se dispone de las nuevas disposiciones de creación, modificación y/o supresión de ficheros de la Comunidad de Madrid, consiguiendo de esta forma informar al ciudadano que se dirige a este Registro de los centros directivos en los que puede ejercitar sus derechos de acceso, rectificación y cancelación de ficheros de la Comunidad Autónoma.
Así, además del Decreto 133 de 16 de octubre de 1997 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 de 21 de abril de 1995, de la Comunidad Autónoma de Madrid, publicado en el suplemento al BOCM número 259 del 31 de octubre de 1997, del que se tenía constancia en el año anterior, durante 1998 han sido publicadas las siguientes:
* Decreto 7/98, de 15 de enero, de la Consejería de Hacienda, por el que se crean ficheros automatizados de datos de carácter personal de la Empresa Pública "Madrid 112, Sociedad Anónima" (BOCM 25 de 30 de enero de 1998)
* Decreto 15/98, de 5 de febrero, del Consejero de Gobierno por el que se crea el fichero de datos de carácter personal de residentes fallecidos en la Comunidad Autónoma de Madrid (BOCM 43 de 20 de febrero de 1998)
* Decreto 63 de la Consejería de Economía y Empleo de la Comunidad de Madrid, de 23 de abril de 1998, de creación de nuevos ficheros de datos de carácter personal, (BOCM nº 104, de 4 de mayo de 1998).
* Decreto 105 de 18 de junio de 1998 del Consejo de Gobierno por el que se crean y modifican ficheros automatizados de datos de carácter personal en la Consejería de Presidencia de la Comunidad Autónoma de Madrid (BOCM 154 de 1 de julio de 1998)
* Decreto 129 de 3 de julio de 1998, de la Consejería de Educación y Cultura de la Comunidad de Madrid, de creación del fichero MADRIMASD, de datos de carácter personal (BOCM 161 de 9 de julio de 1998)
* Decreto 127 de 2 de julio de 1998 por el que se crean los ficheros que contienen datos de carácter personal de la Agencia de Protección de Datos de la Comunidad de Madrid (BOCM 164 de 13 de julio de 1998)
* Decreto 225 de 30 de diciembre de 1998, del Consejo de Gobierno de la Comunidad de Madrid, por el que se crea un fichero automatizado de datos de carácter personal de la Agencia de Protección de Datos de la Comunidad de Madrid (BOCM 16 de 20 de enero de 1999)

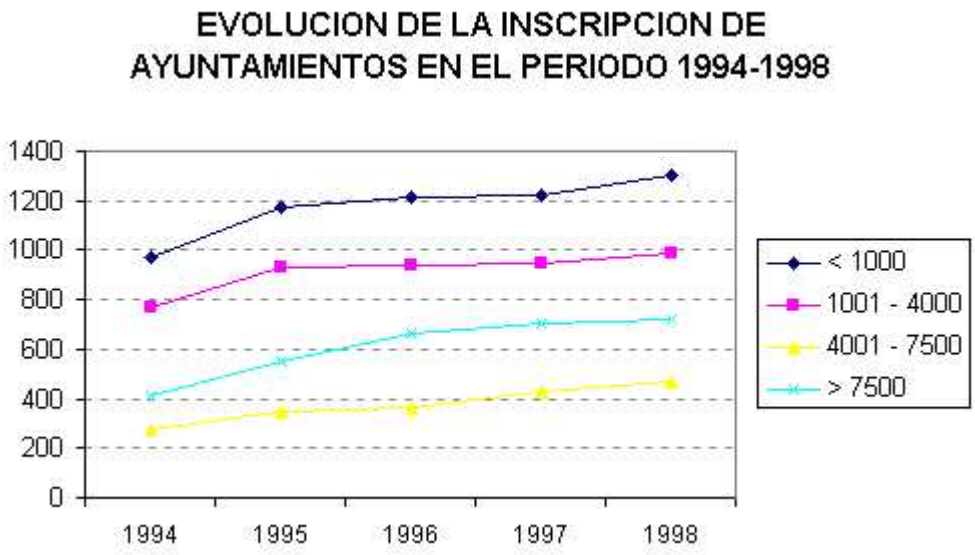
3.7.2.4. Actuaciones relacionadas con Administración Local

La inscripción en el Registro de los ficheros automatizados pertenecientes a las Entidades de la Administración Local ha superado, en 1998, el 70% de las altas registrales de ficheros de titularidad pública.
No obstante, pese a este volumen de operaciones que, al finalizar 1998, supone que se encuentren inscritos 23.031

ficheros de Administración Local, continúa siendo la Administración Pública en la que existe un número más alto de organismos que no ha notificado 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	1.299	3.599	73,4
1001 - 4000	1.885	983	902	48
4001 – 7500	540	469	71	13,1
> 7500	764	721	43	5,6
Total	8.087	3.472	4.615	57

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



Durante el año 1998 se ha continuado requiriendo 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.
Continuando con los requerimientos solicitando la inscripción de ficheros a los municipios con población comprendida en el tramo de 4.000 a 7.500 habitantes, en el mes de julio fueron requeridos los 88 Ayuntamientos que no tenían inscritos sus ficheros. De éstos, al finalizar el año, 17 habían completado la inscripción. Con los 71 Ayuntamientos restantes, se elaboró un informe al respecto. El Director de la Agencia, puso este hecho en conocimiento del Consejo Consultivo de la Agencia, del que forma parte un representante de la Federación Española de Municipios y Provincias, esperando que su colaboración se refleje en el año 1999 con un aumento de la inscripción de aquellos Ayuntamientos que aún no han procedido al cumplimiento de esta obligación.
El incremento mayor de municipios inscritos en 1998 se ha producido en los Ayuntamientos con menos de 4.000 habitantes pertenecientes a la provincia de Barcelona debido a la colaboración, ya iniciada el año anterior, de la Diputación de Barcelona.
El número de Ayuntamientos con población superior a 7.500 que ha efectuado la inscripción de ficheros en 1998 ha sido de 18, quedando aún 43 Ayuntamientos sin inscribir. Sobre este grupo de Ayuntamientos ya se están efectuando acciones desde la Inspección.
Continúa siendo el Ayuntamiento de Ourense el único órgano de la Administración Local perteneciente a una capital de provincia, que no ha notificado sus ficheros a efectos de inscripción en el Registro. Ello, a pesar de los requerimientos que le han sido remitidos. Concretamente y, después de una conversación telefónica mantenida con el Alcalde en diciembre de 1998, se envió información detallada del procedimiento a seguir para cumplir el trámite de notificación,

tanto telefónicamente como mediante fax y correo ordinario.

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

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

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

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

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

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

Mediante este Convenio, en el año 1997, fueron 68 los Ayuntamientos que aceptaron la encomienda a la Diputación de Barcelona, de la gestión de la informatización del padrón de habitantes, que incluye la tramitación en el Registro de la inscripción de los ficheros correspondientes a estos municipios. La formalización de la inscripción en le Registro para los Ayuntamientos de este grupo que no habían realizado anteriormente la notificación de su fichero de Padrón se ha realizado en el año 1998.

En este sentido, en 1998 se han continuado produciendo nuevos acuerdos de este tipo con otros 100 Ayuntamientos de Barcelona, que han sido publicados en el Boletín Oficial de la Provincia de Barcelona números 45, 139, 161 y 299, de fechas 21 de febrero, 111 de junio, 7 de julio y 15 de diciembre, respectivamente, recibiéndose las correspondientes solicitudes de inscripción.

- Policía Local.

Como consecuencia de 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, sobre los Ayuntamientos de Barcelona, Bilbao, Marbella, Murcia, Sevilla, Valladolid, Vigo y Zaragoza, en los primeros meses de 1998 se recibió la notificación de todos ellos, excepto del Ayuntamiento de Marbella que no llegó a contestar a los requerimientos del Registro, por lo que se ha remitido el asunto a la Inspección de Datos para que adoptara las medidas oportunas.

3.7.2.5. Actuaciones relacionadas con Universidades

El análisis que ya estaba iniciado en el año anterior sobre las Universidades que se encontraban creadas, y el requerimiento a aquellas que no habían realizado la inscripción de sus ficheros se cerró en el primer trimestre de 1998 con la inscripción de las Universidades de Huelva y La Coruña.

La Universidad de Huelva procedió a la notificación de inscripción de sus ficheros, pues había publicado con anterioridad la disposición de creación de los mismos, mientras la Universidad de La Coruña procedió a publicar en el BOE número 51, de 28 de febrero de 1998, la Resolución de 13 de febrero, por la que se regulan los ficheros automatizados con datos personales, y posteriormente realizó la correspondiente notificación al Registro.

En septiembre de 1998 se han completado las actuaciones iniciadas en el año anterior con las Universidades que habían sido creadas desde el inicio del anterior análisis. Se requirió a nueva universidades que se habían creado en este período y que no habían procedido a notificar sus ficheros. Al finalizar el año han cumplimentado la inscripción de sus ficheros las Universidades de Mondragón, Vic, Internacional de Andalucía e Internacional SEK, quedando pendientes de notificar sus ficheros las Universidades: Internacional Menéndez Pelayo, Oberta de Catalunya, Pablo de Olavide y Rey Juan Carlos, esperándose que la notificación se produzca a lo largo del próximo año 1999.

3.7.2.6. Otras actividades

- Comunidades Autónomas que han implantado un sistema de identificación de recién nacidos a través del ADN .

Teniendo conocimiento en la Agencia, a través de las noticias publicadas en prensa, de la puesta en marcha de un sistema de identificación de recién nacidos, ha sido preocupación del Registro conocer la posible existencia de ficheros automatizados que trataran ésta información, en el ámbito de las Comunidades Autónomas de Andalucía y País Vasco, teniendo en cuenta que, por una parte, se trata de datos que van a identificar a una persona física, y, por tanto, han de ser considerados datos de carácter personal, según dispone la LORTAD, y por otra parte, dada su naturaleza, pueden

considerarse datos de extraordinario sensibilidad, ya que pueden permitir conocer aspectos de la salud del recién nacido, regulados de forma particular en el artículo 7 de la LORTAD.
Con este motivo se remitieron sendos requerimientos a ambas Comunidades Autónomas para conocer la situación de tales proyectos, y concretamente, de la utilización o no de ficheros informatizados con datos de carácter personal.
Dado que el requerimiento se envió en el mes de diciembre, se espera recibir una respuesta en los primeros días de 1999.
- *Delegaciones y Subdelegaciones del Gobierno* .
La Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE), modificó y reformó la estructura y competencias de las Delegaciones y Subdelegaciones del Gobierno (que asumen entre otras las competencias de los anteriores Gobiernos Civiles) y cambió la adscripción orgánica de las Delegaciones del Gobierno, y las posteriores modificaciones de las estructuras orgánicas básicas de los Ministerios de Administraciones Públicas y del Interior. La entrada en vigor de la misma, implicó un cambio en la adscripción de los ficheros de éstos Órganos.
A finales de 1997, se solicitó a la Subsecretaria de Interior la revisión de la inscripción, con la finalidad de adecuarla a la nueva estructura funcional y orgánica de las Delegaciones y Subdelegaciones del Gobierno.
Durante el año 1998 y como respuesta al requerimiento de la Agencia, el Ministerio del Interior ha remitido la relación de ficheros que permanecían bajo su responsabilidad, y a su vez, se ha procedido de oficio a actualizar la inscripción del resto de ficheros de Delegaciones y Subdelegaciones del Gobierno que fueron adscritos funcionalmente al Ministerio de Administraciones Públicas.

3.8. 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 el artículo 12 del Convenio 108 del Consejo de Europa, estableciendo así una regulación del concepto de "flujo transfronterizo de datos". La protección de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituyen una auténtica necesidad de la vida actual, de la que, las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional son simples ejemplos. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la 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 de la LORTAD, se indica que "no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable, salvo que, además de haberse observado lo dispuesto en la Ley, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen las garantías adecuadas".

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

No es necesaria la autorización previa en los siguientes supuestos:

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

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

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

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

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

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

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

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

3.8.1. 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.
En esta relación se incluyen además de los países parte del Convenio 108 del Consejo de Europa para la Protección de las Personas, en relación al tratamiento automatizado de datos, Austria, Israel, Hungría, Nueva Zelanda, República Checa, República de Slovakia, San Marino y Suiza.

También se considera que proporcionan un nivel de protección equiparable a la Ley Española respecto de los datos registrados en ficheros de titularidad pública, la República de Andorra, Japón y Canadá.

Como continuación a esta Orden de 2 de febrero de 1995, el Ministerio de Justicia, previo informe del Director de la Agencia, amplió la relación de países con protección de datos de carácter personal equiparable a la española por Orden de 31 de julio de 1998, publicado en Boletín Oficial del Estado de fecha 21 de agosto de 1998.

A tal fin, se incluye a Italia y Grecia, dado que se ha promulgado por ambas, las correspondientes Leyes de Protección de Datos, de fecha 31 de diciembre de 1996 y 10 de abril de 1997.

Esta enumeración deberá ser revisada por las autoridades de control del Grupo del Trabajo del artículo 29 de la Directiva 95/46/CE, a fin de armonizar una postura común.

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 los dictámenes adoptados por la Comisión de la Unión Europea y de los estudios correspondientes.

3.8.2. 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, establecida 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:

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

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

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

c) Que la titularidad del fichero 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.

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

3.8.3. 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 983 de los cuales 50 corresponden a inscripciones de titularidad pública y 933 de titularidad privada.

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

SUPUESTOS LEGALES	TIT.PUBLICA	TIT.PRIVADA
Se ampara en tratado o convenio del que España forma parte	39	4
Se realiza a efectos de prestar auxilio judicial internacional	9	0
Tiene por objeto intercambiar datos de carácter médico y así lo exige el tratamiento del afectado o la investigación epidemiológica	6	6
Se refiere a transferencias dinerarias	15	50
Se efectúa con destino a algún país de los citados en el reglamento con nivel de protección equiparable	46	841
Se efectúa con autorización del Director de la Agencia	0	145
TOTAL FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES	**50**	**933**

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 destinatarios son los siguientes:

PAÍS DESTINATARIO	TIT. PÚBLICA	TIT. PRIVADA
ALEMANIA	1	59
ANDORRA	0	10
ARGELIA	0	1
ARGENTINA	0	1
AUSTRALIA	0	5
BELGICA	3	42
BOLIVIA	0	1
BRASIL	0	1
CANADA	0	1
COLOMBIA	0	1
CUBA	0	2
CHINA	0	1
DINAMARCA	0	2
ESTADOS UNIDOS	1	146
FILIPINAS	0	2
FINLANDIA	0	1
FRANCIA	7	157
GRECIA	1	0
HONG KONG	0	17
IRLANDA	0	3
ISRAEL	0	2
ITALIA	2	42
JAPON	1	6
MARRUECOS	1	0
NORUEGA	1	0
PAÍSES BAJOS	0	28
PORTUGAL	1	61
REINO UNIDO	3	393
RUSIA	0	1
SINGAPUR	0	1
SUECIA	0	7
SUIZA	0	63
VENEZUELA	0	1

3.8.3.1. 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 841. A continuación con 50 inscripciones, se encuentran los ficheros que declaran transferencias dinerarias conforme a su legislación específica, casi todos ellos pertenecientes a entidades financieras que realizan transferencias amparadas en su legislación en materia dineraria. Normalmente adherido al sistema SWIFT (Sistema internacional de intercambio de datos bancarios).

Se declaran 4 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, es pequeño debido sobre todo a la inexistencia de textos internacionales que recojan mandatos relativos a la protección de datos. Los existentes, son acuerdos ratificados por Estados que a su vez suelen tener legislación equiparable a la española. Seis ficheros realizan la transferencia de datos a otros países con objeto de intercambiar datos de carácter médico cuando así lo exija el tratamiento del afectado o una investigación epidemiológica.

3.8.3.2. 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 46 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 declaran transferencias de carácter dinerario, amparándose en el supuesto de legislaciones específicas.

En este supuesto se encuadran los ficheros de operaciones exteriores inscritos por el Banco de España, los ficheros de gestión de ayudas económicas de la Unión Europea al sector agrario del Organismo Parques Nacionales y de la Comunidad Foral 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.

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

Seis ficheros tienen por objeto intercambiar datos de carácter médico.

3.8.3.3. Expedientes de autorización de Transferencia Internacional

Se han resuelto, hasta diciembre de 1998, 100 expedientes de solicitud de Autorización de transferencias internacionales, encontrándose otros 13 expedientes más iniciados durante 1998 en fase de tramitación. Su distribución según el año de solicitud se puede comprobar en la siguiente tabla:

ESTADO	1995	1996	1997	1998	TOTAL
Resuelto	15	41	25	20	101
En tramitación	0	0	1	13	13
T OT A L	**15**	**41**	**26**	**33**	**114**

Durante el año 1998, se han solicitado 32 expedientes de autorización; resolviéndose en el año, 19 de ellos. Además se ha resuelto uno, iniciado en el año 1997. Se han archivado tres y, en uno, el responsable ha desistido de su solicitud. Por lo tanto, se han autorizado e inscrito en el Registro General 20 autorizaciones de transferencia internacional, quedando pendiente de realizar los últimos trámites previos a su resolución nueve expedientes. Estados Unidos es el país que más autorizaciones ha recibido, debido a que un gran porcentaje de las multinacionales tienen su empresa matriz ubicada en dicho país.

3.8.4. ANÁLISIS DEL MOVIMIENTO INTERNACIONAL DE DATOS

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

Las motivos se pueden resumir:

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

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

Normalmente existe una relación contractual entre el interesado y el responsable del fichero. Los sectores que justifican esta razón para solicitar la autorización de transferencia son muy diversos, pudiéndose resaltar entidades del sector del crédito, seguros, química y fabricantes de bienes informáticos.

Se debe hacer mención aparte, a las autorizaciones cuya finalidad es la gestión integral de Recursos Humanos, de una multinacional que se autorizan en razón del consentimiento del interesado.

b) Mejor servicio al cliente.

Se encuentra en diferentes sectores y para fines muy diferentes en:

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

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

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

- Sistemas de distribución mundial. La generalización de reserva, emisión de billetes y otros servicios del transporte a nivel internacional 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.

Los sectores más representativos serían aquellos relacionados con actividades de reserva, emisión de billetes y transporte internacional, las líneas aéreas, las de alquiler de automóviles y el transporte de mercancías de ámbito mundial.

- 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.

Los sectores más representativos serían los medios de pago y tarjetas de fidelización de clientes de ámbito mundial.

3.8.5. ANÁLISIS DE LOS FLUJOS DE INFORMACIÓN

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

3.8.5.1. La Transferencia Internacional de Datos se realiza a un gran número de países donde se ubican las delegaciones o filiales de la empresa responsable de la Transferencia Internacional.

La entidad ubicada en el territorio español es una de las delegaciones que la compañía matriz (ubicada fuera del ámbito de la Unión Europea) tiene en distintos países para realizar una cobertura mundial 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 a la entidad responsable que garantice que los datos de sus clientes se van a tratar globalmente 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 de la empresa en relación a las normas de seguridad de acceso a la información a nivel mundial.

3.8.5.2. La Transferencia Internacional de Datos se realiza por empresas ubicadas en España que ofrecen productos de terceras empresas ubicadas fuera del territorio de la Unión Europea.

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

En el caso de extinción del acuerdo de licencia, se exige al responsable del fichero establecido fuera del territorio de la Unión, la obligación de 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.

3.8.5.3. 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 integran 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.

3.8.5.4. La Transferencia Internacional se realiza por un grupo de empresas con la finalidad de gestionar los recursos humanos de una forma global para el grupo de empresas con sede en diversos países 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.

3.8.5.5. La Transferencia Internacional se realiza por Empresas Españolas con delegaciones en distintos países.

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

El centro de procesos de datos 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.

3.8.5.6. La Transferencia Internacional se realiza por 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.

3.8.5.7. 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.

En este caso se dan dos variantes:

a) Con consentimiento del interesado:

La finalidad de la transferencia es el tratamiento automatizado centralizado de los datos de los socios de una cadena de alquiler de videos, a los efectos estrictamente estadísticos y 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.

b) Sin consentimiento del interesado: Este caso por su especial naturaleza se analiza por separado, en el apartado de solución contractual.

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

Los datos a transferir son los propios de un sistema de correo electrónico, 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.

3.8.6. LA DIRECTIVA EUROPEA Y LA TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

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

Para esto establece los siguientes principios a tener en cuenta:

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

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

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

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

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

Los principios que se recogen en el artículo 25 apartado 2 consideran que el carácter adecuado de un nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias que concurran o estén relacionadas con la transferencia o con una categoría de transferencias de datos. En particular considera:

- la naturaleza de los datos,
- la finalidad y la duración del tratamiento o de los tratamientos previstos,
- el país de origen y el país de destino final,

- las normas de derechos generales o sectoriales, vigentes en el país tercero de que se trate,
- las normas profesionales en vigor en dichos países,
- y las medidas de seguridad.

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

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

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

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

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

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

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

Estas excepciones no coinciden en su totalidad con las excepciones que recoge nuestra Ley en su artículo 33, siendo, sobre todo, el consentimiento del interesado el que los diferencia de una forma más notable, dado que en nuestra legislación no se recoge esta exclusión, en la actualidad es necesaria una autorización previa del Director de la Agencia para efectuar una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado, aunque el interesado haya dado su consentimiento.

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

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

Con esta forma de proceder se evitará la existencia de divergencias, en la práctica, en relación con las autorizaciones realizadas por las autoridades de control en el movimiento internacional de datos.

El artículo 4 del Capítulo I de Disposiciones Generales, relativo al Derecho nacional aplicable, incide considerablemente en el aspecto práctico de la Transferencia Internacional de datos en relación con la ubicación del establecimiento del responsable, y así, en su apartado 1 c), determina que se aplicarán las Disposiciones Nacionales cuando "el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea" en este caso y según el artículo 4 apartado 2 "el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

La Directiva considera que, para evitar que una persona sea excluida de la protección garantizada, es necesario que todo tratamiento de datos personales efectuado en la Comunidad, respete la legislación del Estado miembro donde esté establecido el responsable del fichero.

El hecho de que el responsable del tratamiento de datos esté en un país tercero no debe obstaculizar la protección de las personas por lo que, en estos casos, el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos de los ciudadanos.

Uno de los problemas que se han planteado en la Agencia de Protección de Datos, con el movimiento internacional de

datos y que la legislación española no contempla, es la situación que se produce cuando el responsable del tratamiento no está establecido en el territorio nacional. En estos casos se ha interpretado que es necesario que se designe un representante, al que se le puedan exigir las obligaciones y responsabilidades emanantes de nuestra Ley y, en caso contrario, no se están autorizando los tratamientos de datos y su consiguiente movimiento internacional.

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, y 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 que 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, 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.

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 datos 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 país 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.

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.

3.8.7. SOLUCIÓN CONTRACTUAL: CONTEXTO TRANSFERENCIAS INTERNACIONALES A TERCEROS PAÍSES. ART. 26.2 DIRECTIVA 95/46/CE

La idea de utilizar un contrato para regular las Transferencia Internacionales de Datos proviene:

- Consejo de Europa
- Cámara Internacional del Comercio
- Comisión Europea. Estrasburgo 2 de noviembre de 1992

- Grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales4. Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países. (DG XV D/5005/98 final)

El contrato debe ser el medio que permite al responsable del fichero ofrecer garantías adecuadas al transmitir datos fuera de la Unión Europea y, por lo tanto, fuera del ámbito de aplicación de la Directiva y del marco general del Derecho Comunitario.

Por lo tanto para cubrir esta función, la cláusula contractual debe compensar de manera satisfactoria la ausencia de una protección general adecuada, incluyendo los elementos esenciales que permitan una protección adecuada junto con las garantías suficientes.

Este binomio exigirá que:

- El nivel de cumplimiento de los principios básicos para la protección de datos, en la práctica sea satisfactorio y se apliquen íntegramente,

- Se ofrezca a las personas afectadas apoyo y asistencia en el ejercicio de sus derechos,

- Quienes resulten perjudicados, cuando no se apliquen los principios, tengan a su disposición procedimientos de recursos apropiados (art. 17 LORTAD).

Cláusulas a estipular **:**

La primera vez que se ha utilizado la solución contractual en el contexto de la Transferencia Internacional ha sido a finales de 1998.

Las cláusulas que se han exigido han sido las siguientes:

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

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

c) Calidad y Proporcionalidad de los datos.

d) Delimitación del interés legítimo del responsable del tratamiento, garantizando que este interés no va en detrimento de los derechos del afectado y que no se ha procedido a informar al titular del hecho de la Transferencia Internacional debido a que no existe ningún riesgo de atentado contra la intimidad, y que requeriría un esfuerzo desproporcionado informar al afectado del hecho de la transferencia.

e) Seguridad.

Deberá figurar una descripción general de las medidas de seguridad técnicas y organizativas que permitan evaluar si dichas medidas resultan adecuadas para garantizar la seguridad del tratamiento.

El responsable del fichero debe asumir la responsabilidad principal del cumplimiento de los principios sustantivos de protección de datos; el *encargado del tratamiento* será el responsable de la seguridad de los datos (como entidad encargada del tratamiento o que presta materialmente el correspondiente servicio).

La relación entre ambos se rige por lo dispuesto en el artículo 17.3 de la Directiva 95/46 "*La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:*

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del fichero,

- que las obligaciones del apartado 1 "*Seguridad del tratamiento, medidas técnicas y organizativas" tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste."*

A los efectos de conservación de prueba, las partes del contrato relativas a la protección de datos y a los requisitos relativos a las medidas de seguridad constarán por escrito o en otra forma equivalente.

Por lo tanto, las cláusulas contractuales relacionadas con las medidas de seguridad, deberán disponer:

- que el *encargado del tratamiento* sólo actúa siguiendo instrucciones del *responsable del fichero* .

- que las obligaciones establecidas en el artículo 9 y 10 de la LORTAD (seguridad de los datos y deber de secreto para todas las personas que intervengan en cualquier fase del tratamiento de datos y el deber de guardarlos, obligaciones que subsistirán aún después del finalizar sus relaciones con el *responsable del fichero* o el *encargado del tratamiento*) incumben también al *encargado del tratamiento* .

- Cláusula relativa al artículo 27 de la LORTAD:

"*Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación.*

Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años."

- Se tendrá que determinar el plazo límite de la transferencia y/o en su caso de la conservación de los datos.

f) Estipulación pormenorizada de las dos partes contratantes, es decir, el responsable del fichero y el encargado del tratamiento.

Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal, tendrán la consideración de *encargados del tratamiento* (definido en el artículo 2.e de la Directiva).

La realización de tratamiento por encargo deberá estar regulada por un contrato que vincule al *encargado del tratamiento* (tercer país) con el *responsable del fichero* (establecido en España).

- Se deberá especificar el principio de finalidad como estipulación pormenorizada del objeto del contrato.

El receptor vendrá obligado a seguir exclusivamente las instrucciones del remitente. El remitente seguirá siendo el *responsable del fichero*, en tanto que el receptor será el encargado del tratamiento. En tales circunstancias, dado que los datos estarán bajo el control de una entidad establecida en España, el tratamiento realizado en el tercer país seguirá estando sujeto a la normativa española5, y además el *responsable del fichero* o del tratamiento continuará respondiendo, en virtud de la legislación española, de los daños causados como consecuencia de un tratamiento ilegal de los datos6 y, en su caso, se impondrán las sanciones correspondientes7.

g) Derecho de acceso, rectificación, cancelación y oposición:

- 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 dispuestos en la Ley Orgánica 5/1992 de regulación del tratamiento automatizado de datos de carácter personal, así como que se continuará facilitando desde España los derechos de acceso, rectificación y cancelación.

- Determinación de cómo se van a ofrecer a los interesados apoyo y asistencia para garantizar el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia y en los plazos que determina la LORTAD.

- Deberá existir en el expediente un documento que defina de forma detallada como se facilitarán los derechos de acceso, rectificación y cancelación desde la sede del Responsable en España.

h) Vías adecuadas de Reclamación.

- Se deberán aplicar cláusulas que garanticen al afectado, cuando resulte perjudicado, el pago de indemnizaciones por el *responsable del fichero* y la posibilidad en su caso, de imponer sanciones por la Agencia de Protección de Datos Española.

- La empresa española responderá solidariamente con la destinataria de la Transferencia Internacional, frente a la Agencia de Protección de Datos y los Tribunales Españoles, de los eventuales incumplimientos en que ésta última pueda incurrir respecto de las obligaciones asumidas en el contrato

- Para ofrecer a los afectados el recurso legal ante la Agencia es necesario que sea de aplicación en el contrato la legislación Española en materia de protección de Datos.

- Otra posibilidad que mejoraría la situación de los interesados, sería que se incluyera en el contrato el compromiso de las partes a someterse a un arbitraje vinculante (Agencia de Protección de Datos) en el supuesto de que el interesado impugnara la observancia de las disposiciones.

i) Restricciones sobre las transferencias posteriores o cesiones a personas ajenas al contrato.

- Deberá figurar expresamente la prohibición de transferencias o cesiones posteriores a personas ajenas al contrato.

- Únicamente se permitirán si existe una forma de vincular por contrato a ese tercero y ofrecer las mismas garantías de protección de datos.

j) Compromiso del receptor con la Autoridad de Control española, Agencia de Protección de Datos.

- El receptor de los datos se debe comprometer directamente con la Agencia a autorizar el acceso al establecimiento donde se estén tratando los datos de un representante de la Agencia, en el supuesto de que existan sospechas de que se han incumplido los principios de la protección de datos. Así mismo, se deberá garantizar la facultad de realizar auditorías por la propia Agencia o por un auditor externo independiente designado por ésta.

1 La forma jurídica de dicho establecimiento no es un factor determinante.
2 Operaciones y procedimientos técnicos que permitan: Recogida de datos, Grabación de datos, Conservación de

datos, Elaboración de datos, Modificación de datos, Supresión de datos, Comunicaciones de datos, Consultas de datos e Interconexiones de datos.
3 El apartado de Dirección de Derechos de Acceso del Modelo de Notificación.
4 Artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.
5 En virtud del artículo 4.1 a) de la Directiva 95/46/CE.
6 Véase artículo 17 de la LORTAD y artículo 23 de la Directiva.
7 Véase artículo 43 de la LORTAD y artículo 24 de la Directiva.

3.9 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 1998, el número de ficheros inscritos en el Registro General era de 232.028, de los cuales 28.890 correspondían a inscripciones de titularidad pública y 203.138 a inscripciones de titularidad privada.

RESUMEN DETALLADO SEGÚN LA TITULARIDAD Y AÑO DE INSCRIPCION

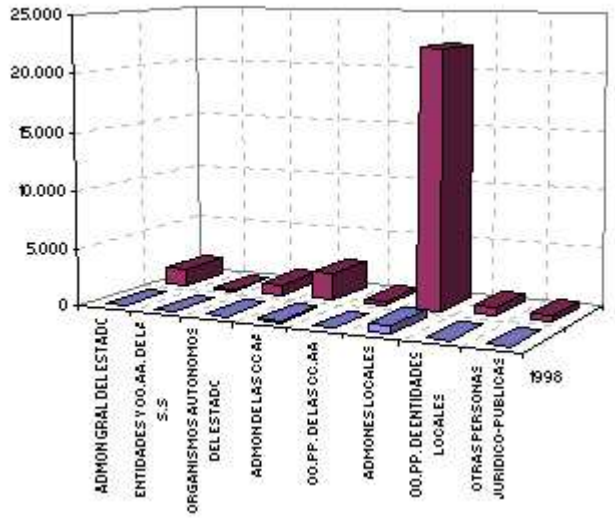
Se recoge en esta tabla el estado de los ficheros a 31 de Diciembre de 1998, en función de la titularidad y año en que se ha realizado la inscripción de los mismos.

AÑO INSCRIPCION	1994	1995	1996	1997	1998
TITULARIDAD PUBLICA	19.833	4.773	1.815	1.522	947
T O T A L	28.890				
TITULARIDAD PRIVADA	189.059	7.911	2.162	1.725	2.281
T O T A L	203.138				
TOTAL AÑO	208.892	12.684	3.977	3.247	3.228
	232.028				

(*) Las cifras que aparecen en esta tabla correspondientes a años anteriores a 1998 no coinciden con las publicadas en memorias anteriores, debido a que durante el año 1998 se han realizado operaciones de supresión sobre ellos.

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

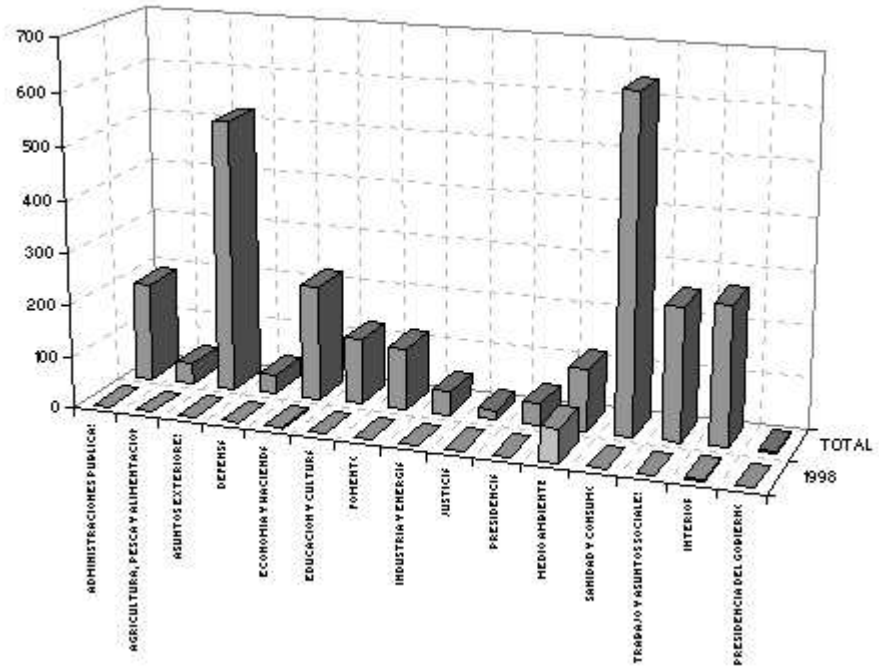
	1998	TOTAL
ADMINISTRACION CENTRAL	**73**	**2.638**
ADMON GRAL DEL ESTADO	40	1.570
ENTIDADES Y OO.AA. DE LA S.S.	0	106
ORGANISMOS AUTONOMOS DEL ESTADO	33	962
ADMINISTRACION CC.AA.	**179**	**2.753**
ADMON DE LAS CC AA	163	2.386
OO.PP. DE LAS CC.AA.	16	368
ADMINISTRACION LOCAL	**677**	**23.031**
ADMONES LOCALES	673	22.243
OO.PP. DE ENTIDADES LOCALES	4	788
OTRAS PERSONAS JURIDICO-PUBLICAS	**18**	**468**
TOTAL	**947**	**28.890**



DISTRIBUCION DE FICHEROS PUBLICOS INSCRITOS DE LA ADMINISTRACION CENTRAL

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

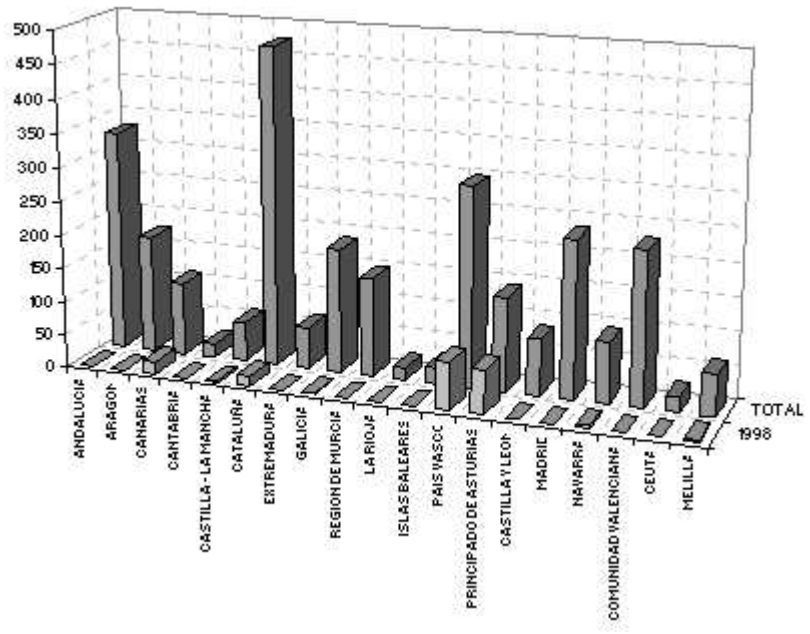
	1998	TOTAL
MINISTERIO DE ADMINISTRACIONES PUBLICAS	0	189
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACION	1	40
MINISTERIO DE ASUNTOS EXTERIORES	0	522
MINISTERIO DE DEFENSA	1	38
MINISTERIO DE ECONOMIA Y HACIENDA	2	221
MINISTERIO DE EDUCACION Y CULTURA	1	126
MINISTERIO DE FOMENTO	0	119
MINISTERIO DE INDUSTRIA Y ENERGIA	0	45
MINISTERIO DE JUSTICIA	0	19
MINISTERIO DE LA PRESIDENCIA	0	42
MINISTERIO DE MEDIO AMBIENTE	64	118
MINISTERIO DE SANIDAD Y CONSUMO	1	636
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	0	253
MINISTERIO DEL INTERIOR	3	266
PRESIDENCIA DEL GOBIERNO	0	4
TOTAL	73	2.638



DISTRIBUCION DE FICHEROS PUBLICOS INSCRITOS POR LAS COMUNIDADES AUTONOMAS

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

COMUNIDAD AUTONOMA	1998	TOTAL
ANDALUCIA	1	328
ARAGON	0	174
CANARIAS	18	107
CANTABRIA	0	20
CASTILLA - LA MANCHA	1	58
CATALUÑA	14	473
EXTREMADURA	0	62
GALICIA	1	185
REGION DE MURCIA	0	146
LA RIOJA	0	19
ISLAS BALEARES	0	25
PAIS VASCO	71	296
PRINCIPADO DE ASTURIAS	65	139
CASTILLA Y LEON	0	84
MADRID	0	234
NAVARRA	4	91
COMUNIDAD VALENCIANA	1	227
CEUTA	0	23
MELILLA	3	62
TOTAL	179	2.753



DISTRIBUCION DE FICHEROS PUBLICOS DE OTRAS PERSONAS JURIDICO PUBLICAS

	1998	TOTAL
CAMARAS DE COMERCIO, INDUSTRIA Y NAVEGACION	0	187
UNIVERSIDADES	18	242
OTROS	0	39
T O T A L	18	468

FICHEROS PUBLICOS DE LA ADMINISTRACION LOCAL INSCRITOS DISTRIBUIDOS POR COMUNIDADES AUTONOMAS 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	
	1998	TOTAL	1998	TOTAL
ANDALUCIA	**23**	**672**	**138**	**5.422**
ALMERIA	0	104	0	950
CADIZ	5	45	57	318
CORDOBA	6	57	17	238
GRANADA	0	168	0	1.182
HUELVA	0	85	0	1.150
JAEN	5	81	30	462
MALAGA	5	41	28	393
SEVILLA	2	91	6	729
ARAGON	**33**	**434**	**80**	**1.967**
HUESCA	24	156	53	536
TERUEL	8	45	24	152
ZARAGOZA	1	233	3	1.279
ASTURIAS	**0**	**44**	**0**	**268**
ILLES BALEARS	**4**	**65**	**26**	**628**
CANARIAS	**11**	**63**	**64**	**386**
PALMAS, LAS	2	24	6	175
SANTA CRUZ DE TENERIFE	9	39	58	211

	ORGANISMOS		FICHEROS	
	1998	TOTAL	1998	TOTAL
CANTABRIA	**2**	**40**	**10**	**178**
CASTILLA-LA MANCHA	**3**	**338**	**13**	**1.830**
ALBACETE	0	72	0	347
CIUDAD REAL	0	107	0	557
CUENCA	1	82	7	556
GUADALAJARA	1	11	3	59
TOLEDO	1	66	3	311
CASTILLA Y LEON	**5**	**499**	**27**	**2.198**
AVILA	2	7	4	19
BURGOS	0	91	0	318
LEON	0	163	0	801
PALENCIA	0	18	0	76
SALAMANCA	0	80	0	338
SEGOVIA	0	14	0	103
SORIA	1	9	4	31
VALLADOLID	2	82	19	355
ZAMORA	0	35	0	157
CATALUÑA	**91**	**496**	**116**	**2.475**
BARCELONA	85	253	95	1.316
GIRONA	2	55	12	347
LLEIDA	2	105	6	394
TARRAGONA	0	83	0	418
COMUNIDAD VALENCIANA	**6**	**309**	**32**	**2.165**
ALICANTE	1	137	13	1.195
CASTELLON DE LA PLANA	0	35	0	225
VALENCIA	5	137	19	745
EXTREMADURA	**3**	**186**	**19**	**1.555**
BADAJOZ	1	155	9	1.390
CACERES	2	31	10	165
GALICIA	**15**	**220**	**60**	**899**
A CORUÑA	6	86	32	434
LUGO	4	39	13	155
OURENSE	2	35	7	131
PONTEVEDRA	3	60	8	179
RIOJA, LA	**0**	**30**	**0**	**131**
MADRID	**5**	**51**	**20**	**648**

	ORGANISMOS		FICHEROS	
	1998	TOTAL	1998	TOTAL
MURCIA	**2**	**35**	**19**	**401**
NAVARRA	**6**	**80**	**6**	**426**
PAIS VASCO	**5**	**178**	**34**	**1.454**
ALAVA	0	39	0	181
GUIPUZCOA	2	66	12	736
VIZCAYA	3	73	22	537
CEUTA	**0**	**0**	**0**	**0**
MELILLA	**0**	**0**	**0**	**0**

FICHEROS PRIVADOS INSCRITOS DISTRIBUIDOS POR COMUNIDADES AUTONOMAS Y PROVINCIAS

	EMPRESAS		FICHEROS	
	1998	TOTAL	1998	TOTAL
ANDALUCIA	**86**	**9.041**	**137**	**17.069**
ALMERIA	4	413	4	804
CADIZ	15	1.637	19	2.546
CORDOBA	6	1.079	11	2.420
GRANADA	11	734	21	1.395
HUELVA	5	621	5	1.002
JAEN	6	825	6	1.743
MALAGA	15	2.006	32	3.400
SEVILLA	24	1.733	39	3.759
ARAGON	**22**	**7.974**	**85**	**13.034**
HUESCA	1	1.801	1	2.493
TERUEL	2	574	2	893
ZARAGOZA	19	5.604	82	9.648
ASTURIAS	**37**	**1.946**	**60**	**3.545**
ILLES BALEARS	**4**	**1.207**	**8**	**2.860**

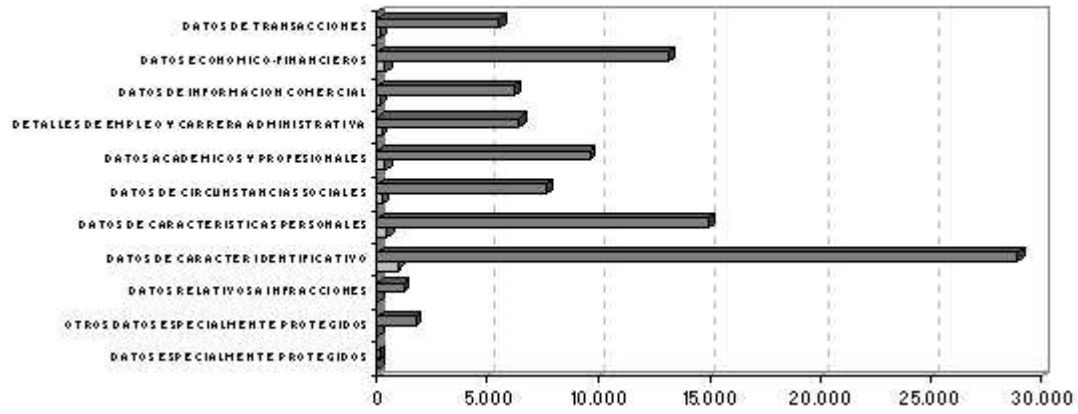
	EMPRESAS		FICHEROS	
	1998	TOTAL	1998	TOTAL
CANARIAS	**19**	**1.215**	**46**	**2.232**
PALMAS, LAS	11	698	25	1.293
SANTA CRUZ DE TENERIFE	8	520	21	939
CANTABRIA	**7**	**562**	**16**	**1.227**
CASTILLA-LA MANCHA	**3**	**2.955**	**12**	**5.162**
ALBACETE	1	911	5	1.408
CIUDAD REAL	2	613	7	1.100
CUENCA	0	521	0	872
GUADALAJARA	0	222	0	523
TOLEDO	0	688	0	1.259
CASTILLA Y LEON	**12**	**4.508**	**14**	**8.304**
AVILA	0	195	0	348
BURGOS	1	1.262	1	2.025
LEON	3	641	5	1.214
PALENCIA	0	232	0	452
SALAMANCA	1	531	1	1.249
SEGOVIA	2	282	2	486
SORIA	0	240	0	388
VALLADOLID	4	894	4	1.596
ZAMORA	1	237	1	546
CATALUÑA	**355**	**30.286**	**623**	**55.386**
BARCELONA	220	22.939	463	42.785
GIRONA	2	2.816	2	4.913
LLEIDA	131	2.818	154	4.564
TARRAGONA	3	1.731	4	3.124
COMUNIDAD VALENCIANA	**72**	**14.287**	**104**	**23.598**
ALICANTE	5	5.634	6	8.989
CASTELLON DE LA PLANA	7	2.316	12	3.976
VALENCIA	60	6.343	86	10.633
EXTREMADURA	**80**	**2.069**	**82**	**3.446**
BADAJOZ	78	1.628	80	2.519
CACERES	2	442	2	927
GALICIA	**17**	**6.412**	**31**	**11.539**
A CORUÑA	9	3.344	16	5.883
LUGO	1	857	1	1.333
OURENSE	0	561	0	1.056
PONTEVEDRA	7	1.654	14	3.267

	EMPRESAS		FICHEROS	
	1998	TOTAL	1998	TOTAL
RIOJA, LA	**9**	**1.672**	**9**	**3.080**
MADRID	**344**	**16.294**	**933**	**37.400**
MURCIA	**11**	**2.754**	**15**	**4.535**
NAVARRA	**8**	**1.697**	**15**	**3.192**
PAIS VASCO	**69**	**3.696**	**90**	**7.359**
ALAVA	5	529	7	1.078
GUIPUZCOA	6	1.832	7	3.617
VIZCAYA	58	1.342	76	2.664
CEUTA	**1**	**53**	**1**	**116**
MELILLA	**0**	**35**	**0**	**53**

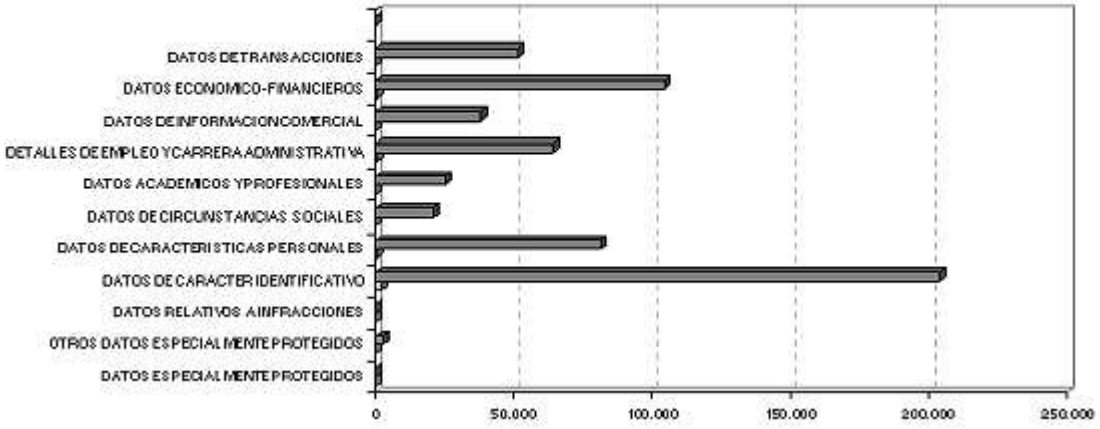
DISTRIBUCION DE FICHEROS SEGÚN LA TIPOLOGIA DE DATOS QUE CONTIENEN

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1998	TOTAL	1998	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	0	56	9	312
OTROS DATOS ESPECIALMENTE PROTEGIDOS	29	1.693	206	3.466
DATOS RELATIVOS A INFRACCIONES	43	1.145	---	---
DATOS DE CARACTER IDENTIFICATIVO	947	28.890	2.281	203.138
DATOS DE CARACTERISTICAS PERSONALES	447	14.938	1.238	81.768
DATOS DE CIRCUNSTANCIAS SOCIALES	218	7.650	418	20.976
DATOS ACADEMICOS Y PROFESIONALES	344	9.587	418	25.941
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	170	6.400	782	64.420
DATOS DE INFORMACION COMERCIAL	158	6.196	350	38.439
DATOS ECONOMICO-FINANCIEROS	344	13.171	1.014	104.354
DATOS DE TRANSACCIONES	162	5.566	415	51.930

FICHEROS DE TITULARIDAD PUBLICA



FICHEROS DE TITULARIDAD PRIVADA



FICHEROS INSCRITOS CON DATOS SENSIBLES

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1998	TOTAL	1998	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	**0**	**56**	**9**	**312**
Ideología	0	37	6	124
Creencias	0	17	1	38
Religión	0	12	4	175
OTROS DATOS ESPECIALMENTE PROTEGIDOS	**29**	**1.693**	**206**	**3.466**
Origen Racial	3	77	2	33
Salud	28	1.671	202	3.439
Vida Sexual	3	342	6	101
DATOS RELATIVOS A INFRACCIONES	**43**	**1.145**	---	---
Infracciones Penales	26	720	---	---
Infracciones Administrativas	37	815	---	---

--- No aplicable a esta titularidad

DISTRIBUCION DE FICHEROS PUBLICOS SEGÚN SU FINALIDAD

	1998	TOTAL
PROCEDIMIENTOS ADMINISTRATIVOS	258	8.177
GESTION TRIBUTARIA Y DE RECAUDACION	229	6.544
GESTION DE ESTADISTICAS INTERNAS	223	7.796
PADRON	203	4.323
GESTION ECONOMICA CON TERCEROS	137	5.814
FUNCION ESTADISTICA PUBLICA	120	5.098
GESTION DE PERSONAL	116	4.106
GESTION DEUDA PUBLICA Y TESORERIA	83	2.421
OTRAS FINALIDADES	61	4.084
CONCESION Y GESTION DE PERMISOS Y LICENCIAS	55	3.159
GESTION DE CATASTROS INMOBILIARIOS RUSTICOS Y URBANOS	47	1.816
ACTUACIONES POLICIALES	40	2.043
GESTION SANCIONADORA	39	2.219
SERVICIO MILITAR	36	2.113
RELACIONES LABORALES Y CONDICIONES DE TRABAJO	33	1.327
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD	31	1.791
SEGURIDAD Y CONTROL INTERNO	29	1.927
PRESTACIONES DE ASISTENCIA SOCIAL	27	1.528
PROCEDIMIENTOS JUDICIALES	27	822
PROMOCION Y GESTION DE EMPLEO	26	760
FORMACION DE PERSONAL	24	1.338
PROTECCION CIVIL	23	1.637
PUBLICACIONES	21	556
OTROS SERVICIOS SOCIALES	19	1.092
PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONOMICAS	18	1.835
SEGURIDAD VIAL	18	1.305
OTRAS ENSEÑANZAS, BECAS Y AYUDAS A ESTUDIANTES	17	947
INVESTIGACIONES CIENTIFICAS O MEDICAS Y ACTIVIDADES ANALOGAS	16	938
NACIONALIDAD	16	940
DEPORTES	15	859
FORMACION PROFESIONAL	15	1.028
INSPECCION Y CONTROL DE SEGURIDAD Y PROTECCION SOCIAL	15	661
AYUDAS ACCESO A VIVIENDA	14	1.012
ACCION SOCIAL EN FAVOR DEL PERSONAL DE ADMONES. PUBLICAS	13	773
GESTION Y CONTROL SANITARIO	12	1.137
SERVICIOS SOCIALES A MINUSVALIDOS	12	1.022
SERVICIOS SOCIALES DE LA TERCERA EDAD	12	722
FOMENTO Y APOYO A ACTIVIDADES ARTISTICAS Y CULTURALES	11	305
PROMOCION Y SERVICIOS A LA JUVENTUD	11	634
PROMOCION Y SERVICIOS A LA MUJER	10	570
RELACIONES COMERCIALES CON EL EXTERIOR	10	402
EDUCACION INFANTIL Y PRIMARIA	9	712
PRESTACION SOCIAL SUSTITUTORIA	9	829
PROTECCION DEL MENOR	9	599
EDUCACION UNIVERSITARIA	8	433
PRESTACIONES A LOS DESEMPLEADOS	8	946

DISTRIBUCION DE FICHEROS PRIVADOS SEGÚN SU FINALIDAD

	1998	TOTAL
GESTION CONTABLE, FISCAL Y ADMINISTRATIVA	753	133.328
GESTION DE CLIENTES	682	64.198
OBTENCION DE ESTADISTICAS DIVERSAS	639	54.489
GESTION DE COBROS Y PAGOS	585	87.874
PUBLICIDAD PROPIA	518	19.521
GESTION DE PERSONAL	484	53.083
SEGURIDAD Y CONTROL INTERNO	312	10.058
HISTORICOS DE RELACIONES COMERCIALES	308	32.019
PROSPECCIONES DE MERCADO	234	6.908
OTRAS FINALIDADES	218	8.561
ENCUESTAS DE OPINION	156	2.896
SELECCION DE PERSONAL	140	3.561
PUBLICIDAD PARA TERCEROS	130	2.720
OTRO TIPO DE SEGUROS	122	5.560
SEGUROS DE VIDA Y SALUD	113	5.460
INFORMACION SOBRE LA SOLVENCIA PATRIMONIAL Y CREDITO	113	3.497
AUDITORIAS, ASESORIAS Y SERVICIOS RELACIONADOS	111	13.415
INVESTIGACION	109	533
PRESTACIONES SOCIALES	98	13.609
HISTORIAL CLINICO	97	1.936
OTROS SERVICIOS FINANCIEROS	92	3.945
GESTION Y CONTROL SANITARIO	83	1.735
CUENTA DE CREDITO	61	4.306
FORMACION PROFESIONAL	61	1.487
SERVICIOS DE TELECOMUNICACION	59	1.103
GESTION ADMINISTRATIVA DE LOS INTEGRANTES DE CLUBES	57	2.086
SEGURIDAD	51	682
MEDIOS DE COMUNICACION SOCIAL	49	480
OTRAS ENSEÑANZAS	48	1.390
GESTION DE FONDOS DE PENSIONES Y SIMILARES	34	2.225
GESTION DE TARJETAS DE CREDITO Y SIMILARES	31	1.635
INVESTIGACIONES CIENTIFICAS Y MEDICAS	28	703
CUENTA DE DEPOSITO	25	2.334
REGISTRO DE ACCIONES Y OBLIGACIONES	25	2.115
EDUCACION UNIVERSITARIA	25	745
EDUCACION INFANTIL PRIMARIA	21	475
GESTION DE PATRIMONIOS	19	2.012
EDUCACION SECUNDARIA	18	536
EDUCACION ESPECIAL	14	296
RESERVA Y EMISION DE BILLETES	12	313
INVESTIGACIONES PRIVADAS A PERSONAS	1	82

DISTRIBUCION DE EMPRESAS INSCRITAS SEGÚN LA CLASIFICACION NACIONAL DE ACTIVIDADES ECONOMICAS DE PERTENENCIA

	C N A E	EMPRESAS		FICHEROS	
		1998	TOTAL	1998	TOTAL
1	AGRICULTURA, GANADERIA, CAZA Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	4	2.024	11	3.110
2	SELVICULTURA, EXPLOTACION FORESTAL Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	1	99	1	165
5	PESCA, ACUICULTURA Y ACTIVIDADES DE LOS SERVICIOS RELACIONADOS CON LAS MISMAS	0	251	0	444
10	EXTRACCION Y AGLOMERACION DE ANTRACITA, HULLA, LIGNITO Y TURBA	0	88	0	141
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	8	122	9	228
12	EXTRACCION DE MINERALES DE URANIO Y TORIO	3	33	4	64
13	EXTRACCION DE MINERALES METALICOS	3	40	4	66
14	EXTRACCION DE MINERALES NO METALICOS NI ENERGETICOS	2	311	2	525
15	INDUSTRIA DE PRODUCTOS ALIMENTICIOS Y BEBIDAS	37	2.844	71	5.905
16	INDUSTRIA DEL TABACO	6	49	32	249
17	INDUSTRIA TEXTIL	4	1.237	7	2.235
18	INDUSTRIA DE LA CONFECCION Y DE LA PELETERIA	0	678	0	1.136
19	PREPARACION, CURTIDO Y ACABADO DEL CUERO; FABRICACION DE ARTICULOS DE MARROQUINERIA Y VIAJE; ARTICULOS DE GUARNICIONERIA TALABARTERIA Y ZAPATERIA	3	759	3	1.157
20	INDUSTRIA DE LA MADERA Y DEL CORCHO, EXCEPTO MUEBLES; CESTERIA Y ESPARTERIA	5	861	6	1.346
21	INDUSTRIA DEL PAPEL	3	439	10	867
22	EDICION, ARTES GRAFICAS Y REPRODUCCION DE SOPORTES GRABADOS	35	1.519	103	3.953
23	COQUERIAS, REFINO DE PETROLEO TRATAMIENTO DE COMBUSTIBLES NUCLEARES	0	62	0	128
24	INDUSTRIA QUIMICA	13	1.088	20	2.839
25	FABRICACION DE PRODUCTOS DE CAUCHO Y MATERIAS PLASTICAS	4	952	5	1.965
26	FABRICACION DE OTROS PRODUCTOS MINERALES NO METALICOS	2	1.043	3	1.978
27	METALURGIA	3	465	6	894
28	FABRICACION DE PRODUCTOS METALICOS, EXCEPTO MAQUINARIA Y EQUIPO	10	1.548	13	2.658
29	INDUSTRIA DE LA CONSTRUCCION DE MAQUINARIA Y EQUIPO MECANICO	4	934	8	1.781
30	FABRICACION DE MAQUINAS DE OFICINA Y EQUIPOS INFORMATICOS	1	78	1	145
31	FABRICACION DE MAQUINARIA Y MATERIAL ELECTRICO	1	780	1	1.592
32	FABRICACION DE MATERIAL ELECTRONICO; FABRICACION DE EQUIPO Y APARATOS DE RADIO, TELEVISION Y COMUNICACIONES	3	323	3	604
33	FABRICACION DE EQUIPO E INSTRUMENTOS MEDICO-QUIRURGICOS, DE PRECISION, OPTICOS Y RELOJERIA	3	176	5	330
34	FABRICACION DE VEHICULOS DE MOTOR, REMOLQUES Y SEMIRREMOLQUES	6	335	9	812
35	FABRICACION DE OTRO MATERIAL DE TRANSPORTE	1	130	1	267
36	FABRICACION DE MUEBLES; OTRAS INDUSTRIAS MANUFACTURERAS	9	1.431	11	2.469
37	RECICLAJE	0	73	0	106
40	PRODUCION Y DISTRIBUCION DE ENERGIA ELECTRICA, GAS, VAPOR Y AGU CALIENTE	2	189	4	451
41	CAPTACION, DEPURACION Y DISTRIBUCION DE AGUA	8	237	18	931
45	CONSTRUCCION	46	6.404	52	9.845
50	VENTA, MANTENIMIENTO Y REPARACION DE VEHICULOS DE MOTOR, MOTOCICLETAS Y CICLOMOTORES; VENTA AL POR MENOR DE COMBUSTIBLE PARA VEHICULOS DE MOTOR	32	6.087	69	11.458
51	COMERCIO AL POR MAYOR E INTERMEDIARIOS DEL COMERCIO, EXCEPTO DE VEHICULOS DE MOTOR Y MOTOCICLETAS	55	11.903	79	21.305

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

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
SOPORTE	**1.998**	**TOTAL**	**1.998**	**TOTAL**
SOPORTE PAPEL	853	27.451	1.828	164.366
SOPORTE INFORMATICO/MAGNETICO	410	11.375	812	28.955
VIA TELEMATICA	148	3.176	370	5.431
OTROS SOPORTES	34	3.090	245	33.674
PROCEDENCIA DE LOS DATOS	**1.998**	**TOTAL**	**1.998**	**TOTAL**
ENTIDAD PRIVADA	51	3.063	312	25.754
ADMINISTRACIONES PUBLICAS	415	10.688	107	3.567
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	846	27.092	2.087	182.718
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	68	3.915	156	4.205
FUENTES ACCESIBLES AL PUBLICO	45	2.760	213	8.944
PROCEDIMIENTO DE RECOGIDA	**1.998**	**TOTAL**	**1.998**	**TOTAL**
ENCUESTAS O ENTREVISTAS	96	3.800	557	44.132
DECLARACIONES O FORMULARIOS	779	24.908	1.236	85.541
REGISTROS PUBLICOS	193	6.613	93	3.852
TRANSMISION ELECTRONICA DE DATOS	131	4.590	259	3.737
DIRECTORIOS TELEFONICOS, COMERCIALES, CATALOGOS, MEMORIAS	20	1.835	164	9.140
OTROS PROCEDIMIENTOS DE RECOGIDA	145	2.829	619	69.373

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

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1998	**TOTAL**	**1998**	**TOTAL**
EXISTE CONSENTIMIENTO DE LOS AFECTADOS	138	6.916	434	17.266
EXISTE UNA RELACION JURIDICA CUYO DESARROLLO, CONTROL Y CUMPLIMIENTO IMPLICA NECESARIAMENTE LA CONEXION DEL FICHERO CON FICHEROS DE TERCEROS	95	4.119	219	12.796
EXISTE UNA NORMA REGULADORA QUE LAS AUTORIZA	592	10.547	323	19.657
SE TRATA DE DATOS RECOGIDOS DE FUENTES ACCESIBLES AL PUBLICO	81	4.844	86	2.309
CORRESPONDEN A COMPETENCIAS IDENTICAS O QUE VERSAN SOBRE LAS MISMAS MATERIAS, EJERCIDAS POR OTRAS ADMINISTRACIONES PUBLICAS	238	10.579	---	---
SON DATOS OBTENIDOS O ELABORADOS CON DESTINO A OTRA ADMINISTRACION PUBLICA	183	9.405	---	---
TOTAL FICHEROS INSCRITOS CON CESIONES	**649**	**17.014**	**649**	**34.655**

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

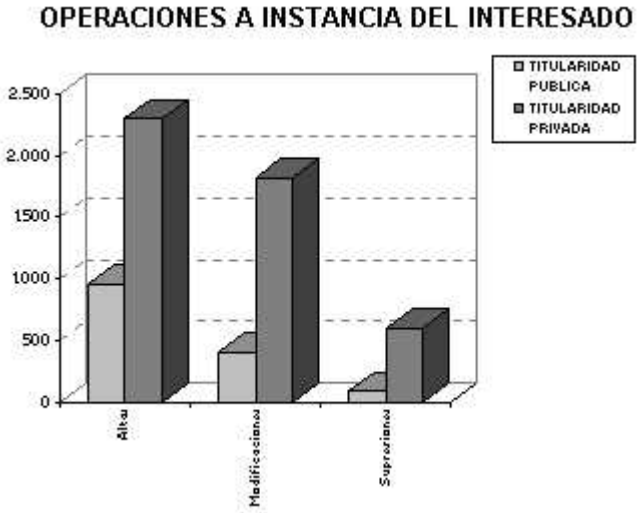
INTERNACIONALES DE DATOS

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	1998	TOTAL	1998	TOTAL
SE AMPARA EN TRATADO O CONVENIO DEL QUE ESPAÑA FORMA PART	0	39	1	4
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	0	9	0	0
TIENE POR OBJETO INTERCAMBIAR DATOS DE CARACTER MEDICO Y ASI LO EXIGE EL TRATAMIENTO DEL AFECTADO O LA INVESTIGACION EPIDEMIOLOGICA	1	6	0	6
SE REFIERE A TRANSFERENCIAS DINERARIAS	0	15	1	50
SE EFECTUA CON DESTINO A ALGUN PAIS DE LOS CITADOS EN EL REGLAMENTO CON NIVEL DE PROTECCION EQUIPARABLE	2	46	49	841
SE EFECTUA CON AUTORIZACION DEL DIRECTOR DE LA AGENCIA	0	0	16	145
TOTAL FICHEROS CON TRANSFERENCIAS INTERNACIONALES	**2**	**50**	**50**	**933**

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 1998 SOBRE FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCION DE DATOS SEGÚN LA TITULARIDAD Y TIPO DE OPERACION

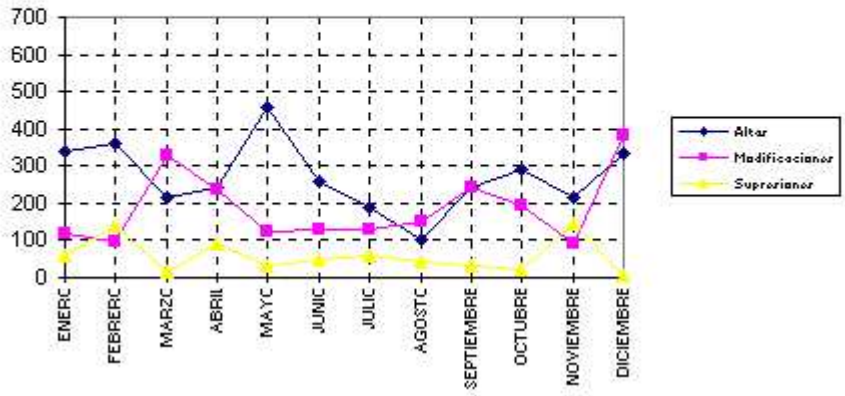
	TITULARIDAD PUBLICA	TITULARIDAD PRIVADA	TOTAL
OPERACIONES A INSTANCIA DEL RESPONSABLE			
Altas	957	2.296	3.253
Modificaciones	408	1.817	2.225
Supresiones	91	600	691
T O T A L	1.456	4.713	6.169
OPERACIONES REALIZADAS DE OFICIO			
Altas	0	0	0
Modificaciones	1.697	1.782	3.479
Supresiones	2	541	543
T O T A L	1.699	2.323	4.022
TOTALES	**3.155**	**7.036**	**10.191**

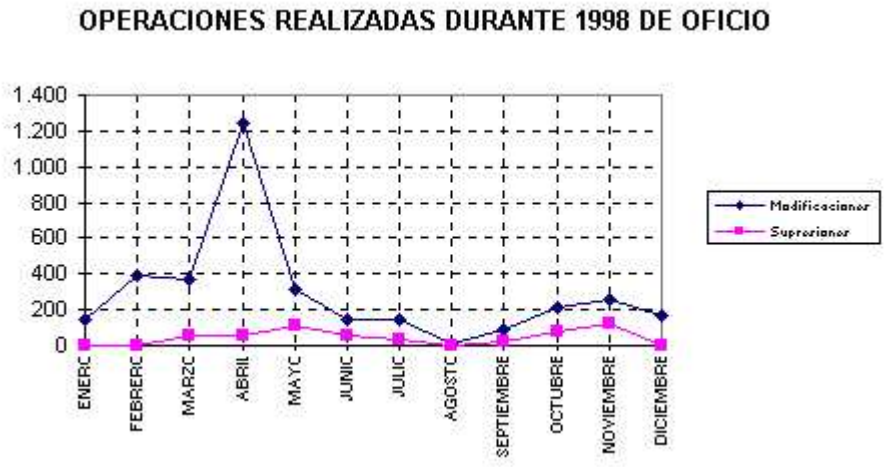


RESUMEN DE OPERACIONES REALIZADAS DURANTE EL AÑO 1998 SOBRE FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCION DE DATOS POR MESES

	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTA
OPERACIONES A INSTANCIA DEL INTERESADO													
Altas	339	359	217	243	457	261	190	103	244	291	214	335	3.2
Modificaciones	120	99	328	235	125	130	128	152	241	194	89	384	2.2
Supresiones	60	139	15	94	33	47	57	43	30	22	143	8	6
T O T A L	519	597	560	572	615	438	375	298	515	507	446	727	6.1
OPERACIONES DE OFICIO													
Modificaciones	147	388	366	1.244	311	150	143	10	85	218	253	164	3.4
Supresiones	2	2	52	54	116	61	32	0	27	74	122	1	5
T O T A L	149	390	418	1.298	427	211	175	10	112	292	375	165	4.0
TOTALES	**668**	**987**	**978**	**1.870**	**1.042**	**649**	**550**	**308**	**627**	**799**	**821**	**892**	**10.1**

OPERACIONES REALIZADAS DURANTE 1998 A INSTANCIA DEL INTERESADO





4 LA INSPECCIÓN DE DATOS.

4.1. INTRODUCCIÓN

El artículo 27 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 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 se recogen en el artículo 39 de la Ley Orgánica 5/1992.

Esta potestad, tal y como la describe la Ley Orgánica 5/1992, consiste, fundamentalmente, en la revisión y examen *in situ* de los ficheros y sistemas informáticos en los que se procesen datos de carácter personal y en la obtención de toda aquella información relevante para el cometido de los fines de la Agencia.

Como lógico correlato de esta capacidad de acceso a la información de organizaciones públicas y privadas, se establece el deber de guardar secreto que tienen los funcionarios que ejerzan la función inspectora respecto de todas aquellas informaciones que conozcan en el ejercicio de dicha tarea.

Por lo que se refiere a la información de carácter general relativa a la actividad de la Inspección, a lo largo del año 1998 se iniciaron, por parte de la misma, 493 Expedientes 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, procedentes, en su mayor parte, de denuncias presentadas por los ciudadanos ante la Agencia de Protección de Datos.

De los 493 expedientes arriba mencionados, 312 correspondieron a expedientes de investigación, 27 a expedientes de información previa y 154 correspondieron a reclamaciones por la no atención de los derechos de acceso, rectificación o cancelación.

Por otra parte, en el año 1998, de los 312 expedientes de investigación, se resolvieron 191, además de otros 171 expedientes que fueron abiertos en 1997 y cuya tramitación continuó en 1998, lo que hace un total de 362 expedientes cerrados. Además, estas cifras suponen que se resolvieron en el mismo año prácticamente dos tercios de los expedientes que tuvieron su entrada en 1998.

Asimismo, se finalizó la tramitación de los 27 expedientes de información previa que no dieron lugar a expediente de investigación debido, en su mayor parte, a que los afectados no proporcionaron la información requerida desde la Inspección y que era imprescindible para poder continuar la tramitación de los mismos.

Por lo que se refiere a los procedimientos de tutela de los derechos, en 1998 se iniciaron 154, de los que se resolvieron 117, a los que hay que sumar otros 37 procedimientos correspondientes a tutelas iniciadas en 1997.

Por otro lado, en lo referente a la tramitación de procedimientos sancionadores y procedimientos de Administraciones Públicas, se resolvieron 147 y 6 respectivamente. Además, se elaboraron 292 resoluciones motivadas de archivo de las actuaciones.

En los gráficos I y II podemos observar la distribución geográfica, tanto por provincia del denunciado como por provincia del denunciante, de todos los expedientes a los que nos hemos referido.

GRÁFICO I

(expedientes por provincia denunciante)

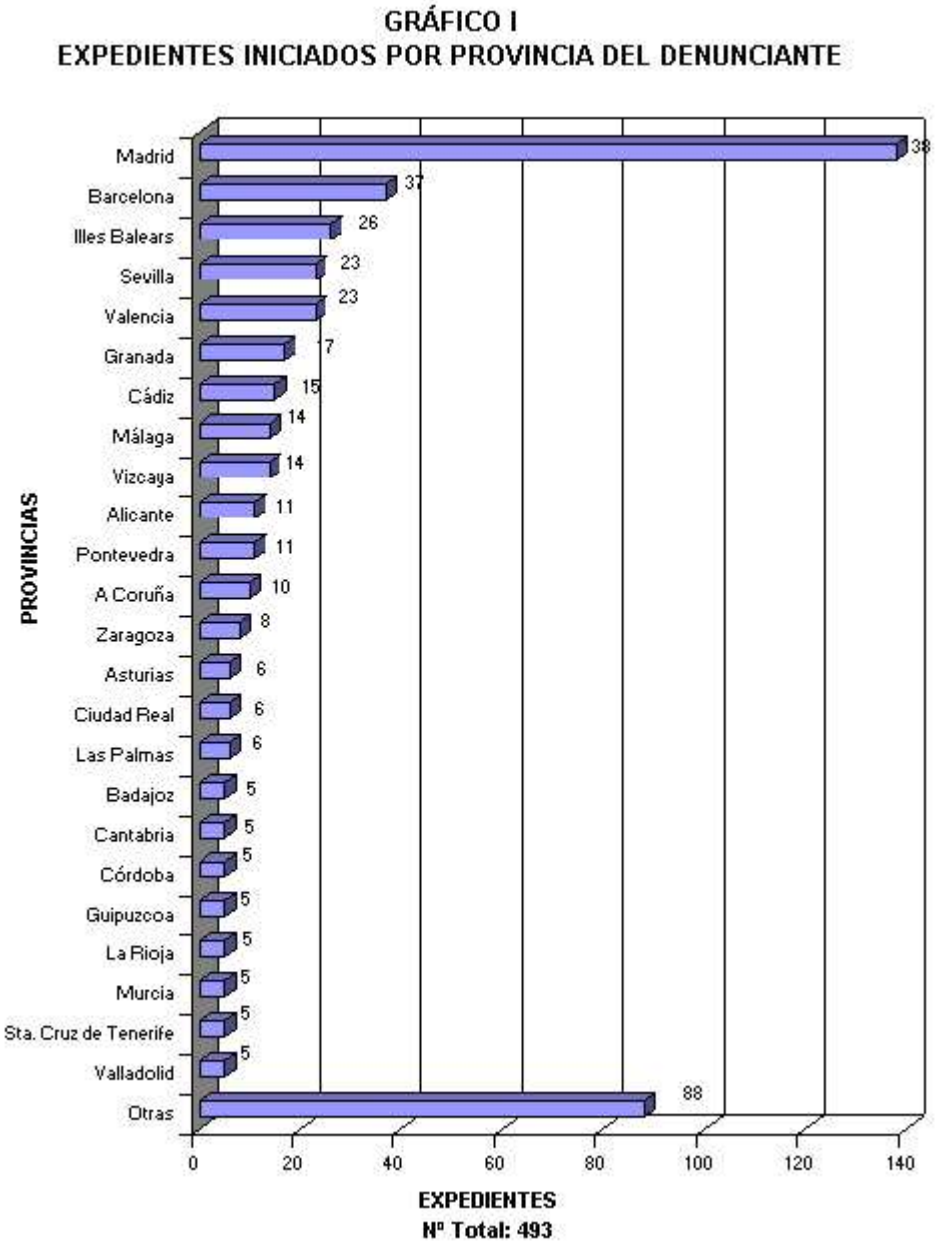
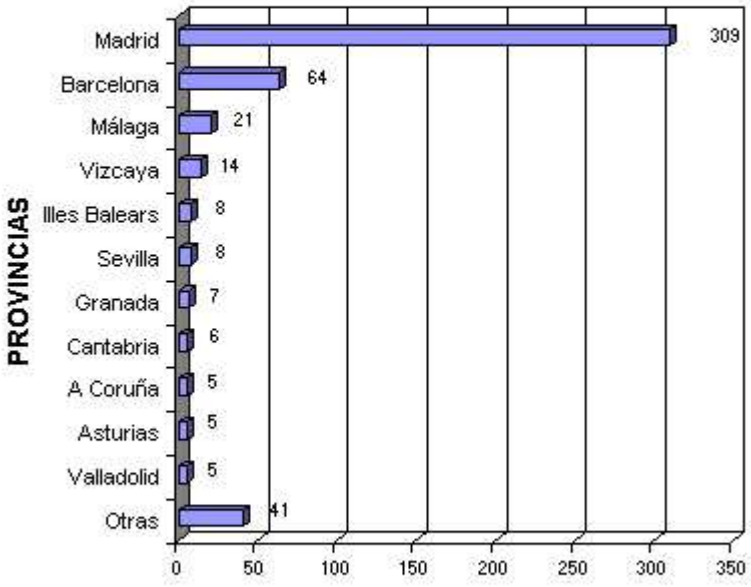


GRÁFICO II
(expedientes por provincia denunciado)

GRÁFICO II

EXPEDIENTES INICIADOS POR PROVINCIA DEL DENUNCIADO



Por otra parte, en los gráficos III a V podemos apreciar, de forma detallada, la distribución por sectores de actividad de cada uno de los tipos de expedientes mencionados: información previa, investigación y tutela de los derechos, habiéndose preferido hacerlo así a diferencia de años anteriores en los que se ofrecía esta información de forma conjunta porque cada uno de ellos tiene su propia especificidad.

GRÁFICO III
(información previa por sectores denunciado)

GRÁFICO III

INFORMACIÓN PREVIA POR SECTORES

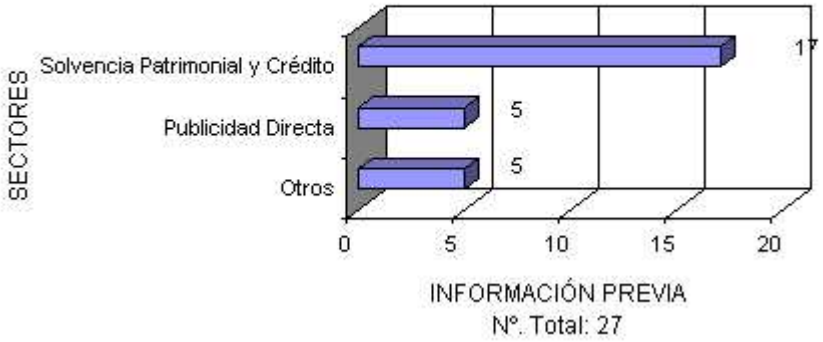


GRÁFICO IV
(investigación por sectores investigado)

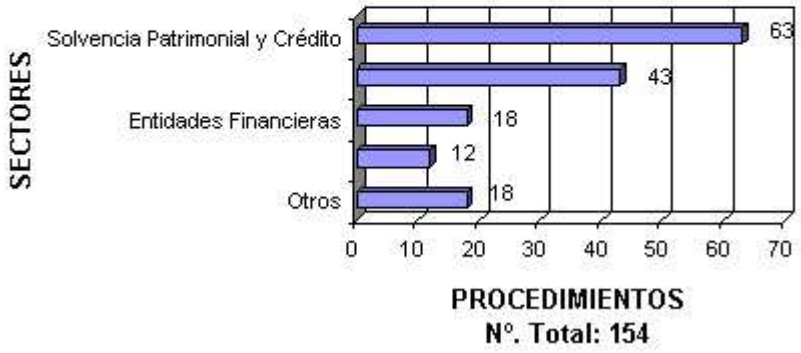
GRÁFICO IV

EXPEDIENTES DE INVESTIGACIÓN POR SECTORES

GRÁFICO V
(tutela de los derechos por sectores)

GRÁFICO V

PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR SECTORES



Si establecemos una comparación con las cifras del año 1997, se observa que el número de expedientes tramitados ha disminuido con respecto a dicho año. Ello ha venido motivado por un descenso en el número de denuncias recibidas en la Agencia de Protección de Datos y, fundamentalmente, en los sectores que más incidencia han tenido tradicionalmente en la entrada de reclamaciones: solvencia patrimonial y crédito (218 en 1997 frente a 148 en 1998), entidades financieras (84 frente a 58) y publicidad directa (126 en 1997 frente a 100 en 1998).

La razón que puede justificar este descenso en la entrada de denuncias es que, tanto la labor que ha venido realizando la Agencia como el progresivo conocimiento de la legislación en materia de protección de datos en las empresas de los

sectores mencionados, ha propiciado que se establecieran procedimientos para garantizar una mejor atención de los derechos de los ciudadanos (especialmente los relativos a acceso, rectificación y cancelación). Por otro lado, han disminuido las denuncias que hacían referencia a la utilización de datos procedentes del censo electoral en campañas de publicidad, habiéndose reducido, en la misma proporción, la constatación por parte de la Inspección de la Agencia de Protección de Datos de la utilización de dicho fichero en la elaboración de listas de destinatarios de publicidad.

Por otro lado, también se puede apreciar que, a lo largo del año 1998, la Agencia ha optado por la vía del procedimiento de tutela de los derechos en lugar de por el de expediente de investigación cuando, de la reclamación efectuada por el ciudadano, se deducía claramente que su principal interés era que se le rectificaran o cancelaran datos que consideraba erróneos o bien que se le manifestara la procedencia de determinados datos personales utilizados por un tercero. Todo ello sin perjuicio de la posterior incoación del correspondiente procedimiento sancionador si durante la tramitación de la tutela de derechos se ponía de manifiesto la posible vulneración de alguno de los preceptos de la Ley Orgánica 5/1992.

Asimismo hay que mencionar que la menor actividad de la Inspección en lo que a la tramitación de denuncias de los ciudadanos se refiere, ha venido compensada con el incremento significativo de las actuaciones en el marco de inspecciones sectoriales encaminadas a conocer en profundidad el estado y grado de cumplimiento de la normativa sobre protección de datos personales en determinados sectores de actividad, con el fin último de realizar una política preventiva que mejor garantice los derechos de los ciudadanos.

En esta línea, en el año 1997 sólo fue posible revisar, dentro de planes sectoriales, los ficheros de un conjunto de Policías Locales. Por el contrario, en el año 1998 se ha procedido a una revisión en profundidad de los sistemas de información de Telefónica, dentro de un plan más ambicioso que se irá completando con otros operadores de telecomunicaciones. También se han revisado exhaustivamente los sistemas de las mayores entidades dedicadas a la información sobre solvencia patrimonial y crédito, de una muestra de las más grandes compañías aseguradoras españolas, a la revisión de la Oficina SIRENE española, órgano de colaboración policial establecido en el marco del Convenio de Schengen y a la inspección de diversas salas de bingo repartidas entre las provincias de Valencia, Bilbao, Madrid, Barcelona y Sevilla, destinada a comprobar el cumplimiento de lo que establece la Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

Por otra parte, en el año 1998 se llevaron a cabo 182 inspecciones in situ. La reducción de las realizadas en los sectores de solvencia patrimonial y crédito y publicidad directa es congruente con la disminución del número de denuncias relativas a dichos sectores y ha permitido el empleo de los recursos de la Inspección en las grandes inspecciones sectoriales mencionadas anteriormente.

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

GRÁFICO VI
(inspecciones por provincias)

GRÁFICO VI

INSPECCIONES REALIZADAS POR PROVINCIAS

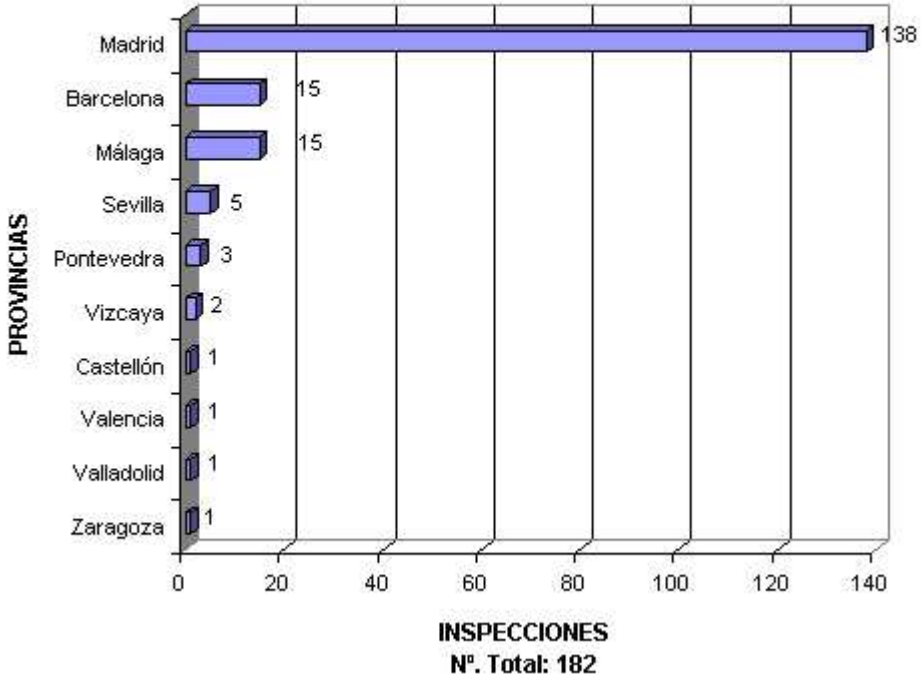
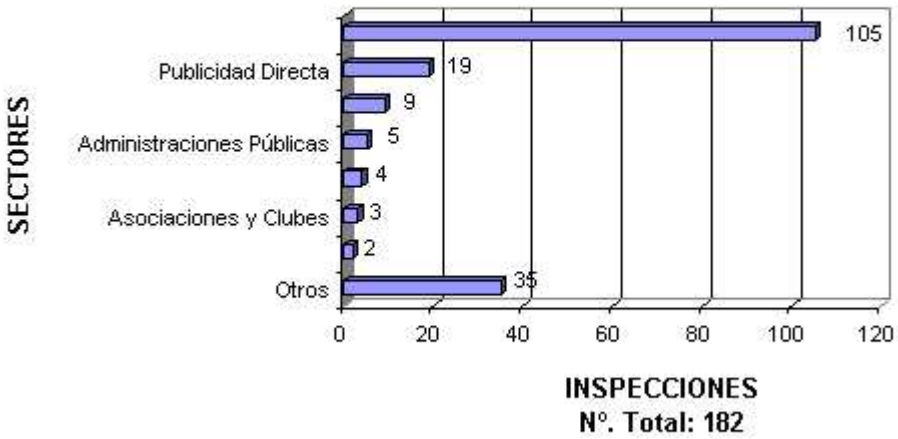


GRÁFICO VII
(inspecciones por sectores investigados)

GRÁFICO VII

INSPECCIONES REALIZADAS POR SECTORES



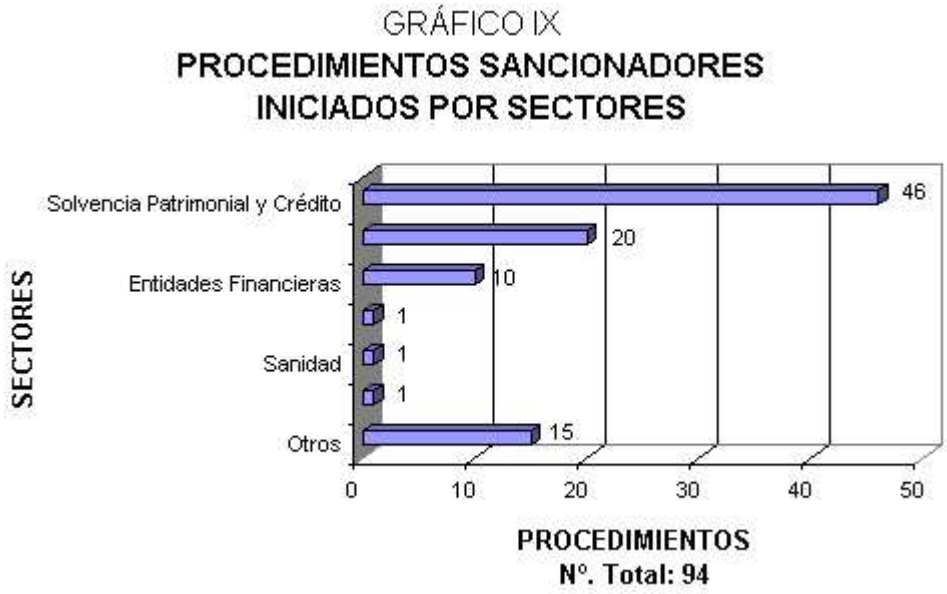
Como consecuencia de las actividades de la Inspección, se procedió a la apertura de 94 Procedimientos Sancionado - res y 9 Procedimientos de Infracción de Administraciones Públicas, correspondiendo 6 de ellos a la Administración

General del Estado, 2 a la Administración Local y 1 a la Administración Autonómica.

Por lo que se refiere a procedimientos sancionadores resueltos a lo largo de 1998, se produjeron 147 resoluciones, que dieron lugar a la imposición de 4 sanciones muy graves, 72 graves y 46 leves, declarándose la no responsabilidad en 44 casos 1.

GRÁFICO VIII
(procedimientos sancionadores por provincia denunciado)

GRÁFICO IX
(procedimientos sancionadores por sectores denunciado)



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 el presente apartado se analizarán las actuaciones llevadas a cabo por la Inspección de Datos en el ámbito de la Administración General del Estado (AGE) excluyendo aquellos organismos que por su idiosincrasia se detallaran en apartados específicos como son las relativas al sector Sanitario y a las Fuerzas y Cuerpos de Seguridad.

Durante 1998 se ha procedido a la apertura de diecinueve expedientes de investigación relacionados con ficheros gestionados por la AGE con objeto de realizar actuaciones para constatar la posible vulneración de la Ley Orgánica 5/1992. Las citadas actuaciones han sido iniciadas en un caso de oficio, en tres de ellas a instancias de organizaciones sindicales y el resto por reclamaciones formuladas por ciudadanos.

No obstante, podemos destacar como en años anteriores el número sorprendentemente bajo de reclamaciones en este sector con respecto al número total de actuaciones llevadas a cabo por la Inspección de Datos. Otro dato importante a considerar es el gran número de organismos incluidos en este sector y que, algunos de ellos, disponen de los ficheros automatizados con datos personales más voluminosos del país y de gran riqueza con respecto a su contenido.

Las organismos de la AGE que han sido objeto de investigación son:

Administración Estatal de Administración Tributaria (en adelante AEAT)
Dirección General de Tráfico
Instituto Nacional de la Seguridad Social
Instituto Nacional de Empleo
Dirección General de Instituciones Penitenciarias
Ministerio de Educación y Cultura
Dirección General de Objeción de Conciencia
Universidad Nacional de Educación a Distancia.
Dirección General del Catastro

No obstante, el organismo sobre el que se han centrado una gran parte de las actuaciones, como el año anterior, ha sido la AEAT. Ello no debe sorprender dado que la misma dispone de información relativa a una gran parte de la población española y de una gran riqueza desde el punto de vista económico y financiero. Entre las actividades llevadas a cabo por la Inspección de Datos relativas al citado organismo, debemos hacer especial mención a la denuncia formulada por una organización sindical, en la que se ponía de manifiesto la vulneración de la Ley Orgánica 5/1992, por una posible cesión de datos tributarios de los ciudadanos a una empresa privada con objeto de la prestación de servicios relacionados con la campaña del Impuesto sobre la Renta de las Personas Físicas (IRPF) del ejercicio 1997. Los mismos hechos también fueron objeto de investigación durante el año anterior. Como resultado de las investigaciones realizadas, no se ha podido constatar, al igual que en el año anterior, la existencia de actuaciones contrarias a lo establecido en la normativa de protección de datos, ni por parte de la AEAT, ni por parte de la empresa que prestataria de los servicios especificados.

Atendiendo a la naturaleza de las reclamaciones presentadas ante la Agencia con respecto a su tipificación por posible vulneración de la Ley Orgánica 5/1992 las podemos agrupar en:

Cesión de datos por parte del responsable del fichero a otras Administraciones Públicas o a entidades privadas

Falta del deber de secreto por parte del responsable del fichero o de quienes intervienen en cualquier fase del tratamiento

Tratamiento de datos de carácter personal sin recabar el consentimiento de las personas afectadas

En la mayor parte de las actuaciones no se ha podido constatar la existencia de posibles infracciones a la Ley Orgánica 5/1992 y por consiguiente se ha procedido al archivo de las actuaciones. No obstante, a continuación se detallan algunos que por sus características se consideran de especial interés:

En la reclamación presentada ante la Agencia un ciudadano manifiesta que la AEAT emitió un certificado del Impuesto sobre la Renta a partir de una solicitud cumplimentada su nombre y, cuya firma, al parecer, había sido suplantada y sin la preceptiva presentación del DNI.

Un funcionario adscrito a la Dirección General de Instituciones Penitenciarias ha puesto en conocimiento de la Agencia que la citada Dirección General ha facilitado datos relativos a su puesto de trabajo (que no habían sido publicados en el BOE) a una empresa que se dedica a la confección de un fichero en el que se detallan ciertos datos profesionales de un gran número de funcionarios y que, posteriormente, se comercializa entre entidades públicas y privadas. De las actuaciones practicadas por la Inspección se encontraron indicios de la posible existencia de una cesión de datos no procedentes de fuentes accesibles al público y sin que existiera el consentimiento del afectado.

Por parte de la Tesorería General de la Seguridad Social se procedió a la cesión de los datos de afiliación de un trabajador al Ayuntamiento de Albacete para el cobro de una multa de tráfico. Los citados hechos pueden ser constitutivos de una infracción, por parte de la Tesorería General de la Seguridad Social, del artículo 11 de la Ley Orgánica 5/1992, que establece que "los datos de carácter personal objeto de tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario". Igualmente los anteriores hechos pueden ser constitutivos de una infracción, por parte del Ayuntamiento, del artículo 6 de la Ley Orgánica que establece que " el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que una Ley disponga otra cosa".

El afectado pone en conocimiento de la Agencia que ha recibido en el buzón de su domicilio particular un documento que podría ser copia de la consulta realizada de sus datos personales al Sistema de Información de Afiliación de la Tesorería General de la Seguridad Social. Realizada las oportunas actuaciones por parte de la Inspección de Datos se concluye que se han realizado consultas de los datos personales del afectado por parte de un funcionario destinado en la Dirección General de Costes de Personal del Ministerio de Economía y Hacienda. En la fecha en que se desarrollaron los hechos, la citada Dirección General no estaba realizando actuaciones que justificaran consultas sobre los datos personales del afectado, pudiendo, por lo tanto, haberse vulnerado el deber de secreto previsto en el artículo 10 de la Ley Orgánica 5/1992.

4.2.2. FICHEROS DE FUERZAS Y CUERPOS DE SEGURIDAD

Durante el año 1998 no se ha recibido ninguna reclamación relacionada con las actividades del sector de las Fuerzas y Cuerpos de Seguridad, por lo que todas las actuaciones se realizaron de oficio. En concreto, se inspeccionaron los ficheros automatizados de la Oficina SIRENE, unidad encargada de gestionar los intercambios complementarios de información relativos al Sistema de Información Schengen, así como un sistema piloto de atención telefónica de denuncias que puso en marcha la Dirección General de la Policía.

4.2.2.1. Sistema de Información Schengen. Oficina SIRENE

La Oficina SIRENE (Supplementary Information Request at the National Entry) se encuadra en la Dirección General de la Policía, bajo la dirección y responsabilidad de la Subdirección General Operativa. El Área Schengen, dependiente del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, es el encargado de proporcionar el soporte técnico en lo concerniente a la gestión de los tratamientos automatizados llevados a cabo por esa Oficina.

Las funciones desempeñadas por la Oficina SIRENE dentro del Sistema de Información Schengen (SIS), consisten en la gestión, envío y recepción de información complementaria a los señalamientos introducidos en el SIS, la cual proviene de las Oficinas SIRENE de terceros países y de las propias autoridades nacionales. Dicho intercambio de información ha sido estandarizado en el "Manual SIRENE" que recoge las especificaciones y requerimientos de los intercambios de información entre las diferentes Oficinas SIRENE, definiéndose para ello unos formularios estándar.

Como consecuencia de una importante fuga de información que se produjo en la Oficina SIRENE belga y que puso en peligro la seguridad del SIS, la Autoridad de Control Común de Schengen (ACCS) realizó un requerimiento a las autoridades de protección de datos de los países firmantes del Convenio para que verificaran el estado de la seguridad de las oficinas SIRENE nacionales. Por ello, la Agencia inició una inspección de oficio con el objeto de comprobar el estado de la seguridad de la Oficina SIRENE nacional y, en concreto, la aplicación del artículo 118 del Acuerdo de Schengen, que recoge las medidas de seguridad que deben establecerse en las instalaciones donde residan los ficheros nacionales del SIS.

Durante el desarrollo de la inspección se comprobó que la implantación de las medidas de seguridad exigidas en el artículo 118 del Convenio de Aplicación del Acuerdo Schengen era, en general, satisfactoria, aunque se detectaron algunos aspectos de las mismas que podían mejorarse. Por ello, la Agencia elaboró una serie de recomendaciones con el fin de incrementar los niveles de protección de la información recogida en los equipos informáticos de la Oficina SIRENE, dando traslado de las mismas al Ministerio del Interior.

4.2.2.2. Sistema de atención de denuncias telefónicas

Como consecuencia de la puesta en marcha por parte de la Dirección General de la Policía de un sistema de atención telefónica de denuncias, que se contrató a una empresa externa, se inició expediente de oficio con el fin de verificar la adecuación de dicho sistema a la Ley Orgánica 5/1992.

De la información requerida a la Dirección General de la Policía y de las comprobaciones efectuadas en la inspección realizada en los locales de la empresa que prestaba el servicio, se desprende:

El proyecto se puso en marcha el día 18 de mayo de forma experimental en siete Comisarías de Distrito de Madrid: Chamberí, Villa de Vallecas, Usera, Puente de Vallecas, Centro, Arganzuela y Carabanchel. La empresa contratada para la prestación del servicio debía aportar los operadores de telefonía y la infraestructura necesaria para la recepción de las llamadas; la duración del contrato de prestación del servicio era de seis meses.

El proyecto fue informado favorablemente por la Secretaría General Técnica del Ministerio del Interior, por la Comisión Nacional de Coordinación de la Policía Judicial y por el Decanato de los Juzgados de Madrid.

Las hechos que podían denunciarse a través de este sistema eran las siguientes:

* Sustracción y recuperación de vehículos.
* Sustracción de efectos de interior de vehículos.
* Daños en vehículos.
* Robo y hurto de todo tipo de documentos y efectos personales.
* Pérdida y recuperación de todo tipo de documentos.

La operativa del servicio era la siguiente:

El ciudadano se ponía en contacto telefónico con el Centro de Recepción de llamadas, donde aportaba sus datos de identidad y las circunstancias del hecho denunciado. Estos datos eran recogidos por un operador bajo la supervisión y control de un funcionario del Cuerpo Nacional de Policía. Los datos grabados en un servidor local eran transmitidos aproximadamente cada 30 minutos al servidor central de la Dirección General de la Policía.

Para que la denuncia fuera válida, el ciudadano debía personarse en la Comisaría elegida antes de 48 horas, al objeto de verificar y firmar la denuncia que se confeccionó por teléfono. En las comisarías se podía editar e imprimir la denuncia. El ciudadano en la comisaría comprobaba los datos de la denuncia y efectuaba las modificaciones que considerara oportunas, firmando su denuncia en presencia de un funcionario policial, quien la suscribía y le entregaba una copia de la misma como justificante. Transcurridas 72 horas desde la grabación de la denuncia sin que el ciudadano se personara en comisaría, los hechos denunciados se ponían en conocimiento de las autoridades judiciales.

En el pliego de cláusulas administrativas suscrito, figuraba que, tanto la empresa adjudicataria como el personal incorporado al proyecto, asumían expresamente el guardar una estricta confidencialidad respecto de los datos tratados, formalizándose declaración jurada al respecto. También se incluyó una cláusula adicional de confidencialidad de los datos, por la que se obligaba al adjudicatario a respetar, en lo relativo al tratamiento de lo datos obtenidos, lo establecido en la Ley Orgánica 5/1992.

El nivel de seguridad de los equipos informáticos ubicados en los locales desde donde se prestaba el servicio y en los que se encontraba la aplicación de gestión del sistema de atención telefónica, era, en general, adecuada, aunque se detectaron algunos aspectos de la misma que podían mejorarse y que debían ser tenidos en cuenta en futuras implantaciones del sistema.

Por tanto, de las investigaciones realizadas, no se desprendió la existencia de ninguna infracción a la Ley.

4.2.3. ADMINISTRACIÓN AUTONÓMICA

Por parte de la Inspección de Datos se ha procedido a la apertura de cuatro expedientes de investigación con relación al posible incumplimiento de lo establecido en la Ley Orgánica 5/1992 por parte de responsables de ficheros pertenecientes al ámbito de las Comunidades Autónomas. Los citados expedientes se iniciaron a instancia de las reclamacio-

nes formuladas por ciudadanos y en un caso de oficio y se pueden resumir de la siguiente forma:

Recepción por parte de personas mayores de 65 años en su domicilio particular de una invitación para asistir a la "Gran fiesta de la tercera edad" remitido por la Consejería de Bienestar Social de la Generalitat Valenciana. Como consecuencia de ello, se iniciaron por la Inspección las correspondientes actuaciones tendentes a determinar si ha existido algún tipo de infracción.

Contratación a una empresa externa, por parte de la Generalitat de Cataluña, de todas las actividades relacionadas con el tratamiento automatizado de datos de carácter personal. Los citados hechos se encuentran en proceso de investigación previa.

El Servicio Canario de Salud no ha procedido a notificar la declaración de inscripción en el Registro General de Protección de Datos de los ficheros automatizados que incluyen datos relativos a la salud a pesar de los reiterados requerimientos efectuados por el citado Registro. Como consecuencia de ello se da traslado a la Inspección de este hecho, quien, asimismo, les ha requerido sin haber obtenido respuesta al finalizar este año.

Se ha recibido en la Agencia escritos de la Federación de Servicios Públicos FSP-UGT y de la Unión de Consumidores de Alicante en los que comunican la contratación por parte de la Generalitat Valenciana de la prestación de servicios para la introducción e informatización de datos referentes a la tramitación de expedientes de viviendas de protección oficial. Dado que en la tramitación de los expedientes relacionados con dicha actividad la empresa adjudicataria tendrá acceso a información confidencial de los solicitantes, incluyendo domicilios particulares, ingresos y retribuciones, patrimonio, declaraciones de la renta, cuentas corrientes, etc. los denunciantes consideran que se podría estar vulnerando lo que establece la Ley Orgánica 5/1992, por lo que se han abierto las correspondientes actuaciones de investigación.

4.2.4. ADMINISTRACIÓN LOCAL

El número de expedientes que se iniciaron para investigar posibles infracciones a la Ley Orgánica 5/1992 relacionadas con ficheros gestionados por la Administración Local fue de catorce, abiertos todos ellos a raíz de denuncias presentadas en la Agencia. La gran mayoría de estas denuncias se referían a la existencia de una posible cesión de los datos que mantienen las Entidades Locales a entidades privadas o particulares sin el consentimiento de los afectados; dos de los expedientes iniciados estaban relacionados con la no inscripción de los ficheros en el Registro General de Protección de Datos de la Agencia.

De entre los expedientes de investigación tramitados cabe destacar el iniciado contra el Ayuntamiento de Palma de Mallorca por haber suscrito un contrato con dos entidades bancarias y la Agrupación Empresarial de Agencias de Viajes de Baleares, con objeto de efectuar la solicitud y expedición de los certificados de residencia de ciudadanos empadronados en la citada ciudad a través de la red de cajeros automáticos y de las agencias de viajes. De la documentación examinada parece desprenderse que para efectuar la solicitud y emisión de un certificado a través de un cajero automático de una de las entidades bancarias, era necesario disponer de una tarjeta operativa y válida en la red de cajeros de esa entidad y bastaba teclear un número de DNI o un número de Tarjeta de Residencia de cualquier ciudadano empadronado en la ciudad para obtener dicho certificado, pudiendo incluso obtenerse no sólo el certificado del titular de ese número de DNI, sino los de todas las personas que figuraran empadronadas en el mismo domicilio. Al finalizar el año, queda pendiente de constatar los hechos por parte de la Inspección.

4.2.5. SANIDAD

En el año 1998 se tramitaron 11 expedientes relacionados con datos de salud. Entre los más relevantes podemos destacar los siguientes:

Facilitar datos de pacientes tratados en una consulta de salud mental, lo que implicaba el conocimiento del hecho de que el afectado estaba siendo tratado clínicamente por dicha patología. En este caso, por tratarse de un fichero público de la Administración Autonómica, se dio traslado del expediente a la Agencia de Protección de Datos de la Comunidad de Madrid.

Acceso en fines de semana a los datos clínicos de pacientes de determinados Centros de Salud de Atención Primaria por parte del personal de la empresa de seguridad contratada.

En este expediente se determinó que se trataba de extraer las historias clínicas de pacientes que acudían a Urgencias en fines de semana. Sin embargo, se constató que únicamente el personal médico o de enfermería tenía acceso a dichos datos.

Asimismo, aunque esporádicamente pudiera tener acceso el personal de seguridad los fines de semana y para colaborar en la atención médica de urgencias, el personal de empresas de seguridad está sujeto a confidencialidad respecto a los datos con los que trata en virtud de la Ley 23/1992 sobre seguridad privada.

Otro de los expedientes tratados se refiere a los ficheros creados para controlar la expansión de la enfermedad del SIDA.

Con la finalidad de analizar la incidencia del SIDA en la población española, la mortalidad, las características epidemiológicas de los afectados, la distribución geográfica, las patologías asociadas, etc., en 1983 se creó el fichero *Registro Nacional de SIDA,* inscrito en el Registro General de Protección de Datos con el código 1942346891.

Dicho fichero contiene únicamente lo que se denomina "casos SIDA", es decir datos relativos a afectados que ya han desarrollado la enfermedad, no recogiendo datos de infectados por VIH.

Las personas incluidas en este fichero están identificadas por nombre, apellidos y fecha de nacimiento, que se utilizan como identificadores para evitar duplicados y para poder incorporar información de interés epidemiológico que se genere "a posteriori", especialmente los datos del fallecimiento. La detección de duplicados es frecuente ya que un mismo enfermo puede ser notificado desde diferentes hospitales e incluso desde diferentes provincias. Además se recogen datos sociales y de riesgo y clínicos, que se utilizan para estudios epidemiológicos. La fecha de nacimiento se desconoce en un gran porcentaje de los casos.

Como subproductos de este fichero se obtienen diversos informes estadísticos con datos anónimos, un fichero con datos disociados para remitir al Centro Europeo de la O.M.S. en París y un fichero que se remite semestralmente al INE con datos estadísticos.

Los médicos notificadores son una parte activa del sistema de información y el único punto de contacto directo del sistema con los afectados. El médico que trata al enfermo es el que tiene la obligación de declarar el caso al Registro de SIDA de la Comunidad Autónoma (tal como establece el RD 2210/1995 de 28 de diciembre, de Creación de la Red

Nacional de Vigilancia Epidemiológica).
Las peticiones de acceso a la información de este fichero, son estudiadas por la Secretaría del Plan Nacional sobre SIDA, que autoriza o no la cesión de la información solicitada en función de la legislación vigente.
La única transferencia internacional que se realiza es al Centro Europeo de la O.M.S. ubicado en París, donde se centraliza en Europa toda la información relativa al SIDA. Se remiten datos anónimos en una estructura de registro normalizada por dicho organismo.
Por otra parte, el Centro Nacional de Epidemiología remite a cada Comunidad Autónoma únicamente sus propios casos.
Las actuaciones de este expediente continuarán a lo largo de 1999, dándose cuenta de su resultado en la próxima memoria.
Por último, se ha estudiado el proyecto del Terminal Autónomo de Identificación de Recetas (TAIR) implantado en Centros de Salud de Atención Primaria.
El objetivo fundamental del proyecto TAIR, es el de proporcionar a los médicos de Atención Primaria del INSALUD un dispositivo de lectura, registro e impresión de los datos contenidos en la Tarjeta Sanitaria Individual con el fin de:
* Asegurar la correcta identificación de los pacientes.
* Mejorar los Sistemas de Información para la gestión de los servicios sanitarios.
* Ayudar al médico a cumplimentar los documentos derivados de la asistencia sanitaria mediante la emisión de etiquetas (interconsultas, historia clínica, pruebas de laboratorio, recetas, incapacidad laboral, etc.)
* Colaborar en el control y lucha contra el fraude en la prestación farmacéutica, a través del conocimiento de los perfiles de prescripción de cada paciente y de la correcta identificación de los diferentes tipos de usuarios.
* Seguimiento de las recetas.

El TAIR es un dispositivo asociado a cada médico, que funciona de forma independiente y que permite almacenar hasta un total de 1.000 actos médicos. Se han distribuido dispositivos a los médicos ubicados en aquellos centros y servicios relacionados con la Atención Primaria, donde es necesaria la emisión de etiquetas.
Por cada acto médico derivado de la atención al paciente, el médico, mediante el TAIR, recoge los siguientes datos:
* Identificación del médico
* Identificación del paciente
* Datos de la actividad asistencial

A partir de estos datos se generan dos flujos distintos de información:
* Interno de INSALUD: datos recogidos con el TAIR en cuanto a Actividad Asistencial y dispensación de recetas médicas.
* Externo a INSALUD: información generada por la propia receta médica. La grabación de los datos se realiza por parte de los Colegios Farmacéuticos y revierte posteriormente en INSALUD. La grabación de recetas realizadas por terceras entidades, está sujeta a un Concierto suscrito entre las partes participantes del proyecto, no registrándose ni el nombre ni los apellidos de los pacientes.
El fichero final resultante de todo el proceso, que se ubicará en los Servicios centrales de INSALUD, se encuentra en fase de definición por lo que no ha sido posible terminar el estudio, que continuará en 1999.

4.2.6. PARTIDOS POLÍTICOS
Durante el año 1998 se han abierto tres expedientes de investigación referidos a partidos políticos, todos ellos a consecuencia de diversos escritos de denuncia recibidos en la Agencia. Estos expedientes se referían, fundamentalmente, a la presunta utilización indebida de los datos de afiliados o ex afiliados
De estos expedientes se obtuvieron las siguientes conclusiones :
En uno de los expedientes, en el escrito de reclamación se ponía de manifiesto la posible utilización de los datos personales de un conjunto de afiliados de un determinado partido político desde algunas empresas de carácter privado, solicitando telefónicamente su intención directa de voto de cara a un proceso de votaciones interno. Además, se manifestaba que en dichas entrevistas telefónicas se solicitaba el voto para un candidato determinado.
De las actuaciones practicadas no se ha podido constatar la utilización del censo de afiliados del partido con finalidades distintas a las que marcaban los estatutos del partido ni su comunicación a terceras partes.
Otro de los expedientes se refería a la utilización indebida de datos de no afiliados, que anteriormente sí lo habían sido, en base a un mailing realizado por un tercero.
Según los estatutos del partido en cuestión, las bajas deben realizarse de forma individual.
En el caso de los denunciantes, se constató que, o bien no habían manifestado su deseo de no seguir siendo afiliados al partido o bien habían solicitado la baja en fecha posterior a la celebración de la Asamblea anual correspondiente, que es cuando se facilitan datos actualizados a las distintas federaciones territoriales.
Por otra parte, el partido político denunciado contrató a una empresa para la realización de los servicios informáticos, que consistieron en la actualización y unificación de los ficheros de las distintas federaciones territoriales. Entre ambas entidades existía un contrato de servicios para el tratamiento automatizado de dichos datos que incluía la correspondiente cláusula de confidencialidad.
En el tercero de los expedientes varios miembros de una coalición interpusieron una denuncia ante la Agencia que hacía referencia a que habían recibido una carta firmada por la dirección de un partido, que ya no era miembro de la coalición, explicando la situación política existente en el momento.
Tras las oportunas investigaciones, se pudo comprobar que las etiquetas identificativas utilizadas fueron obtenidas con anterioridad al abandono de la coalición.

4.2.7. SINDICATOS.
En primer lugar, hemos de señalar que bajo este epígrafe englobamos tanto las actuaciones relativas a organizaciones sindicales como las referentes a representantes sindicales, juntas de personal o comités de empresa.
Bajo esta perspectiva, durante este año, la Inspección ha procedido a la apertura de cinco expedientes de actuaciones previas en los cuales la entidad objeto de investigación era un sindicato, siendo de especial relevancia los siguientes:

Posible cesión de datos personales de ciudadanos pertenecientes a una organización sindical a una entidad privada. Realizadas las actuaciones por parte de la Inspección, se constato que los citados hechos no llegaron a producirse por lo que se procedió al archivo de las actuaciones.

Recepción, por parte de funcionarios de un Ayuntamiento y del sector de la enseñanza, de envíos postales de propaganda electoral en sus domicilios particulares en relación con la celebración de las elecciones sindicales en la Administración Local y en el ámbito de la Enseñanza Pública de una Comunidad Autónoma. Los citados expedientes se han abierto en diciembre por lo que aún se están realizando actuaciones de investigación.

Remisión por parte de una organización sindical de un sector sanitario de una publicación periódica a los domicilios de los profesionales que se encuentran colegiados. Hechos similares a estos fueron también objeto de investigación en años anteriores. El citado expediente se ha abierto en diciembre por lo que está en fase de investigación.

4.2.8. COLEGIOS PROFESIONALES.

Del análisis de los hechos puestos en conocimiento de la Agencia por parte de los denunciantes durante 1998 podemos indicar que, en general, hacen referencia al suministro por parte de los Colegios Profesionales o de los Consejos Generales de Colegios, de la información relativa a sus miembros, nombre y dirección, a entidades privadas con objeto de la remisión de envíos promocionales o publicaciones del ámbito especifico profesional. No obstante, en algunos casos el suministro de la información se establece en acuerdos o convenios de colaboración suscritos entre las partes y por acuerdos de las Juntas de Gobierno o de las Asambleas Generales.

En 1998 se han recibido en la Agencia de Protección de Datos nueve escritos en los que se ponía de manifiesto la posible utilización irregular de los datos personales de profesionales colegiados. Las reclamaciones han sido formuladas por los propios colegiados, en tres casos han sido efectuadas por las propias organizaciones colegiales y una de ellas se realizó de forma anónima.

Debemos hacer especial mención en este apartado al gran número de profesionales que integran algunas organizaciones colegiales. Este es el caso de los profesionales de la salud y los abogados. Asimismo, debemos destacar que la Ley 2/1994, de Colegios Profesionales, establece la colegiación obligatoria para poder ejercer algunas profesiones. Este hecho, en conjunción con las tecnologías de la información y de las comunicaciones, convierte a estos colectivos en una fuente de información muy apreciada por algunos sectores.

Otro aspecto importante que debemos indicar es la publicación por parte de algunos colegios de la relación de sus miembros para su difusión de forma exclusiva entre su propio grupo profesional o, en algunos casos, para su disposición al público en general. Todo ello se podría enmarcar en lo especificado en el artículo 1 del Real Decreto 1332/1994, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que otorga la consideración de fuentes accesibles al público a los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Entrando ya en casos concretos, cabe destacar la resolución de archivo del procedimiento sancionador abierto a la Asociación Española de Fisioterapeutas por facilitar etiquetas con los nombres y domicilios de sus asociados a una de las candidaturas que se presentaba a las elecciones para la Junta de Gobierno del recién constituido Colegio Profesional de Fisioterapeutas de Madrid. En este caso no es posible entender que existiera una vulneración de la Ley ya que se trata de una utilización de datos de sus miembros dentro de las finalidades de la Asociación especificadas en sus estatutos, en relación con la Ley 10/1997, de creación del propio Colegio, por lo que los hechos analizados deben considerarse conforme a las previsiones del artículo 11 de la Ley Orgánica 5/1992.

Por otra parte, se ha procedido a la apertura de procedimiento sancionador a una entidad que había realizado envíos informativos a profesionales del sector sanitario. Estos datos procedían de la organización colegial, sin que constase ni el consentimiento de los afectados y ni la autorización del propio colegio, por lo que se procedió a incoar el correspondiente procedimiento que se encuentra pendiente de resolución.

Por lo que se refiere al resultado del procedimiento sancionador mencionado en la memoria del año anterior, abierto a una asociación por cesión de los datos de sus miembros para que fueran utilizados en el proceso de elecciones del colegio profesional correspondiente de una determinada Comunidad Autónoma, el Director de la Agencia ha dictado Resolución de Archivo del Procedimiento Sancionador, al entender que la cesión debe reputarse conforme al artículo 11 de la Ley Orgánica 5/1992 en relación con lo establecido en la Ley autonómica por la que se crea el antedicho colegio profesional y los estatutos de la asociación. Dicha Ley encomendaba a la asociación antes mencionada, tanto la aprobación de los estatutos provisionales que regularan la condición de colegiado como el procedimiento de convocatoria y desarrollo de la Asamblea Constituyente del colegio, dimanando la Comisión Gestora de creación del colegio de la propia asociación.

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

La Agencia ha desarrollado una activa labor en relación con los ficheros de prestación de servicios sobre solvencia patrimonial y crédito, potenciada en cierta medida por la preocupación que genera el posible uso indebido de los datos de carácter personal que se tratan en estos ficheros. Las actuaciones desarrolladas por la Agencia en el ámbito de los ficheros de esta naturaleza han seguido dos líneas claramente diferenciadas.

La primera línea de actuación, mantenida desde la creación de la Agencia, consiste en la lógica obligación de atender todas las reclamaciones y denuncias presentadas por los ciudadanos. La segunda línea, realizada por primera vez durante este ejercicio, ha supuesto el desarrollo de un plan de inspección de oficio con el objetivo de alcanzar una visión global de la situación en la que se encuentran las principales empresas del sector; así como un conocimiento detallado de la operativa de los ficheros más significativos y, en la medida de lo posible, los planes de futuro previstos.

A lo largo de este epígrafe, además de ofrecer los resultados de ambas líneas de actuación, presentaremos los datos de las auditorías de seguridad exigidas por la instrucción 1/1995 de la Agencia y concluiremos haciendo mención a las resoluciones que, versando sobre los ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, se han considerado de especial relevancia.

4.2.9.1. Actuaciones motivadas por reclamaciones y denuncias de los ciudadanos

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 1998, 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, aunque, como ya señalamos antes, se ha producido un descenso de las denuncias recibidas.
El tiempo y los recursos empleados en actuaciones sobre ficheros de esta naturaleza suponen la mayor parte sobre el total de las actuaciones practicadas por la Subdirección de Inspección de la Agencia; destacando el hecho de que la gran mayoría de las reclamaciones y denuncias recibidas, casi el 95%, hacían referencia únicamente a los cuatro ficheros más significativos del sector.
En 148 de los expedientes de investigación y de tutelas de derechos iniciados en 1998 estaban implicados ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito. De entre las tutelas de derechos, 63 de los 154 pertenecían a este sector y de los 94 procedimientos sancionadores, correspondían 46.
Sin embargo, observando las cifras con mayor detenimiento, sí que es posible establecer diferencias sustanciales en la conducta de actuación. A diferencia de lo acontecido en 1997, durante 1998 la Agencia ha impulsado proporcionalmente la tramitación de un mayor número de procedimientos de tutelas de derechos que de expedientes de investigación, confirmando la creciente preocupación de la Agencia por satisfacer los derechos individuales de los afectados. Mientras que en 1997 la relación entre tutelas de derechos y expedientes de investigación iniciados fue de uno a tres, el presente ejercicio la relación ha sido de uno a dos. Es decir, en las actuaciones desarrolladas por la Agencia ha primado la satisfacción de los derechos de los afectados frente al ejercicio de la potestad sancionadora. Todo ello, sin perjuicio de que se abrieran los correspondientes procedimientos sancionadores si, tras la tramitación de los procedimientos de Tutela de Derechos, se apreciaba la existencia de infracciones a lo que la Ley establece.
El número de actas de inspección levantadas por los inspectores de la Agencia durante 1998 ascendió a 182, de las cuales 105 correspondieron a actuaciones practicadas sobre ficheros de prestación de servicios sobre solvencia patrimonial y crédito, destacando que en 97 de estas actas estaban involucrados los 4 ficheros referidos con anterioridad.
Las cifras de procedimientos tramitados e inspecciones realizadas presentadas confirman la experiencia de años anteriores y permite concluir, sin lugar a dudas, que la información tratada en los ficheros a los que se refiere artículo 28 de la Ley Orgánica 5/1992, es la que continúa despertando una mayor inquietud entre los ciudadanos.

4.2.9.2. Plan de inspección de oficio sobre ficheros de prestación de servicios sobre solvencia patrimonial y crédito

La importancia para los ciudadanos de los ficheros de esta naturaleza constatada en las cifras expuestas, la repercusión en la actividad de la Agencia y la reconversión de procesos y servicios en la que se encontraban inmersas las principales sociedades de este sector, fueron los factores que propiciaron que el Director de la Agencia impulsara un plan de inspección de oficio sobre los ficheros de prestación de servicios de solvencia patrimonial y crédito a los que se refiere el artículo 28 de la LORTAD.
El plan pretendía que, mediante las actuaciones pertinentes, la Agencia dispusiera de un conocimiento preciso y detallado de los tratamientos a los que se ven sometidos los ficheros más significativos; así como de una panorámica de la situación global del sector.
El punto de partida del proyecto fue la definición de una serie de criterios objetivos que permitiera seleccionar los ficheros que deberían ser incluidos en el plan. Los criterios más significativos de entre los utilizados fueron los siguientes:
* Investigar los dos tipos de ficheros diferentes que establece el artículo 28 de la Ley Orgánica 5/1992: ficheros de cumplimiento e incumplimiento de obligaciones dinerarias, cuyos datos son facilitados por una entidad informante, persona física o jurídica acreedora o quien actúe por su cuenta o interés; y ficheros de solvencia patrimonial y crédito que tratan otro tipo de datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento.
* El volumen de denuncias recibidas ante la Agencia.
* La cantidad y calidad de la información registrada en el fichero.
* Las posibles repercusiones para los afectados.

Una vez seleccionados los ficheros que debían ser investigados, se elaboró un plan de inspección que permitiera determinar el grado de adecuación de la operativa de estos ficheros a la Ley Orgánica 5/1992, teniendo en cuenta los requisitos fijados en el artículo 28, en relación con el resto de requerimientos de la normativa vigente en materia de protección de datos.
Como resultado del desarrollo de las inspecciones previstas, se ha constatado que, si bien se producido una continuada mejoría en su operativa, confirmada año tras año, todavía se han encontrado actuaciones que podrían mejorarse para un más adecuado cumplimiento de la Ley.
A continuación, se comentan sucintamente las conclusiones obtenidas como resultado del plan que han resultado más significativas:

4.2.9.2.1. Calidad de datos

* Los ficheros existentes únicamente facilitan información relativa a incumplimientos de obligaciones dinerarias y reclamaciones de cantidad. No obstante, para el presente año se prevé la creación de varios ficheros que faciliten datos sobre el cumplimiento de las obligaciones dinerarias. Uno por parte de una sociedad que ya se encuentra operativa en el mercado español y dos más con motivo de la creación de dos sociedades vinculadas con multinacionales del sector.
* Prácticamente la totalidad de los datos registrados sobre el impago son objetivos: importe, fecha de impago, procedencia del dato, etc., es decir, no se incorporan valoraciones sobre los afectados. Sin embargo, hay ficheros en los que en el importe de las anotaciones registradas resulta imposible discernir la parte correspondiente al principal de la deuda de la correspondiente a los intereses.
* Las entidades que facilitan información a ficheros comunes de incumplimiento de obligaciones dinerarias han incrementado sus controles antes de enviar los datos de los impagos. En algún caso, incluso se ha ampliado el tiempo mínimo desde que se produce el incumplimiento hasta que se facilitan los datos al fichero común.
* Uno de los problemas principales consiste en mantener la información puesta al día. Se ha constatado que los proce-

dimientos para atender el ejercicio de los derechos de rectificación y cancelación empleados en algunos ficheros pueden dar lugar al incumplimiento de plazos previsto en la normativa. Asimismo, se ha detectado que siguen planteándose problemas tanto respecto del cumplimiento de los plazos previstos en la normativa respecto de las rectificaciones y cancelaciones de oficio como en el caso de ficheros obtenidos de fuentes accesibles al público, respecto de su actualización, dada la dificultad de obtener información sobre incidencias que se producen con posterioridad a la publicación de los datos que produjeron la anotación.

* Otro problema es la imputación de varias deudas a un afectado de forma incorrecta, debido al enriquecimiento de la información utilizando diversas fuentes, que, al menos, debería ser posible distinguir. También se ha constatado que se reflejan datos erróneos, puesto que en lugar del importe de la deuda reclamada, se registra, por ejemplo, el tipo de subasta.

4.2.9.2.2. Derechos de acceso, rectificación y cancelación

* Los procedimientos habilitados por los responsables de ficheros garantizan el cumplimiento de los plazos previstos en la normativa vigente tanto para los derechos de acceso, rectificación y cancelación como para la cancelación cautelar dispuesta por la Instrucción 1/1995 de la Agencia. Es más, el tiempo medio de contestación a un ejercicio del derecho de acceso se encuentra muy por debajo del mes previsto en la normativa y no se ponen impedimentos, por lo general, para atender el derecho de acceso de los afectados aunque se ejercite en intervalos inferiores a 12 meses.

* La información facilitada al afectado como resultado del ejercicio de su derecho de acceso varía en función del fichero en cuestión. En algunos ficheros no es posible informar al afectado de las consultas que sobre sus datos se han realizado durante los últimos 6 meses. Las contestaciones a los afectados suelen remitirse por correo ordinario.

* Algunas entidades que disponen de acceso a ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, no cumplen la obligación establecida en la Instrucción 1/1998 de la Agencia de atender los derechos que los afectados ejerciten. En ciertos casos se limitan a no contestar a la solicitud del afectado y en otros remiten al responsable del fichero.

4.2.9.2.3. Cesiones

* Un año más, la Agencia ha constatado la existencia de empresas cuya actividad se basa en disponer de los datos registrados en ficheros de esta naturaleza, especialmente alguno de incumplimiento de obligaciones dinerarias. Efectuar "mailings" a las personas incluidas en estos ficheros ofreciéndose a tramitar su baja o la utilización para la elaboración de informes comerciales son un claro ejemplo de que entidades que no aportan información al fichero común disponen de acceso al mismo.

* La cesión de datos a las entidades que han contratado el acceso a este tipo de ficheros, en algunos casos se realiza de un modo en que la entidad contratante dispone, en sus equipos informáticos, de una copia de la totalidad, o parte, del fichero de información de solvencia patrimonial. Sin embargo, en ninguna de las entidades inspeccionadas se ha constatado que esta cesión se notifique a los afectados. Es más, en la mayoría de los casos, al contestar el ejercicio del derecho de acceso realizado por los afectados no se informa de la totalidad de las entidades a las que se han facilitado datos relativos a su persona.

4.2.9.2.4. Notificación

* Los procedimientos de notificación definidos por los responsables de ficheros garantizan el envío de una carta por correo ordinario a los afectados cuyos datos son incluidos en el fichero, aunque existen casos en que la aplicación de estos procedimientos no garantiza de forma absoluta la recepción de las mismas.

4.2.9.2.5. Plazo de retención de los datos en el fichero.

* Aunque la mayoría de los responsables de ficheros agota el plazo previsto por la normativa para la permanencia de datos en el fichero, seis años en caso de datos adversos, un responsable de fichero mantiene esta información únicamente durante treinta meses.

* Los procedimientos aplicados por los responsables de ficheros evitan que el fichero trate datos de una antigüedad superior a seis años. No obstante, algunas entidades que facilitan información a ficheros comunes, no efectúan con el debido cuidado la solicitud de cancelación al responsable del fichero común de aquellos datos cuya antigüedad ha excedido los seis años, habiéndose constatado que este hecho se produce con mayor asiduidad en aquellas anotaciones en las que no es posible discernir el importe del principal de la deuda del de los intereses.

Como consecuencia de las actuaciones inspectoras, el año 1999 se tomarán, por parte de la Agencia, las medidas oportunas para corregir las deficiencias observadas y, en su caso, sancionar las que supongan una infracción de la Ley Orgánica 5/1992.

4.2.9.3. Resoluciones del Director de Agencia de Protección de Datos, de una especial relevancia

Las resoluciones del Director de la Agencia tienen una importancia capital, en cuanto que en ellas se establecen los criterios fundamentales que han de regir en las actuaciones de la Agencia. De entre todas las resoluciones dictadas durante 1998 referentes a ficheros a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, dos de ellas merecen especial atención: R/00105/1998, referente a la Central de Información de Riesgos del Banco de España, y R/00202/1998, referente a los datos de personas físicas en el ejercicio de una actividad empresarial.

4.2.9.3.1. Resolución R/00105/1998

Como resultado de la tramitación de varios expedientes iniciados por denuncias presentadas ante esta Agencia, se decidió la apertura de un procedimiento de infracción de Administraciones Públicas a Banco de España, en su calidad de responsable del fichero Central de Información de Riesgos (en adelante CIR).

La CIR contiene información sobre los riesgos financieros contraídos por personas físicas y jurídicas. Los datos son facilitados por las entidades bancarias y financieras y el Banco de España, tras consolidar la información recibida, remite a cada entidad los datos relativos a sus clientes. Durante la tramitación de los expedientes, se constató que el citado fichero trata datos relativos a deudas, transcurridos más de seis años desde la fecha en que fueron contraídas.

La Resolución del Director de la Agencia concluye que la CIR, por ser un fichero de titularidad pública, debe considerarse un fichero excluido del régimen que establece el artículo 28 de la Ley Orgánica 5/1992, por lo que no le resultan de aplicación las obligaciones dispuestas en el citado artículo, tales como la notificación de inclusión a los interesados, la comunicación de las evaluaciones de los seis últimos meses o limitar la cesión de datos de carácter personal a aquéllos que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando

sean adversos a más de seis años.
En la Resolución del citado procedimiento, se ponen de manifiesto dos aspectos que presentan un interés especial:
* Aunque el Banco de España alegó que, para la interposición de una denuncia ante la Agencia, consideraba indispensable que el denunciante hubiera ejercido previamente sus derechos de acceso, rectificación o cancelación, el Director de la Agencia entiende que: "*la posible reclamación de un afectado por la presunta desestimación de alguno de sus derechos es por el responsable del fichero automatizado (lo cual daría lugar al procedimiento de tutela de derechos) es totalmente independiente de que, al examen de la denuncia interpuesta, documentación aportada y resultado de las actuaciones de inspección al respecto, se aprecien indicios de presuntas infracciones a la Ley Orgánica 5/1992, lo cual exige la apertura del correspondiente procedimiento sancionador a los efectos de comprobar si la infracción se ha cometido, así como determinar responsabilidades* ."
* El fichero CIR es un fichero de titularidad pública, siendo una de sus funciones informar a las entidades de crédito la totalidad del riesgo contraído por sus clientes en el sistema financiero. No obstante la similitud existente entre este hecho y las funciones previstas para los ficheros a los que se refiere el artículo 28 de la Ley 5/1992, el Director de la Agencia considera que, "*el carácter objetivo que determina el régimen regulador, atendiendo sólo a la titularidad de los ficheros en cuestión, sin que ningún precepto permita la posibilidad de distinguir su carácter en atención a las funciones que efectivamente preste ni al origen de la fuente de que se nutre, no parece que pueda hacerse dicha consideración. Tratándose de un fichero de titularidad pública, debe entenderse que se encuentra excluido del régimen que se establece en el artículo 28 de la LORTAD.* "
No obstante lo anterior, con objeto de evitar cualquier duda sobre la suficiencia de la cobertura legal de la normativa vigente (Decreto-Ley 18/1962, de 7 de junio), el Director de la Agencia realizó gestiones ante el Banco de España para que se promoviera un marco legal más adecuado, obteniendo el compromiso del Gobernador del Banco de España al respecto.
4.2.9.3.2. Resolución R/00202/1998
Durante la tramitación de un expediente de investigación iniciado por una denuncia ante la Agencia, quedó acreditado que una entidad financiera había facilitado a un fichero de incumplimiento de obligaciones dinerarias datos sobre los impagos producidos en una operación de "leasing" inmobiliario suscrita por un empresario individual. Asimismo, se constató que estos datos figuraron en el fichero después de seis años desde la fecha en que los impagos se habían producido.
Como resultado del expediente de investigación se procedió a la apertura de un procedimiento sancionador que se resolvió en la R/00202/1998, en el sentido de considerar fuera del ámbito de aplicación de la Ley Orgánica 5/1992 los datos de un empresario individual por hacer referencia a su actividad como empresa y no a la intimidad del denunciante.
Durante la tramitación del procedimiento sancionador la entidad financiera alegó el hecho de que la operación había sido contratada por un empresario individual, refiriéndose el contrato suscrito al tráfico de su empresa, por lo que este supuesto debería entenderse excluido del ámbito de la Ley Orgánica 5/1992, conforme al artículo 1.
La Resolución del Director de la Agencia describía el problema planteado en el expediente de la siguiente manera: "*en el caso de la empresa-persona física se plantea el problema de que no existe la diferenciación patrimonial que existe en el caso de una sociedad, lo que dificulta enormemente la posibilidad de distinguir cuándo un dato se refiere a la empresa o a la persona que la ejercita y, si solo en este último caso cabe aplicar el manto protector de la LORTAD, la distinción debe ser esencial* ."
Considerando que a lo largo de la tramitación del procedimiento sancionador quedó acreditado que los datos del denunciante que fueron facilitados al fichero de incumplimiento de obligaciones dinerarias eran relativos a un crédito obtenido en una operación de "leasing", el Director de la Agencia, finalmente, concluye que:
"La Disposición adicional 7ª.1 de la LEY 26/1988 de 29 de julio, de Disciplina e Intervención de las entidades de crédito dispone que: Tendrán la consideración de operaciones de arrendamiento financiero aquellos contratos que tengan por objeto exclusivo la cesión del uso de bienes muebles o inmuebles, adquiridos para dicha finalidad según las especificaciones del futuro usuario, a cambio de una contraprestación consistente en el abono periódico de las cuotas a que se refiere el número 2 de esta disposición. Los bienes objeto de cesión habrán de quedar afectados por el usuario únicamente a sus explotaciones agrícolas, pesqueras, industriales, comerciales, artesanales, de servicios o profesionales. El contrato de arrendamiento financiero incluirá necesariamente una opción de compra, a su término, en favor del usuario.
No contradice esta exclusividad del contrato de "leasing" a los comerciantes la Disposición Adicional primera 5, segundo párrafo de la Ley 28/1998, de 13 de julio, BOE del 14, de Venta a Plazos de Bienes Muebles al prever los supuestos de quiebra o concurso de acreedores del arrendatario financiero, puesto que lo que se está resolviendo al contemplar ambas figuras es el problema de la inexistencia de separación de patrimonios en el caso de que la empresa se ejecute por una persona física, el empresario individual, que puede encontrarse en cualquiera de dichos supuestos según sea la causa de la insolvencia, afectando la insolvencia en ambos casos a la totalidad de su patrimonio, el afectado a la empresa y el personal.
En consecuencia, debe entenderse que la operación de "leasing" que dio lugar a los impagos que se anotaron en el fichero (...) tan sólo pudo suscribirse por parte del denunciante en la ejecución de su empresa, por lo que los datos se refieren a esta y no a la intimidad del denunciante y no es de aplicación la LORTAD ."
En conclusión, los datos relativos a la actividad empresarial de las personas físicas exceden del ámbito de aplicación de la Ley Orgánica 5/1992, pudiendo, por tanto, ser tratados de forma automatizada sin quedar al amparo del citado precepto.

4.2.9.4. Auditorías de Seguridad. Cumplimiento de la Norma Cuarta de la Instrucción 1/1995 de 1 de marzo de la Agencia de Protección de Datos.

La norma cuarta de la Instrucción 1/1995 de 1 de marzo relativa a Medidas de Seguridad de los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias establece que aquellas entidades responsables de ficheros de esta naturaleza deberán acreditar la efectiva implantación de las medidas de seguridad exigidas en el artículo 9.1 de la Ley Orgánica 5/1992 de 29 de Octubre mediante la realización de una auditoria, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y remitir a la Agencia de Protección de Datos el informe final de la misma.

Asimismo, se establece en el apartado 6 de la citada norma cuarta que los sistemas obligados por esta norma deberán ser auditados periódicamente a intervalos no mayores de dos años, a partir de la entrada en vigor de la citada instrucción. En cumplimiento de esta norma, a lo largo del año 1998 se han recibido numerosos informes de auditoría remitidos por entidades, que en la mayoría de los casos, ya habían auditado sus sistemas durante los años 1995 y 1996, correspondiéndoles según el período establecido en la norma cuarta una nueva revisión de sus sistemas.

La Agencia de Protección de Datos, una vez recibidos estos informes, ha procedido a su estudio y revisión detallados, con el objeto de extraer conclusiones, tanto a nivel específico respecto de una determinada entidad, como a nivel general respecto de las medidas de seguridad adoptadas en el tratamiento y almacenamiento de este tipo de información, que tiene un especial impacto social, pues afecta a una gran cantidad de actividades cotidianas de los ciudadanos donde se establecen relaciones mercantiles o económicas, acceso a servicios o productos financieros, etc. Es por esto que los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias son motivo de una especial atención en la Instrucción 1/95, que dedica la norma cuarta a establecer garantías específicas que vienen a concretar lo establecido en artículo 9.1 de la Ley Orgánica con carácter general para los ficheros automatizados con datos de carácter personal.

4.2.9.4.1. Características generales

Como datos generales, el número total de informes de auditoría recibidos en la Agencia asciende a un total de 62, que corresponden a la revisión de los sistemas de información de 98 entidades. La diferencia entre el número de informes y el mayor número de entidades revisadas responde en general al hecho de que algunas entidades que pertenecen a un mismo grupo empresarial y comparten, bien totalmente, bien de forma parcial, los recursos de información y los sistemas de tratamiento y gestión de dicha información.

En cuanto a la distribución geográfica de las entidades, podemos destacar que la mayor parte de las sociedades están radicadas en Madrid y Barcelona, siendo la distribución correspondiente al resto de provincias de una a dos sociedades como media, según se muestra en el cuadro número 1.

Provincia donde está radicada la sociedad	Número de entidades por provincia
A CORUÑA	1
ÁLAVA	1
BARCELONA	21
CÁCERES	1
CANTABRIA	1
CASTELLÓN	2
CÓRDOBA	1
GIRONA	1
GUIPÚZCOA	1
ILLES BALEARS	2
LA RIOJA	1
LAS PALMAS	1
LEÓN	1
MADRID	48
MÁLAGA	1
MURCIA	1
NAVARRA	1
PONTEVEDRA	1
SALAMANCA	1
SEVILLA	2
STA. C. DE TENERIFE	1
TOLEDO	1
VALENCIA	2
VIZCAYA	2
ZARAGOZA	2

Cuadro 1. Distribución de entidades auditadas por provincia donde está radicada la sociedad

En cuanto al sector de actividad, hay que destacar el hecho de que mayoritariamente las entidades auditadas pertenecen al sector bancario y financiero (cajas de ahorro, bancos privados, sociedades de financiación), mientras que el resto se incluyen en el sector de información sobre la solvencia patrimonial y el crédito, tal como se ve en el cuadro número 2.

Sector de Actividad	Nº Entidades/Sector
BANCA PRIVADA	63
CAJAS DE AHORRO	18
SOCIEDADES DE FINANCIACIÓN	12
SERV. INFORMACIÓN SOBRE SOLVENCIA PATROMONIAL	5

Cuadro 2. Distribución de entidades auditadas por sector de actividad

En cuanto a las características generales de los informes de auditoría remitidos, se puede destacar en primer lugar, la naturaleza de los auditores en cuanto a su vinculación con la entidad auditada. En este sentido la norma cuarta de la instrucción establece en su apartado 3 la posibilidad de que la auditoria sea realizada bien por el departamento de auditoría interna de la entidad responsable del fichero, si aquél está formalmente constituido, profesionalmente cualificado y es independiente del órgano responsable del tratamiento y gestión de los datos, o bien por un auditor externo profesionalmente cualificado e independiente del responsable del fichero. Como se puede apreciar en el cuadro número 3, la gran mayoría de las auditorías practicadas ha sido realizada por personal interno de la entidad responsable del fichero, perteneciente al departamento de auditoría. Si ponemos en relación estas cifras con las correspondientes al sector de actividad de las entidades auditadas, es posible encontrar cierta correlación, ya que en el sector bancario y financiero, es habitual la existencia dentro de la organización de un departamento de auditoría y/o control, y dada la amplia implantación de sistemas informáticos en este tipo de actividad, dentro del departamento de auditoría también empieza a ser habitual encontrar un área o grupo especializado en auditoría informática, como se refleja también en el cuadro número 3.

Tipo de Auditor	Nº Entidades Auditadas
INTERNO (Dpto. Auditoría Interna)	41
INTERNO (Dpto. Auditoría Interna con área o grupo de auditoría informática)	12
EXTERNO	9

Cuadro 3. Distribución de auditorías ejecutadas en función del tipo de auditor

En lo que respecta a los ficheros auditados, el aspecto más destacable es que la mayoría de los informes se refieren por una parte, a los ficheros internos de la entidad responsable que almacenan información relativa a sus propios clientes, y por otra a ficheros con información sobre cumplimiento o incumplimiento de obligaciones dinerarias denominados comunes, es decir aquéllos que consolidan información procedente de los ficheros internos de las entidades y cuya finalidad, más que la de la obtención de la satisfacción de las obligaciones dinerarias, está orientada a proporcionar información sobre la solvencia económica de una determinada persona. En este último caso, cabe destacar el hecho, por otra parte lógico, dado que se trata de entidades dedicadas al mismo tipo de actividad, de que coincidan los mismos ficheros en la mayoría de las entidades.

4.2.9.4.2. Contenido y conclusiones de los informes de auditoría

En relación al contenido de las auditorías, en lo que sigue se comentarán tres aspectos de las mismas: procedimientos y/o metodologías estándar empleados en la práctica de auditoría, tipo de controles revisados en relación con las medidas de seguridad implantadas y medidas correctoras o complementarias dictaminadas por los equipos auditores.

En el primer aspecto, es necesario señalar que, en términos generales, no se han aplicado procedimientos o técnicas avaladas por metodologías generalmente aceptadas entre los profesionales de la auditoría, hecho éste que conduce a una amplia diversidad de estilos en lo que respecta a las normas aplicables en la ejecución de la auditoría y a una falta de homogeneidad en los informes resultantes. Quizá esta conclusión está de acuerdo con el panorama que, a nivel general, existe en el campo de la auditoría informática, la cual, por ser un una disciplina emergente, adolece de prácticas más homogéneas presentes por ejemplo, en la auditoría de tipo contable o financiera.

En el segundo aspecto, relativo al tipo de controles de seguridad revisados, se puede concluir, a modo de resumen global, que estos controles en la práctica totalidad de las auditorías ejecutadas se refieren a tres grupos de medidas:

Seguridad organizativa: En este apartado se presta especial atención a los controles de seguridad establecidos orientados a garantizar la integridad y confidencialidad de la información que es tratada por el personal a cargo de la operativa del tratamiento y explotación del fichero, ya sea éste de perfil informático (desarrollo y mantenimiento) o de gestión (explotación). Los aspectos más relevantes revisados por los auditores en este apartado se refieren a la existencia de

políticas o procedimientos de seguridad formalmente establecidos, sistemas de control, seguimiento y auditoría internos y segregación de funciones entre el personal, en particular en lo que se refiere a administración de seguridad.

Seguridad física: Este apartado se refiere básicamente a las instalaciones donde se ubican los sistemas informáticos donde se realizan los tratamientos de la información y al equipamiento existente en dichas instalaciones. Los aspectos más relevantes revisados por los auditores se refieren a ubicación de las instalaciones, medidas y controles de acceso a las mismas, medidas y controles físicos de seguridad contra contingencias accidentales y no accidentales como incendios, inundaciones, robos, etc., medidas de seguridad específicas relativas al mantenimiento de la integridad física de los soportes donde se almacena la información, medidas de seguridad relativas al almacenamiento, transporte y acceso a los soportes, y existencia de un plan de contingencias específicamente diseñado en función de las características de las instalaciones y de los sistemas y equipos de tratamiento ubicados en las anteriores.

Seguridad lógica: Las medidas y controles de seguridad lógica se refieren fundamentalmente a las técnicas de control de identificación de los usuarios que acceden a los sistemas de información, a técnicas que permitan asociar diferentes tipos de disponibilidad de la información a cada usuario (sin acceso, acceso sin autorización para efectuar modificaciones, acceso con autorización para efectuar modificaciones, etc.) y técnicas que permitan asegurar la confidencialidad de la información manejada por los usuarios. En este apartado los aspectos revisados por los auditores se pueden resumir en: existencia de mecanismos de control y autenticación de acceso de usuarios (identificador de usuario y contraseña, etc.), existencia de mecanismos que permitan elaborar la contabilidad de usuarios (usuarios que han accedido, recursos que han utilizado, qué actividades han realizado, etc.), existencia de mecanismos que permitan detectar fallos en la seguridad de acceso (alarmas de intrusiones, intentos de violación de derechos de acceso), control de la disponibilidad de la información y existencia de mecanismos que permitan asegurar la confidencialidad de la información (técnicas de cifrado, técnicas de desconexión automática, etc.)

Finalmente, el tercer aspecto a comentar se refiere al tipo de medidas correctoras que los auditores han recomendado en sus informes. Entre aquellas, se pueden destacar:

Aunque en la mayor parte de los casos existe una política de seguridad formalmente establecida, se aprecia la necesidad de elaborar procedimientos que permitan actualizar esta política cuando se producen cambios tecnológicos u organizativos que así lo requieran, así como la carencia, en algunos casos de objetivos de control concretos.

Necesidad de elaborar y ejecutar planes de formación a los usuarios en relación con la adopción de prácticas de seguridad con carácter habitual, como por ejemplo en lo relativo a la elección y cambio periódico de contraseñas, etc.

Necesidad de establecer políticas organizativas orientadas a la disgregación de funciones, en especial en lo relativo a la administración de la seguridad.

Necesidad de implantar software de seguridad especializado que refuerce las medidas y controles que proporcionan los sistemas operativos o las aplicaciones de tratamiento de la información, y que en algunos casos, proporcione la capacidad de establecer medidas de control de intrusión y de auditoría y contabilidad de usuarios.

Necesidad de elaboración e implantación de un Plan de Contingencias o de Recuperación frente a desastres en unos casos, y en otros necesidad de actualización con periodicidad razonable del Plan de Contingencias existente.

Necesidad de actualizar o sustituir determinados mecanismos de seguridad física, por obsolescencia del sistema o bien por obligación legal, (por ejemplo, la sustitución de los sistemas de extinción de incendios basados en disparo automático de gas halón, la actualización de sistemas de alimentación ininterrumpida, actualización de sistemas de detección de incendios, etc.).

Necesidad de establecer ubicaciones alternativas a las copias de seguridad en lugares externos a las propias instalaciones de los centros de proceso, y suficientemente alejados de éstas como para no ser afectados por contingencias que pudieran ocurrir en los centros de tratamiento.

Necesidad de establecer cláusulas referentes a medidas y controles de seguridad en los contratos con terceras entidades que suministran determinados servicios, como el transporte de soportes de unos centros de tratamiento a otros, operadores de servicios de telecomunicaciones para el transporte de datos o entidades que prestan servicios de acceso telemático a ficheros de información sobre la solvencia patrimonial y el crédito o de cumplimiento o incumplimiento de obligaciones dinerarias.

Necesidad de reforzar las medidas y controles de seguridad lógica en todo el ciclo de vida de la información: recepción, tratamiento y acceso, almacenamiento, transporte o transmisión, transcripción al papel, etc. con objeto de preservar la integridad de la información como la confidencialidad y disponibilidad (por ejemplo, establecimiento de técnicas de cifrado en el almacenamiento y transmisión).

4.2.10. PUBLICIDAD DIRECTA

La publicidad directa ha sido una de las actividades que más denuncias ha generado. En la mayor parte de los casos sigue denunciándose la obtención de datos no ajustada a lo que establece el artículo 29 de la Ley ("*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")* .

Durante este año se han iniciado en la Agencia un total de 100 expedientes, tanto de investigación como de tutela de los derechos, relacionados con el envío postal de publicidad, lo que supone un decremento de aproximadamente el 21% con respecto a los iniciados en el año anterior.

Considerando el número de Procedimientos Sancionadores que han finalizado en 1998 con una resolución sancionadora, se observa que en torno al 20% de ellos versaban sobre actividades relacionadas con el envío postal de publicidad, siendo reseñable que de las 4 resoluciones con que se sancionaba una falta muy grave, la mitad de ellas se refieren a hechos relacionados con este tipo de actividad.

De éstas últimas, cabe destacar la sanción impuesta a una entidad cuya actividad se centra en la distribución de productos a través del procedimiento de "*televenta*", habiendo quedado probado durante el Procedimiento Sancionador que incumplió el mandato contenido en el artículo 11 de la Ley, al haber cedido los datos de al menos uno de sus clientes a otra entidad (que los utilizó para el envío postal de publicidad) sin contar con el consentimiento previo de aquél.

La otra resolución que sancionaba la comisión de una falta muy grave fue la recaída en una entidad dedicada a labores relacionadas con el marketing directo, que había utilizado datos del Censo Electoral para el envío postal de publicidad de una editorial y que además había cedido posteriormente datos procedentes de la misma fuente a una tercera entidad perteneciente a su mismo sector de actividad.
Respecto de las sanciones impuestas por falta grave, la mayor parte se refieren a infracciones tipificadas en el artículo 43.3.d) y consistentes en el tratamiento automatizado de datos personales de los que no se acreditó su procedencia o bien ésta resultó ser ilegítima. Cabe destacar que 9 de las 14 sanciones recayeron sobre entidades cuya actividad principal es el marketing directo y que 3 de ellas ya habían sido sancionadas previamente por hechos similares.

4.2.11. ENCUESTAS SOBRE EL CONSUMO DEL CIUDADANO.

En la Memoria correspondiente al año 1997 ya se reseñaba el inicio de sendos Procedimientos Sancionadores a dos empresas que se habían constituido por separado para recopilar información detallada de los ciudadanos a través de las denominadas "*encuestas sobre el consumo*", con objeto de configurar sendas bases de datos que pudiesen ser empleadas posteriormente por otras entidades con finalidades de marketing directo. En 1998 estos Procedimientos fueron sobreseídos al entenderse que ninguna de las iniciativas vulneraba lo establecido en la Ley Orgánica 5/1992. En este sentido, resulta útil conocer lo que se valoraba en las correspondientes Resoluciones:
* En el folleto remitido por VNU MARKETING INFORMATION SERVICES, S.A. debe entenderse que no deja dudas al destinatario de que, salvo que manifieste lo contrario, sus datos personales, que cede voluntariamente, podrán ser cedidos a empresas comerciales que se dedican a la promoción de bienes y servicios por medio de ofertas dirigidas al domicilio de los posibles interesados.
En el folleto remitido por CONSODATA ESPAÑA, S.A. se advierte de que, salvo que manifieste lo contrario, sus datos personales, que cede voluntariamente, podrán ser cedidos a primeras firmas comerciales del sector del consumo con el fin de determinar qué productos merecen su confianza y son objeto de su demanda.
Según el texto de la Resolución, ambas descripciones permiten a quien lee la cláusula hacerse a la idea del uso que van a hacer de sus datos, por lo que debe entenderse que la cláusula cumple suficientemente con la condición incluida en el artículo 11.3 de la Ley Orgánica 5/1992, de 29 de octubre. Por otra parte, no puede ignorarse que el fichero resultante de la campaña resulta un activo empresarial de enorme valor y que la explotación que se pretende va a ser ejercida por la propia empresa que recaba los datos mediante la segmentación de la información y la prestación de la actividad de mailing a quienes quieran anunciarse mediante sus servicios y que, conforme al artículo 15 de la Ley Orgánica 5/1992, el interesado podrá siempre pedir la cancelación de sus datos, o determinar aquellas finalidades o usos a los que no quiere que se destinen sus datos.

4.2.12. UTILIZACIÓN DE DATOS PERSONALES DE ABONADOS A SERVICIOS DE TELECOMUNICACIÓN.

En el año 1998 finalizaron los procedimientos iniciados en 1997 referentes a Telefónica de España, S.A. como consecuencia de la utilización que la citada compañía realizaba de los datos personales de sus abonados y de las polémicas circulares que les remitió con objeto de recoger el consentimiento para poder tratar y ceder sus datos personales a terceros.

Estos hechos fueron ampliamente recogidos por diversos medios de comunicación durante la segunda mitad de 1997 y la primera mitad de 1998 y a ellos se dedicó un apartado en la memoria de la Agencia correspondiente al ejercicio de 1997. Como ya se recogió en dicha memoria, al cierre de la misma quedaban dos procedimientos sancionadores abiertos contra Telefónica de España, S.A. por los hechos señalados. Ambos procedimientos, originados por la recepción de más de 80 denuncias entre los dos, se resolvieron durante 1998 y trajeron dos consecuencias importantes.

La primera de ellas supuso la sanción a Telefónica de España, S.A. por falta de información durante la recogida de los datos. La segunda supuso el que se elevara a definitiva la medida cautelar adoptada en el Acuerdo de Apertura del procedimiento sancionador y por la cual se instó a Telefónica a que se abstuviera de realizar cualquier cesión de datos personales de sus clientes en los términos establecidos en la circular remitida a lo largo del mes de diciembre de 1997 y encabezada como *"INFORMACIÓN CONCERNIENTE A LA LEY DE PROTECCIÓN DE DATOS AUTOMATIZADOS."*, no siendo sancionada Telefónica en este caso toda vez que la medida cautelar decretada al inicio del procedimiento impidió el que se cometiera la infracción.

A modo de resumen, podemos decir que, en relación a la utilización de los datos personales de los abonados a Telefónica, el resultado final de las actuaciones de la Agencia de Protección de Datos ha sido el siguiente:

* Dos sanciones a Telefónica de España, S.A.: una por ceder datos a terceros sin disponer para ello del consentimiento de los afectados y otra por no facilitar la información que exige la Ley en el momento de la recogida de los datos. También, como ya se ha mencionado, se ha prohibido a la citada sociedad ceder datos a terceros en base a la circular remitida en diciembre de 1997 ya que la Agencia considera que no amparo legal suficiente.

* Tres sanciones a Telefónica Publicidad e Información, S.A.U. Una por tratamiento de datos sin consentimiento, otra por cesión de datos a terceros sin consentimiento y la tercera por no facilitar toda la información que exige la Ley cuando se ejerce el derecho de acceso.

Por su parte, Telefónica de España, S.A. a primeros de 1998 dirigió un escrito a todos su abonados firmado por su presidente en el que anunciaba que Telefónica de España, S.A. iba a dejar de ceder datos a terceros. Al mismo tiempo, Telefónica Publicidad e Información, S.A.U. solicitaba a la Agencia de Protección de Datos la supresión de la inscripción del fichero TELPART, fichero sobre el que se sustentaba el producto CODITEL HOGARES y a través del cual se producía la venta de los datos de los abonados al servicio telefónico.

Es de destacar en este sentido la aparición, a finales de 1998, de un nuevo marco regulador en torno a los repertorios

de abonados a los servicios de telecomunicaciones. Dicho marco contenido en el Real Decreto 1736/1998, de 31 de julio, recoge nuevas garantías para la privacidad de los ciudadanos, así como una serie de obligaciones para las sociedades operadoras que ayudarán a incrementar el nivel de protección de los datos personales en este sector.

Finalmente, la Agencia de Protección de Datos, consciente del gran volumen de datos que manejan las empresas operadoras de telecomunicaciones, decidió en 1998 la apertura de un plan de oficio con objeto de estudiar el grado de adecuación de los ficheros de estas compañías a la legislación de protección de datos. En este contexto, durante el mencionado ejercicio se han inspeccionado los ficheros de Telefónica de España, S.A., estando prevista la inspección de los ficheros del resto de las operadoras para el próximo ejercicio. En la memoria de 1999 se recogerán los resultados y conclusiones de dicho plan, si bien se puede avanzar, que la inspección realizada a Telefónica de España, S.A. que tuvo una duración de dos meses, dentro de los cuales se analizaron, *in situ*, los 10 ficheros más representativos de la entidad, entrevistándose para ello a cerca de 50 personas. En este sentido conviene destacar que Telefónica de España, S.A. dispone en sus ficheros de datos de aproximadamente unos 12 millones de personas físicas, con información lo suficientemente rica como para poder establecer perfiles de diversos tipos.

4.2.13. SEGUROS PRIVADOS

Durante este año la Inspección ha tramitado 15 expedientes de investigación relacionados con compañías aseguradoras, la mayor parte de los cuales han sido iniciados como consecuencia de la presentación de una denuncia y se refieren a la automatización ilegítima de datos por parte de estas compañías.

Por otra parte, merece destacarse la sanción impuesta a una aseguradora por automatizar, sin mediar autorización de la afectada, datos relativos a su nombre completo, domicilio, número de D.N.I., fecha de nacimiento, sexo, profesión, así como datos relativos a medidas del cuerpo, embarazos, abortos, antecedentes familiares, aptitud para el trabajo, sufrimiento de distintas afecciones médicas (respiratorias, cardíacas, digestivas, urinarias, cerebrales, cutáneas, oftalmológicas, óticas, infecciosas, óseas, sanguíneas, tumorales y cancerígenas), existencia de secuelas de accidentes, tratamiento hospitalario, consumo de estupefacientes y otras medicinas, sometimiento a pruebas de detección del SIDA, consumo de tabaco y alcohol.

Estos datos fueron obtenidos a partir de un formulario de solicitud de póliza, cumplimentado en el año 1990 por la interesada y que no ocasionó la formalización definitiva de póliza. Sin embargo, los datos fueron conservados en los ficheros automatizados de la aseguradora y utilizados en 1997 para denegar la aceptación de una nueva póliza asociada a la concesión de un préstamo hipotecario.

Con carácter general, en la Resolución se entiende que en el caso de contratos de seguro de vida perfeccionados con anterioridad a la LORTAD no será exigible el consentimiento expreso al recabar los datos y que mientras el contrato esté en vigor tampoco será exigible dicho consentimiento, puesto que estará amparado en la excepción del artículo 6.2. Sin embargo, una vez que el contrato se resuelve por cualquier causa, los datos resultarán innecesarios para el fin que justificó su mantenimiento, por lo que conforme al artículo 4.5 de la LORTAD deberían ser cancelados.

Particularmente, en este caso el contrato no había llegado a surtir efectos al resolverse por voluntad del asegurado, quien no atendió el pago de la primera prima, por lo que es obvio que la obligación de cancelar no puede exigirse que se cumpla en ese mismo momento, en que la LORTAD no existía (año 1990), pero sí desde el momento en que ésta entró en vigor, conforme establece la Disposición Transitoria Única y, en consecuencia, la aseguradora debió haber comprobado en el plazo establecido si era o no preciso el consentimiento de la afectada para poder tratar sus datos automatizadamente.

Por tanto, si bien es cierto que, antes de la perfección del contrato, el tomador del seguro debe declarar al asegurador todas las circunstancias por él conocidas que puedan influir en la valoración del riesgo, de acuerdo con el cuestionario al que éste le someta, no es menos cierto que, rellenado el cuestionario y valorados los riesgos, el asegurador podría tener derecho a mantener los datos de salud siempre y cuando se suscriba la póliza de seguro solicitada. Siendo el caso que la solicitante del seguro no cumplió el contrato de seguro al no atender el pago de las primas, lo que provocó su resolución, la aseguradora no podía presumir que tuviese el consentimiento expreso que requiere la Ley para mantener dicho tratamiento, ni existe circunstancia alguna que permita mantener el tratamiento sin concurrir dicho consentimiento expreso.

4.2.13.1. Plan de Inspección a grandes compañías aseguradoras

En 1998, por acuerdo del Director, a propuesta de la Inspección, se acometió la primera fase del análisis de adecuación a los principios de protección de datos de la actuación realizada por el sector asegurador. En este sentido, se seleccionaron cuatro grandes compañías de entre aquellas que poseen una mayor cartera de clientes, descartando en general las que ya hubiesen sido inspeccionadas en el pasado por la propia Agencia. El trabajo realizado consistió en el análisis minucioso de documentación previamente requerida a cada compañía, la realización de una inspección in situ sobre sus ficheros y la posterior evaluación de los elementos obtenidos. Como resultado se obtuvieron las siguientes conclusiones:

* Respecto del cumplimiento del principio de calidad de datos, se ha detectado que en algunos casos las aseguradoras conservan en sus ficheros automatizados los datos de los solicitantes que no han contratado finalmente una póliza, es decir, que no han establecido una relación que justifique el mantenimiento de los datos. En este sentido, también sería cuestionable la fórmula que en algunos casos se utiliza para recabar el consentimiento para la automatización, pues se hace referencia al "*asegurado*" en lugar de al "*solicitante*". En todo caso, debería indicarse explícitamente el hecho de que los datos permanecerán en los ficheros de la compañía aun en el caso de que no se formalice la póliza.
* Se ha podido comprobar que, en general, las aseguradoras no han establecido procedimientos específicos para cancelar de sus ficheros los datos de sus exclientes, una vez transcurridos los plazos legales que obligarían a mantenerlos después de finalizada la relación contractual.
* Sólo la mitad de las aseguradoras analizadas cumplen con el requisito de incluir en sus formularios la información a la que hace referencia el artículo 5 de la Ley Orgánica 5/1992, siendo discutible en los otros casos que su contenido pueda deducirse claramente de la naturaleza de los datos personales solicitados. Por otra parte, es preciso observar lo establecido por la norma 3 de la Instrucción 2/95 de la Agencia de Protección de Datos, aplicable a la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal, según la cual el artículo 5.

3 de la Ley no sería de aplicación en estos casos.
* Las fórmulas utilizadas por las aseguradoras para recabar el consentimiento son, en general, confusas. El consentimiento no se solicita para el tratamiento automatizado de los datos que se recogen (circunstancia que podría considerarse innecesaria sólo en el caso de que llegara a establecerse una vinculación negocial), sino que se aplica a otras circunstancias diversas: cesión a otras entidades, conservación con fines estadístico-actuariales u oferta promocional.
* En algunos casos se sigue recabando el consentimiento para ceder datos a la entidad VIDACUMUL (agrupación de interés económico que en su día agrupaba a una gran cantidad de compañías aseguradoras), aun cuando esta entidad ha cesado ya su actividad como responsable de un fichero común para la prevención del fraude.
* A pesar de que tan sólo una de las compañías inspeccionadas ha reconocido que automatiza los datos de salud de sus asegurados, se ha detectado que no en todos sus formularios recaba el consentimiento expreso para ello. Observado este hecho, se hace imprescindible exigir una mayor escrupulosidad por parte de las compañías a la hora de elaborar sus formularios.
* También se hace necesario decidir si la práctica de asignar un código a un asegurado en función del tipo de sobreprima que se le aplique por causas médicas o sanitarias (o bien de la exclusión de un determinado riesgo) constituye una automatización de sus datos de salud. En tal caso, parece claro que debería recabarse el consentimiento expreso del asegurado.
* Por otra parte, cabría preguntarse si la digitalización de documentos constituye o no una automatización de datos propiamente dicha, dado que lo que se automatiza es el documento, no su contenido. En caso afirmativo sería preciso informar de ello al interesado y recabar su consentimiento expreso si los documentos contienen datos sanitarios (lo que ocurre en el caso de una de las entidades analizadas).
* Se ha observado que algunas de las aseguradoras, que forman parte de grandes grupos empresariales, informan en sus formularios de que los datos del cliente serán utilizados por el resto de empresas del grupo, generalmente con objetivos promocionales. En este sentido, sería deseable que formalmente se le permitiera al solicitante decidir sobre ello a la hora de presentar su solicitud y no se le obligara a aceptar estas condiciones ineludiblemente.
* También se ha observado que en general las aseguradoras no disponen de procedimientos suficientemente documentados que contemplen los criterios de la tramitación de las solicitudes de ejercicio de los derechos de sus clientes, aunque algunas sí están trabajando en ello en la actualidad. Sería así mismo deseable que se desarrollasen iniciativas destinadas a concienciar a sus trabajadores acerca de cómo la entidad ha adaptado sus estrategias corporativas a los principios legales de protección de datos.
* Considerando el tipo de relación que une a las aseguradoras con los mediadores de seguros (tanto agentes como corredores), cabe plantearse si éstos poseen también algún tipo de responsabilidad sobre los ficheros que contienen datos de sus propias carteras (lo que les obligaría a declarar sus propios ficheros) y si, en tal caso, podrían hacer un uso de ellos que estuviese amparado por las actividades legítimas que realizan al margen de la aseguradora. Durante las inspecciones realizadas, se ha podido constatar que las compañías tienen opiniones divergentes y que en general no han establecido normas al respecto, por lo que sería preciso que la Agencia estableciese un criterio único para todo el sector.

4.2.14. DEBER DE SECRETO EN EL SECTOR BANCARIO

Durante el año 1998 se iniciaron doce expedientes para investigar denuncias que se recibieron en la Agencia contra entidades bancarias, relacionadas con una posible vulneración del artículo 10 de la Ley Orgánica 5/1992 del deber de secreto 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"; esta infracción está tipificada en su artículo 43.3.g) como falta grave.

En nueve de los expedientes tramitados los denunciantes manifestaban que terceras personas habían accedido, sin su consentimiento, a sus datos personales recogidos en los ficheros automatizados de las entidades bancarias y que dichos datos habían sido utilizados en su contra en procedimientos judiciales que se estaban tramitando; la mayoría de éstos se refieren a procedimientos de modificación de medidas de divorcio o separación.

Una de las principales dificultades en la investigación de los hechos denunciados y en su resolución radica en probar que efectivamente los datos bancarios utilizados por terceras personas han sido obtenidos efectivamente de los propios ficheros de las entidades bancarias; dicha prueba es en la mayoría de los casos determinante cuando existe una prueba documental, por ejemplo, cuando en los procedimientos judiciales se aportan documentos (extractos de cuenta, listados, impresiones de pantalla, etc.) que provienen de las propias entidades bancarias y los afectados no los han solicitado. De la totalidad de estos expedientes tramitados sólo en tres de ellos existía esta prueba documental.

Respecto de las resoluciones sancionadoras se han emitido dos durante el año 1998 contra una misma entidad bancaria por vulneración del deber de guardar secreto, correspondientes a actuaciones de procedimientos que no se habían iniciado ese año. En la tramitación de esos procedimientos sancionadores se acreditó que la entidad bancaria había facilitado a personas distintas de los titulares información de las cuentas bancarias de éstos. De estas resoluciones cabe destacar que en una de ellas se establece la diferencia existente entre la vulneración del deber de guardar secreto y la cesión de datos sin el consentimiento de los afectados. Así se considera que la diferencia radica en que la cesión "supone un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados de forma automatizada por parte del cesionario o se utilicen por este para cualquier decisión posterior respecto de las relaciones que mantenga o pueda establecer con el afectado". Asimismo se considera que esta interpretación se desprende del texto del artículo 11 de la Ley Orgánica 5/1992, en cuanto "describe la cesión como vinculada al cumplimiento de los fines directamente relacionados con las funciones del cedente y cesionario, al exigir para la legalidad de una cesión que tales funciones, del cedente y cesionario, sean legítimas y que el afectado haya prestado su consentimiento. Es decir, la cesión aparece como una conducta encaminada a la prestación de las funciones o actividades de los que intervienen en la comunicación, de modo que si la comunicación no se afecta a tales actividades, si no se dirige a satisfacer una demanda del cesionario, que se servirá de la información para ejercer su actividad, la comunicación del contenido del fichero deberá ser calificada como una violación del deber de secreto".

4.2.15. SALAS DE BINGO

Como consecuencia de una denuncia anónima presentada en la Agencia de Protección de Datos a finales de 1997, y dada la existencia de la Instrucción 2/96, de 1 de marzo, sobre ficheros automatizados para el control del acceso a los casinos y salas de bingo, se decidió abrir un Plan de Oficio para estudiar el grado de cumplimiento de la Ley Orgánica 5/1992, de 29 de octubre, y de la citada Instrucción.
Como primer paso, se solicitó al Registro General de Protección de Datos el estudio del estado de inscripción de los ficheros privados cuyos responsables pertenecieran al sector de Actividades Recreativas y Bingos.
Una vez analizado el informe remitido por el Registro, se requirió a diversas Asociaciones de Bingos existentes en las distintas Comunidades para que enviaran a la Inspección de Datos la relación de Bingos asociados a cada una de ellas, indicando su nombre, dirección y categoría, así como información relativa a la legislación autonómica existente en esta materia.
A continuación se realizaron inspecciones en once Salas de Bingo ubicadas en Valencia, Bilbao, Madrid, Barcelona y Sevilla, de las que se han extraído las siguientes conclusiones:

4.2.15.1. Información a los afectados

En el transcurso de las inspecciones realizadas se ha podido comprobar que a ninguna de las personas que han entrado en las correspondientes Salas de Bingo, se les ha informado de los puntos incluidos en el artículo 5 de la Ley Orgánica 5/1992, de 29 de octubre. Sin embargo siempre ha sido visible para los afectados la informatización de sus datos.

4.2.15.2. Inscripción de ficheros en el Registro General de Protección de Datos

Únicamente dos de los Bingos inspeccionados, tenían sus ficheros inscritos en el Registro General de Protección de Datos antes de realizar la inspección. El resto de los Bingos ha procedido a cumplimentar dicho requisito con posterioridad a la inspección.

4.2.15.3. Tipología de los datos tratados

Todos los Bingos inspeccionados disponen de datos relativos a:
* Clientes: personas que acceden a la Sala de Bingo. Los datos son facilitados por los propios clientes (nombre y apellidos, domicilio, DNI, pasaporte o permiso de conducir). Se incluyen también observaciones y fechas de las visitas.
* Prohibidos: personas que tienen prohibido el acceso a la Sala. Los datos son facilitados por organismos de la Administración Local y/o Comisión Nacional del Juego, en base a los deseos expresados por los propios afectados, sus familiares o las propias Salas de Bingo.

Uno de los Bingos dispone además de un fichero que recoge los datos de aquellas personas que desean recibir envíos publicitarios. Estas personas prestan su consentimiento para ello firmando una ficha al efecto.
Conforme a lo indicado en la Orden del Ministerio del Interior de 9/1/79, por la que se aprueba el Reglamento del Juego del Bingo, este tipo de establecimientos debe recoger de cada visitante los siguientes datos: nombre y apellidos, domicilio, DNI, pasaporte o permiso de conducir, observaciones y fechas de las visitas.
La Instrucción 2/96 de la Agencia de Protección de Datos indica que no podrán recogerse más datos personales que aquellos estrictamente necesarios para controlar el acceso, quedando, en todo caso, limitados a los que aparecen en el documento identificador exigido a la entrada.

4.2.15.4. Seguridad

En este Plan no se han contemplado en profundidad aspectos relativos a la seguridad de los datos tratados, debido a que todavía no se ha procedido a la publicación del correspondiente desarrollo reglamentario al que alude el artículo 43.3.h) de la Ley Orgánica 5/1992.
Sin embargo, en las inspecciones realizadas sí se ha podido observar el celo con el que se guardan los datos recabados, no permitiendo el acceso a personal no autorizado.
Por otra parte se ha obtenido la siguiente información:
* En general la aplicación que gestiona el control de acceso a las distintas Salas de Bingo inspeccionadas, no permite la realización de consultas masivas.
* A dicha aplicación suele tener acceso únicamente el personal que desempeña las funciones de control de entrada al Bingo, además del Jefe de Sala o el Servicio de Inspección del Juego.

4.2.15.5. Cancelación de datos

De todas las Salas de Bingo inspeccionadas, únicamente 3 de ellas cancelan los datos anteriores a los seis meses, tal como se especifica en la Instrucción 2/96, de 1 de marzo.
El País Vasco y la Comunidad Valenciana disponen de legislación autonómica que especifica un período mayor de permanencia de los datos.

4.2.15.6. Cesiones

En ninguno de los Bingos inspeccionados se ha detectado la existencia de cesiones ilegales. Las declaraciones de los representantes de los mismos indican que únicamente se ceden datos a las autoridades competentes tales como el Servicio de Inspección del Juego de cada una de las Comunidades Autónomas o mediando un mandamiento judicial al efecto.

4.2.16. TARJETAS DE IDENTIFICACIÓN EN UNIVERSIDADES

Como consecuencia de tres escritos de reclamación, se han tramitado tres expedientes relativos a otras tantas Universidades, en relación con la implantación de una tarjeta de identificación universitaria implantada en colaboración con otras tantas entidades bancarias.
Los citados proyectos implican la elaboración de una tarjeta dirigida a alumnos, profesores y personal de administración y servicios, que incluye banda magnética, microchip y, en algún caso, código de barras.
Dicha tarjeta 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 y firmen el correspondiente contrato, puede tener las funcionalidades financieras de tarjeta de crédito y monedero electrónico. La parte universitaria es obligatoria y la parte financiera es optativa.

Las tarjetas pueden ser de uno de los tipos siguientes:
Tarjeta monedero.
Tarjeta de débito mixta
Tarjeta de crédito mixta

Las facilidades incorporadas a las tarjetas serían:
Financieras:
Monedero universal, en el chip, en los tres tipos de tarjetas (será necesaria la firma del correspondiente contrato para poder hacer uso de los monederos electrónicos).
Facilidades propias de las tarjetas de débito (es necesario tener abierta una cuenta de ahorro en la entidad bancaria correspondiente).
Facilidades propias de las tarjetas de crédito (es preciso cumplir las condiciones de concesión de tarjetas de crédito).
Propias de la Universidad
Carnet identificativo que se plasmará en el plástico (con el nombre del titular) y en el chip con nombre, número de identificación, colectivo al que pertenece, número de lector de Biblioteca, información académica y perfil de acceso a áreas restringidas.
Las aplicaciones a implantar en la Universidad, en diferentes fases, y basadas en los datos contenidos en el chip serían:
Control de acceso a áreas restringidas.
Préstamos de libros en Bibliotecas.
Acceso a información universitaria de carácter general.
Acceso a información universitaria de carácter privado.
Expedición de certificados normalizados.
Matriculación y pago de cursos y seminarios.
Petición de certificados no normalizados.
Control de presencia.

Finalidades y usos:
Información: generalizada sobre la actividad universitaria (fechas, cursos, seminarios, etc.) y personalizada sobre notas y comunicaciones particulares para una persona o colectivo.
Gestión: pago de matrículas, expedición de certificados, pago de cursos, etc.
Control de acceso a determinadas áreas y control de presencia de personal.
Biblioteca: control de préstamos.
Funciones bancarias: soportadas por el monedero electrónico de la tarjeta tanto telefónico como abierto para el pago generalizado en los diferentes terminales punto de venta instalados tanto en el entorno de la Universidad como fuera de ella.
Para poner en marcha estos proyectos, las Universidades han facilitado a las entidades bancarias, entidades emisoras de las tarjetas, datos relativos a los posibles titulares de las mismas.
Los datos han sido facilitados en base a un convenio o acuerdo marco de colaboración suscrito en cada caso entre ambas entidades. En algunos casos, existe de forma específica un compromiso de confidencialidad sobre los datos tratados por parte de la entidad bancaria. En otros se menciona que deberá respetarse la legislación vigente.
En general los afectados han sido informados de este proyecto a través de las juntas de personal, secretarías de los centros y delegaciones de alumnos. Así mismo los alumnos reciben una hoja informativa en el momento de realizar las correspondientes matrículas, por lo que pueden decidir si desean que su tarjeta tenga las funcionalidades financieras o no y, caso de desear dichas funciones, pueden dirigirse a la entidad bancaria para formalizar el correspondiente contrato.
En algunos casos está estipulado en el convenio que la entidad bancaria deberá destruir, tanto los datos de los no clientes de dicha entidad como los datos no necesarios para la gestión de tarjeta financiera de los clientes de la misma que la Universidad periódicamente le comunique.
Además, aparte de la labor de la Inspección antes mencionada, el Director de la Agencia ha mantenido diversos encuentros y reuniones con responsables de universidades en las que se han abordado distintos aspectos de esta materia en relación con la protección de datos personales y, en concreto, en el encuentro que mantuvo el mes de diciembre con los gerentes de las universidades catalanas.

5 SECRETARIA GENERAL

Las principales actividades realizadas por la Secretaría General durante 1998 han ido dirigidas a posibilitar el funcionamiento de la Agencia de Protección de Datos, en sus aspectos materiales, técnicos y de recursos humanos, así como el Área de atención al ciudadano. Para ello se han efectuado las siguientes tareas y funciones en cumplimiento de las competencias que el Real Decreto 428/93 de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, atribuye a la Secretaría General :

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 citado Real Decreto 428/93, en los siguientes órganos:

- El Director de la Agencia, asistido por su Secretaría Particular, Unidad de Apoyo y el Jefe del Gabinete Jurídico, integrados por 5 funcionarios.
- El Consejo Consultivo
- El Registro General de Protección de Datos, integrado por 11 funcionarios.
- La Inspección de Datos, constituida por 23 puestos de trabajo de funcionarios.
- 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.

Gráfico S.G. Núm. 1
UNIDAD DE APOYO

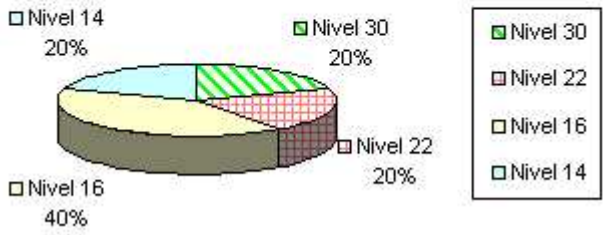
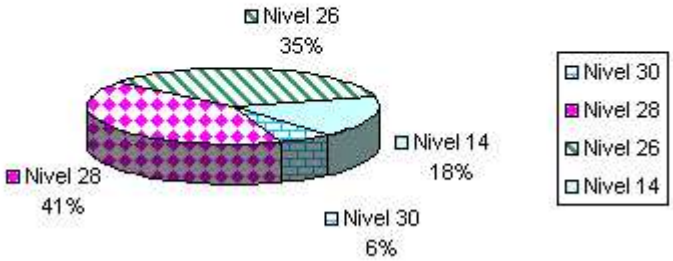
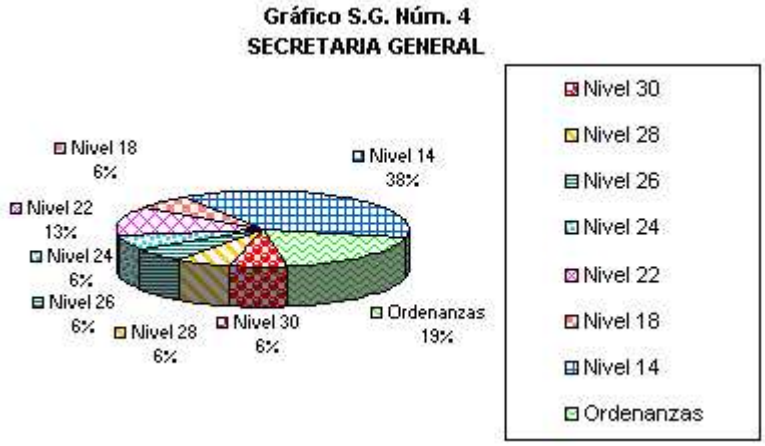


Gráfico S.G. Núm. 2
REGISTRO GENERAL DE PROTECCIÓN DE DATOS

Gráfico S.G. Núm. 3
SUBDIRECCION GENERAL DE LA INSPECCIÓN DE DATOS





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 55 puestos de trabajo que se proveen por funcionarios y 3 ordenanzas con vínculo laboral.

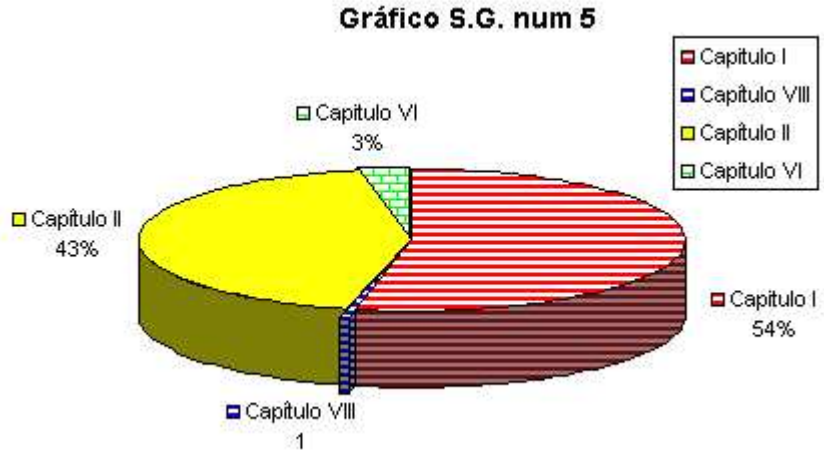
* Elaboración del anteproyecto de la Oferta de Empleo Público, en el que se solicita nuevamente la inclusión de las tres plazas de Ordenanza, actualmente cubiertas con personal eventual, a fin de que puedan ser provistas con personal laboral fijo.

* Ejecución del Plan de Acción Social de la Agencia de Protección de Datos para 1998, así como Aprobación del Proyecto de Plan de Acción Social del Ente Público para 1999, siguiendo las recomendaciones previstas en el Acuerdo de Administración - Sindicatos 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.

* Contratación y 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. En el año 98 se han dictado resoluciones de procedimientos sancionadores imponiendo multas por un importe de 957 millones de pesetas.

* Contrato de arrendamiento: Se mantiene un contrato de arrendamiento de las plantas 3ª, 4ª, y 5ª del edificio del Paseo de la Castellana nº 41, con una extensión de 1725 metros cuadrados. La duración de dicho contrato expira el 31 de diciembre del año 2000. Asimismo se mantiene el contrato de arrendamiento de un pequeño local destinado a almacén y archivo del Ente Público.

* Actualización permanente del inventario de los bienes y derechos que integran el patrimonio de la Agencia.

* Gestión de la Biblioteca de la Agencia: Ha continuado la adquisición de volúmenes y ejemplares para la formación de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales y tecnologías de la información.

5.3. OTRAS FUNCIONES Y TAREAS

En el ejercicio de sus competencias, la Agencia de Protección de Datos Española ha sido designada para organizar **la XX Conferencia Internacional de Autoridades de Protección de Datos** que tuvo lugar en Santiago de Compostela los días 16 a 18 de septiembre de 1998.

Asistieron a la Conferencia las Autoridades de Control de todos los países de la Unión Europea y sus delegaciones, además de un representante de la Comisión Europea y otro del Consejo de Europa. Asimismo, participaron los Directores y miembros de las Autoridades de Control de Australia, Nueva Zelanda, Japón, Hong-Kong, Canadá, Hungría, Suiza, Noruega e Islandia.

Asistieron en calidad de observadores profesores universitarios y altos funcionarios de distintos países, un responsable del Departamento de Comercio del Gobierno de los Estados Unidos y un representante de la Embajada de Estados Unidos en España, así como representantes de asociaciones de marketing .

Durante la celebración de la Conferencia se contó con la estimable colaboración de distintas Consejerías de la Xunta de Galicia así como del Ayuntamiento de Santiago de Compostela.

En la Conferencia se abordaron los temas que se indican en el apartado OTRAS ACTIVIDADES DE LA AGENCIA y se aprobaron dos declaraciones conjuntas que se recogen en el referido apartado.

Se ha convocado la **SEGUNDA 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, constituido por el Consejo Consultivo de la Agencia de Protección de Datos, otorgó el Premio a la obra " La protección de los datos de carácter personal en el ámbito de la investigación penal" presentada por el Profesor Asociado de Derecho Procesal de la Universidad del País Vasco D: José Francisco Etxeberría Guridi. De la referida obra la Agencia ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional.

La obra premiada aborda las materias y contenidos que se relacionan detalladamente en el apartado de otras activi - dades de esta memoria.

Dada la calidad de las obras presentadas el Jurado decidió por unanimidad conceder un accésit, dotado con 100.000 pesetas, a la obra titulada " La responsabilidad civil del responsable del fichero en la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal , de la que es autor el Profesor Titular de la Universidad de las Islas Baleares D. Pedro Grimalt Servera.

* 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 1998.

El contenido de estas reuniones se detalla en el apartado dedicado al Consejo Consultivo de esta memoria.

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 perso - nas 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 comunica - ción 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, 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 ha consistido en la inserción de anuncios divulgativos en prensa escrita diaria y dominical de máxima difu - sión 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 comunica - ción, tanto de los medios impresos como de medios audiovisuales y fundamentalmente emisoras de radio. Se ha podido constatar, una vez más, el importante efecto que la campaña ha producido en el número de ciudadanos que se han dirigido a la Agencia no sólo en demanda de mayor información sobre esta materia sino también mediante la presentación de numerosas consultas, demandas de información, reclamaciones o denuncias. Asimismo ha tenido un importante efecto en el incremento de solicitudes de inscripciones de ficheros automatizados en el Registro General de Protección de Datos.

5.4.2. CAMPAÑA INFORMATIVA MEDIANTE TRÍPTICOS Y MANUALES

Además de la campaña de comunicación en periódicos, se ha continuado con la difusión de varios trípticos divulgativos con información general que permite conocer al público los objetivos de la campaña. Su contenido versa sobre infor - mación general de la Ley Orgánica, las funciones de la Agencia, ejercicio de los derechos por los ciudadanos, ficheros de morosidad y marketing directo. En estos folletos se trata de divulgar de forma simplificada la información elemental en materia de protección de datos. Para su difusión se ha contado, como en años anteriores, con la colaboración del Instituto Nacional de Consumo, Oficinas Municipales de Información al Consumidor, Asociaciones de Consumidores de ámbito Nacional y de ámbito Autonómico y Direcciones Generales de Consumo de las Comunidades Autónomas, así como diferentes asociaciones de consumidores, de vecinos y de colectivos diversos. Asimismo se han entregado a los ciudadanos que se dirigen a la Agencia en demanda de información.

Con el fin de ampliar y complementar el contenido de los trípticos se ha reeditado, introduciendo modificaciones y nuevos modelos, el Manual explicativo del tratamiento automatizado de datos de carácter personal, de la Ley Orgánica 5/92 y de la Agencia de Protección de Datos, dirigido primordialmente a los organismos públicos y privados cuya misión sea la de informar a los ciudadanos de sus derechos en materia de consumo o materias relacionadas con la intimidad y su protección frente al uso indebido de la informática. Se ha entregado también a todos aquellos ciudadanos interesa - dos en la materia.

También, se ha procedido a la edición y distribución del Manual sobre Recomendaciones a Usuarios de Internet elaborado por la Agencia. La distribución se ha efectuado fundamentalmente a través de las Oficinas Municipales de Información al Consumidor y otras Organizaciones y Asociaciones de Consumidores, habiéndose hecho también entrega del mismo a los ciudadanos que lo han solicitado.

Por último se ha llevado a cabo la edición de unos trípticos informativos acerca de los derechos de los ciudadanos, básicamente derechos de acceso, rectificación y cancelación ante el Sistema de Información de Schengen. La Autoridad de Control de Schengen realizó un modelo de cartel y de trípticos, con objeto de que, en base a ese diseño la edición y distribución de carteles y trípticos se llevara a cabo por cada uno de los países integrados en el Convenio de Schengen.

En cumplimiento de tal mandato se procedió a la contratación de una empresa externa para la edición de 4.000 carteles y 50.000 trípticos. La distribución de los mismos se ha efectuado a través de Embajadas y Oficinas Consulares y del Ministerio del Interior que los distribuye en aeropuertos, puertos marítimos fronterizos y otros puestos fronterizos.

Al mismo tiempo se hace entrega de los mismos por la Oficina de Atención al Ciudadano de la Agencia a los ciudadanos que solicitan información en esta materia.

5.4.3. INFORMACIÓN MEDIANTE MEMORIAS Y CD ROM

Con el fin de cumplir con la tarea de informar a los ciudadanos acerca de sus derechos en materia de protección de datos personales y de la existencia de la Agencia, el Area de Atención al ciudadano ha hecho entrega a los ciudadanos que lo solicita de la Memoria Anual de la Agencia, así como del CD Rom que se viene editando anualmente con el siguiente contenido: el catálogo de los ficheros automatizados de carácter personal inscritos en la Agencia a 30 de abril de 1998; las memorias de actividad de los años 1994, 1995, 1996 y 1997, la estadística del Registro General de Protección de Datos; el texto de la conferencia sobre Seguridad Privacidad y Protección de Datos; el libro de las Jornadas sobre el Derecho Español de la Protección de Datos realizado en octubre de 1996; el trabajo ganador del premio Protección de Datos personales 1997, recomendaciones para los usuarios de internet, Legislación sobre Protección de Datos; así como el Manual de Tratamiento de Datos Personales Informatizados.

5.5. EL ÁREA DE ATENCIÓN AL CIUDADANO

El Área de Atención al Ciudadano ha recibido a lo largo de 1998, 12.780 consultas telefónicas (frente a 10.000 en 1997), 1500 consultas presenciales (1.300 en 1997) y 1453 consultas por escrito (1009 en 1997). Estas cifras suponen un incremento del 15,4 % de las consultas presenciales, un incremento del 30% en las llamadas telefónicas, y un 44% de las consultas escritas. 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. Las consultas realizadas a través de Internet superan el 25% del total de las consultas recibidas por escrito.

Resulta particularmente destacable en este año el acceso por parte de los ciudadanos a la página web informativa en Internet de la Agencia (www.ag-protecciondatos.es), que contiene una guía informativa, modelos para ejercer los derechos recomendaciones a usuarios de internet, legislación, que para notificar la inscripción de ficheros tanto de titularidad pública como privada, así como el catálogo actualizado de ficheros inscritos en la Agencia. A lo largo de 1998 se realizaron más de 216.000 accesos.

Dado el interés que las consultas de los ciudadanos 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.

Se clasifican las consultas en función de los sectores de actividad a los que afectan. En primer lugar, se plantean las consultas de 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, consultas sobre ficheros policiales, estadísticos, ficheros creados para el control del acceso a edificios y consultas en relación con el sector de telecomunicaciones Por último, se trata un apartado, que hemos considerado mixto, dada la especial naturaleza de las actividades a que se refiere. Incluimos en este apartado: la Sanidad, las Relaciones Laborales y el Desempleo, la Educación, que pueden llevarse a cabo tanto por el sector público como privado; finalmente se incluyen en este apartado las Corporaciones de Derecho Público, 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 o su finalidad, dependiendo del aspecto que se considere más importante en cada caso, con el fin de evitar repeticiones.

Gráfico Núm. 6

CONSULTAS POR SECTORES A LOS QUE AFECTA

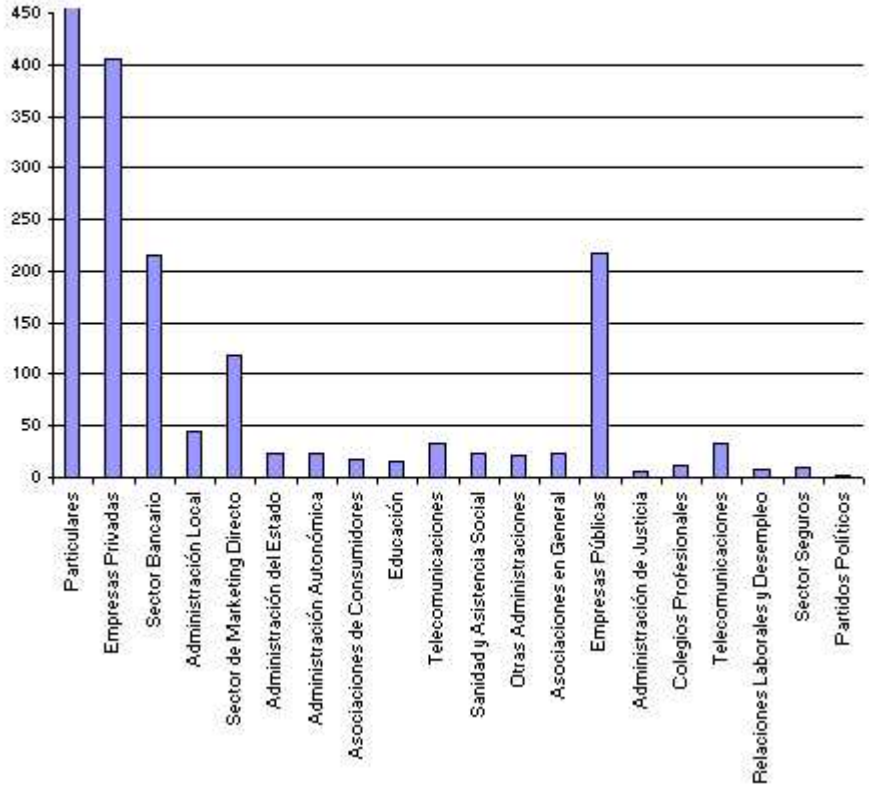
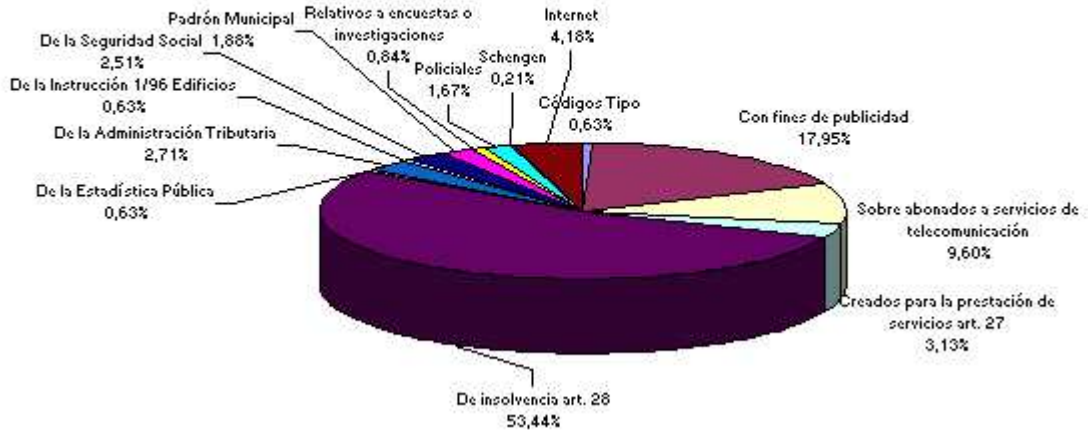


Gráfico S.G. Núm. 7

CONSULTAS POR TEMAS

Gráfico S.G. Núm. 8
TIPOS DE CONSULTAS SOBRE CESIONES DE DATOS

Gráfico S.G. Núm. 9
CONSULTAS SOBRE FICHEROS CONCRETOS 1998



5.5.1. FICHEROS SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Las cuestiones relativas a los ficheros sobre solvencia patrimonial y crédito continúan siendo 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, fundamentalmente este último.

La necesidad de mejorar las garantías en el tráfico mercantil basado en el crédito personal en su sentido más amplio, justifican la existencia de este tipo de ficheros. Ahora bien, la Ley Orgánica, reconoce la legalidad de este tipo de ficheros, pero 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 una restricción importante en las posibilidades de acceso a créditos, 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.

En todo caso la regulación de la LORTAD de este tipo de ficheros se refiere sólo a personas físicas. 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.

5.5.1.1. Información sobre el alcance del deber de comunicación del artículo 28.

En este tipo de ficheros quiebra el principio general de la Ley consagrado en sus artículos 6 y 11, que exigen el consentimiento del afectado para el tratamiento y la cesión de sus datos personales. Se sustituye la necesidad del consentimiento previo informado por la notificación posterior de los datos más relevantes de dicha inclusión, con un doble objetivo: por una parte, informar al ciudadano de la inclusión, dada la gran trascendencia que la misma tiene para sus derechos; por otra dar al ciudadano la posibilidad de rectificar y cancelar dichos datos en el caso de que sean erróneos. La primera garantía establecida por la Ley Orgánica, es la obligación de comunicar al afectado su inclusión en esta clase de ficheros, para que con este conocimiento, el mismo pueda oponerse a su inclusión, solicitando la cancelación o rectificación en su caso.

La información que se proporciona al ciudadano en esta materia se puede resumir en los siguientes puntos:
* La obligación de comunicar la inclusión en estos ficheros se extiende tanto a los supuestos de información sobre solvencia patrimonial y crédito, como a la información relativa al cumplimiento o incumplimiento de obligaciones dinerarias, con independencia del origen de los datos.
* 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.

5.5.1.2. Ejercicio de los derechos de acceso, rectificación y cancelación en relación con los ficheros de solvencia patrimonial y crédito

Se han realizado frecuentes consultas sobre las actuaciones necesarias ante la inclusión de datos personales en un fichero de morosidad o impagados cuando no se conoce la identidad concreta del responsable del fichero de impagados al que se deben dirigir.
El derecho de acceso puede ejercerse bien ante el propio fichero de información sobre solvencia o bien ante todas aquellas personas o entidades bancarias o de financiación que tienen acceso o conocimiento de datos relativos a solvencia patrimonial y crédito, que 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 solicitud 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 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 seis años contados a partir de la inclusión en el fichero de morosos, o, en todo caso, a partir del cuarto mes del vencimiento de la obligación incumplida.
Otros problemas que se plantean con cierta frecuencia, son los relativos a la existencia de números del Documento Nacional de Identidad repetidos y casos de personas cuyo nombre y apellidos es completamente coincidente o sustancialmente coincidente con el de otras u otras personas. En estos supuestos sucede que se deniega habitualmente la cancelación de los datos, porque el responsable del fichero, considera que los datos procesados son correctos. En estos casos se aconseja que el afectado obtenga del Instituto Nacional de Estadística una notificación acreditativa de las personas que ostentan el mismo nombre y apellidos. También se puede efectuar esta misma operación ante la Dirección General de la Policía cuando es el nº de D.N.I. el coincidente para varias personas.
En todo caso el ejercicio de estos derechos es personalísimo lo que justifica que los responsables de estos ficheros exijan el D.N.I. a los afectados para comprobar su identidad.

5.5.2. PUBLICIDAD DIRECTA

También este sector continúa teniendo un número importante de consultas y quejas por parte de los ciudadanos, después de los ficheros de morosidad. La petición más frecuente manifestada ante la Agencia es el deseo de no recibir información comercial. Se han recibido quejas frecuentes y solicitudes de información en relación con la publicidad nominativa no solicitada y remitida por empresas con las que el afectado carece de relación previa.

El afectado debe dirigirse a cada una de las empresas que le remiten publicidad solicitando información sobre qué datos tienen y cómo los han obtenido y, en su caso, la cancelación de los datos en sus ficheros. 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.

El artículo 26 de la Ley Orgánica a la vez que reconoce la facultad de las empresas que presten servicios de telecomunicación, de utilizar los datos sobre sus abonados, y determina que los números de los teléfonos y demás servicios de telecomunicación, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, reconoce el derecho al afectado de exigir su exclusión, en el caso de que no desee aparecer en dichos repertorios.

Hay que destacar que datos como los que proporciona el servicio Servicios Electrónicos de Telecomunicación 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 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.

Para mayor información en relación con publicidad y telecomunicaciones se puede acudir al apartado de telecomunicaciones: utilización de repertorios telefónicos de esta Memoria.

5.5.2.1. Publicidad directa a través de Internet

Un tema nuevo se plantea en relación con publicidad directa 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 es la forma más común de registrar la "identidad" de una persona en Internet. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección se utiliza en múltiples lugares de la red y puede ser conseguida fácilmente sin conocimiento del afectado. Sin embargo, su aspecto más preocupante radica en que sirva de base para la confección de perfiles personales (temas de interés, inclinaciones políticas, orientaciones sexuales, etc.) a partir de la pertenencia a listas de distribución, o basándose en la participación en grupos de discusión, corriendo el riesgo de ser etiquetados por la pertenencia a los mismos.
El envío de publicidad no solicitada a través del correo electrónico requiere, lógicamente, el conocimiento de la dirección de correo electrónico del receptor del mensaje. Adicionalmente, una dirección de correo electrónico puede tener asociada información de carácter personal, tal como la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa que se dedique a la publicidad directa. Las formas más habituales de obtener direcciones de correo sin el conocimiento del usuario son:
* Listas de distribución y grupos de noticias.
* Captura de direcciones en directorios de correo electrónico.
* Venta, alquiler o intercambio de direcciones de correo por parte de los proveedores de acceso.
* Entrega de la dirección de correo, por parte de los programas navegadores, al conectar a los servidores Web.
* Recepción de mensajes de correo requiriendo contestación a una dirección determinada y pidiendo la máxima difusión de los mismos.

La Agencia recomienda a este respecto que cuando se incluya la dirección de correo electrónico en un directorio o lista de distribución, se considere la posibilidad de que la misma pueda ser recogida por terceros para enviar mensajes publicitarios no deseados. También conviene conocer la política de alquiler, venta o intercambio de datos que han adoptado tanto el proveedor de acceso a Internet como los administradores de los directorios y listas de distribución donde esté incluido.
Si no se quiere dar difusión a la dirección de correo electrónico, es necesario configurar el navegador para que no deje su dirección de correo en los servidores Web a los que accede.
Por último conviene destacar que se han producido un nº considerable de peticiones tanto de las Recomendaciones de Internet, como del Código tipo de comercio electrónico recientemente inscrito en la Agencia.

5.5.3. CESIONES DE DATOS CON NATURALEZA TRIBUTARIA

Se han producido algunas consultas de ciudadanos en relación con las cesiones de datos de carácter personal de naturaleza tributaria. En este sentido cabe hacer referencia a la planteada por el director de una residencia asistida que solicita información sobre la legalidad de ceder los datos del Libro de Registro de las personas asistidas a la Inspección de Tributos de la Delegación de Hacienda de Barcelona. Los datos que contiene este libro son: en el libro de Altas, nombre y apellidos, fecha de ingreso, número de D.N.I., número de afiliación a la Seguridad Social, tarifa o cuota acordada por el servicio, depósito efectuado, médico de cabecera y número de colegiado, seguro de accidentes y de defunción, nombre y apellidos del familiar responsable, parentesco, domicilio completo, teléfono. En el Libro de Bajas, fecha de la baja, causa o motivo, observaciones.

Con carácter previo, es necesario tener en cuenta que la Ley Orgánica 5/92, limita su ámbito de aplicación a los datos personales automatizados, por lo que las respuestas se refieren tan sólo a los datos que se encuentren informatizados, pero no a los que se encuentran en papel.

El artículo 11 de la Ley determina que la cesión de datos por parte del responsable del fichero a un tercero sólo 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 en la Ley General Tributaria en su artículo 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:

5.5. 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....

Por otra parte, estos datos se podrán solicitar siempre que se cumpla con lo preceptuado en el artículo 109 de la Ley General Tributaria en conexión con el artículo 4 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal. En el artículo 109 de la L.G.T. se marcan los límites de la comprobación e investigación tributaria, estableciendo lo siguiente:

1. La Administración comprobará e investigará los hechos, actos, situaciones, actividades y demás circunstancias que integren o condicionen el hecho imponible.

2. La comprobación podrá alcanzar a todos los actos, elementos y valoraciones consignados en las declaraciones tributarias y podrá comprender la estimación de las bases imponibles, utilizando los medios a los que se refiere el artículo 52 de esta Ley.

En el artículo 4 de la Ley Orgánica, se establece que los datos han de ser adecuados y no excesivos en relación con la finalidad para la que solicitan.

En consecuencia, sólo podrán facilitarse aquellos datos que sean necesarios, adecuados pertinentes y no excesivos en relación con la comprobación tributaria de que se trate.

5.5.4. FICHEROS POLICIALES

Las principales consultas de ciudadanos sobre ficheros policiales versan sobre los siguientes aspectos que a continuación de desarrollan:

5.5.4.1. Cancelación de datos en los ficheros del Sistema de Información de Schengen

Se ha solicitado información a la Agencia sobre el procedimiento que debe seguirse para recurrir la decisión de las autoridades italianas de denegar la concesión de un visado para el territorio Schengen; la persona en cuestión tiene un nombre muy común en su país de origen, por lo que considera que ésta pueda ser la causa de su inclusión en este fichero. También manifiesta que España es el país que ha incluido a esta persona en el fichero de Schengen, según la información facilitada por las autoridades italianas al denegar el visado.

En relación con esa petición hay que señalar que el acuerdo de adhesión del Reino de España al convenio de aplicación del acuerdo de Schengen de 14 de junio de 1985, regula esta materia. En concreto en el Título IV, sobre el Sistema de información de Schengen establece en su Capítulo III la protección de los datos de carácter personal y seguridad de los datos en el marco del Sistema de Información de Schengen.

En este sentido, el artículo 109 del citado Convenio reconoce:

1. El derecho de toda persona a acceder a los datos que se refieran a ella y estén introducidos en el Sistema de Información de Schengen se ejercerá respetando el Derecho de la Parte contratante ante la que se hubiere alegado tal derecho. Si el Derecho nacional así lo prevé, la autoridad nacional de control prevista en el apartado 1 del artículo 114 decidirá si se facilita información y con arreglo a qué modalidades. Una Parte contratante que no haya realizado la descripción no podrá facilitar información relativa a dichos datos, a no ser que previamente hubiere dado a la Parte contratante informadora la ocasión de adoptar una posición.

2. No se facilitará información a la persona de que se trate si dicha información pudiera ser perjudicial para la ejecución de la tarea legal consignada en la descripción o para la protección de los derechos y libertades de terceros. Se denegará en todos los casos durante el período de descripción con vistas a una vigilancia discreta.

Por su parte, el Artículo 110 del mismo Convenio establece que toda persona podrá hacer rectificar datos que contengan errores de hecho que se refieran a ella o hacer suprimir datos que contengan errores de derecho que se

refieran a ella. Por último, en el artículo 114 se establece que:
1. Cada Parte contratante designará a una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre el fichero de la parte nacional del Sistema de Información de Schengen y de comprobar que el tratamiento y la utilización de los datos introducidos en el Sistema de Información de Schengen no atentan contra los derechos de la persona de que se trate. A tal fin, la autoridad de control tendrá acceso al fichero de la parte nacional del Sistema de Información de Schengen.
2. Toda persona tendrá derecho a solicitar a las autoridades de control que comprueben los datos referentes a ella integrados en el Sistema de Información de Schengen, así como el uso que se haga de dichos datos. Este derecho estará regulado por el Derecho nacional de la Parte contratante ante la que se presente la solicitud. Si los datos hubieran sido integrados por otra Parte contratante, el control se realizará en estrecha colaboración con la autoridad de control de dicha Parte contratante.
La legislación nacional vigente en España en materia de protección de datos es la Ley Orgánica 5/92. Esta ley reconoce una serie de derechos a los ciudadanos, como son el derecho de acceso, rectificación y cancelación de sus datos personales. El ejercicio de los mismos es personal, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables de los ficheros automatizados, lo que significa que el solicitante debe dirigirse al organismo público responsable del fichero, solicitando información sobre qué datos tienen y cómo los han obtenido (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación). También se pueden ejercer estos derechos a través de representantes legales debidamente acreditados y apoderados.
Para la resolución del problema planteado, es necesario dirigirse en primer lugar a la Secretaría de Estado de Seguridad del Ministerio de Interior, responsable del fichero en España, exponiendo el problema. En la petición se debe hacer referencia al ejercicio de los derechos de acceso, rectificación y cancelación en relación con el fichero NSIS/SIRENE**. Este fichero tiene por finalidad la gestión nacional para el sistema de información de Schengen.**
En el caso de que la petición sea desatendida, podrá entonces dirigirse el afectado, o su representante legal a la Agencia de Protección de Datos, que es la autoridad de control sobre este fichero en España. Si en el plazo de un mes para el derecho de acceso y de 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, nuevamente también podrá dirigirse a la Agencia con copia de la solicitud cursada, para que ésta, a su vez, se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de sus derechos.

5.5.4.2. Cancelación de los 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. Pero esta certificación debe completarse con otros documentos que demuestren que no existen por cada caso concreto otras causas abiertas en las Audiencias ni en los juzgados o tribunales o que la causa concreta que obra en los archivos policiales ha concluido con auto de sobreseimiento o sentencia absolutoria.
Por último, sería necesario evaluar si la cancelación de los datos podría implicar 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. 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 está justificado.

5.5.5. FICHEROS ESTADÍSTICOS

Los ciudadanos consultan con frecuencia sobre la legalidad de las diversas encuestas de familias o de servicios del Instituto Nacional de Estadística. La recogida de los datos se realiza sobre sujetos seleccionados aleatoriamente, a los que se les informa de que la facilitación de estos datos es de cumplimentación obligatoria, basándose en la Ley de la Función Estadística Pública de fecha 9 de mayo de 1.989 y Reglamento de Procedimiento Sancionador de las infracciones por incumplimiento de las obligaciones estadísticas, aprobado por Real Decreto 1.572/1.993.

En este sentido, el artículo 3 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal en su apartado tercero establece lo siguiente:

3. Se regirán por sus disposiciones específicas:
d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, sin perjuicio de lo dispuesto en el artículo 36.

El artículo 10 de la Ley la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública establece que :

1 . Los servicios estadísticos podrán solicitar datos de todas las personas físicas y jurídicas, nacionales y extranjeras, residentes en España.

2. Todas las personas físicas y jurídicas que suministren datos, tanto si su colaboración es obligatoria como voluntaria, deben contestar de forma veraz, exacta, completa y dentro del plazo a las preguntas ordenadas en la debida forma por parte de los servicios estadísticos.

Estos preceptos determinan la obligación por parte de los ciudadanos de aportar la información solicitada. Nos encontramos ante un supuesto en el que las leyes establecen que el derecho a la intimidad debe ceder ante al interés común, representado en este caso por la función estadística pública.

Es de resaltar al respecto que todos los cuestionarios estadísticos deben ser sometidos por el Instituto Nacional de Estadística a dictamen previo de la Agencia de Protección de Datos.

5.5.6. FICHEROS DE ACCESO A EDIFICIOS

Se solicita información sobre la Instrucción 1/1996, de 1 de marzo de la Agencia, sobre el modo de averiguar si en los ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios se mantienen los datos indefinidamente. Para la contestación es necesario tener en cuenta las normas tercera y quinta de la referida Instrucción, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, que establecen lo siguiente:

Norma tercera- Recogida de datos

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. Los datos recogidos serán los estrictamente necesarios para cumplir la finalidad de controlar el acceso.

Norma quinta- Cancelación de los datos

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados.

Para averiguar si los datos se han mantenido en el fichero más allá del plazo establecido, deberá ejercer el derecho de acceso. Si en el plazo de un mes para el derecho de acceso desde la recepción de la solicitud en la oficina referida, ésta no ha sido atendida adecuadamente, 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.

En todo caso es preciso destacar que estas normas son de aplicación a los ficheros de acceso a edificios que se encuentren automatizados, pero no si se encuentran únicamente en soporte papel.

5.5.7. TELECOMUNICACIONES

5.5.7.1. Utilización de los repertorios telefónicos

Los ciudadanos consultan sobre si los datos personales incluidos en los Directorios Telefónicos de acceso público pueden usarse para finalidades de marketing o análogas. En este sentido el artículo 26 de la Ley Orgánica 5/92 establece que los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado. Concretamente, en el fichero Servicios Electrónicos de Telecomunicación aparecen el nombre y apellidos completo (no sólo las iniciales) así como la dirección, y, salvo que el afectado se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general. En relación con la publicidad nominal el artículo 29 relativo a los Ficheros con fines de publicidad establece que:

"1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos figuren en documentos accesibles al público o cuando hayan sido facilitados por los propios afectados u obtenidos con su consentimiento.

2. Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud."

En estos casos se sugiere al ciudadano que, si no desea recibir publicidad, puede ejercer el derecho de exclusión de sus datos de los repertorios telefónicos, al amparo del citado artículo 26.

Conviene destacar la publicación en el mes de julio de una norma que afecta directamente a la privacidad en el marco de las comunicaciones telefónicas. Concretamente nos referimos al Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, aprobado por Real Decreto 1736/1998, de 31 de julio, que establece en su artículo 70 que los operadores que presten servicios avanzados de telefonía con la facilidad de identificación de la línea llamante deberán ofrecer la posibilidad de que el usuario que origine las llamadas pueda suprimir en cada una de ellas y mediante un procedimiento sencillo y gratuito, dicha identificación.

En este sentido la Resolución de 2 de diciembre de 1998 de la Secretaría de Estado de Comunicaciones, el Ministerio de Fomento, publicada en el BOE de 30 de diciembre, establece el código 067 para el servicio de supresión en origen, llamada a llamada, de la identificación de línea llamante.
En consecuencia, el establecimiento del referido código 067 permitirá soslayar la posible lesión contra la intimidad que supone la identificación del número llamante ya que existe un procedimiento previsto para suprimir en origen dicha identificación.

5.5.7.2. mantenimiento de los datos de tráfico telefónico

Algunos ciudadanos han consultado sobre si está previsto en la legislación de protección de datos un período durante el que se pueden mantener los datos del tráfico telefónico, y si se pueden mantener durante un período más prolongado si fuera necesario por razones judiciales y policiales.
Ni la Ley Orgánica 5/92, ni la legislación de desarrollo establecen ninguna previsión concreta limitando el tiempo máximo de permanencia de los datos del tráfico telefónico, sino tan sólo una previsión general en el artículo apartado 5 en relación con la calidad de los datos:

"5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos."
Además en la Ley Orgánica existen previsiones expresas tanto para las cesiones de datos para los Jueces , Tribunales y Ministerio Fiscal, como las Fuerzas y Cuerpos de Seguridad. Para el caso de los Jueces , Tribunales y Ministerio Fiscal, el artículo 11 establece en su apartado 2 d) como excepción al principio de consentimiento del afectado:
"2. El consentimiento exigido en el apartado anterior no será preciso:
.....
d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas."
.....
Por lo que se refiere a las Fuerzas y Cuerpos de Seguridad el artículo 20 establece lo siguiente:

"1. Los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento 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.*

3. la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

4. los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad

5.5.7.3. Exigencia del número de tarjeta de crédito en el alta en un servicio de telecomunicaciones que no conlleva obligación de pago.

Se plantea la cuestión ante la Agencia de la legalidad de la exigencia del número de su tarjeta de crédito por parte de una empresa de telefonía al darse de alta como cliente asociado, a pesar de que la acción en cuestión no implica ninguna obligación de pago.

El artículo 4 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal, relativo a la calidad de los datos, establece en su apartado primero que:

1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dichos tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.

Por su parte, el artículo 11 de la Ley Orgánica determina que con carácter general se requiere el consentimiento previo del afectado para proceder a la cesión de sus datos.

Como conclusión, hay que señalar que sólo podrán recabarse los datos necesarios y no excesivos para aquellas finalidades para las que se solicitaron, lo que al parecer no sucede en el caso que plantea, toda vez que en principio sería excesivo el nº de la tarjeta de crédito para darse de alta como cliente si ello no supone asumir obligación alguna de pago.

5.5.8. SANIDAD

En este capítulo se tratan las cuestiones relativas al sector de la Sanidad, tanto pública como privada, 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 actividades es extraordinariamente relevante, desde el punto de vista de la Ley, toda vez que los datos de salud tienen la consideración de especialmente protegidos.
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.
Se plantea por tanto un conflicto entre el derecho de cancelación de los datos y la necesidad de conservarlos para la realización de estudios epidemiológicos, para los que el mantenimiento de los datos es imprescindible.

5.5.8.1. Historial clínico: derechos de acceso y cancelación

Con carácter previo a la contestación a las 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. 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 y copia de todo su historial médico. La Ley Orgánica 5/92 reconoce el derecho de acceso en el artículo 14 que:
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 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 : *en 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 también por las normas penales y civiles para los supuestos de responsabilidad por posibles negligencias médicas.

5.5.9. 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 a un entramado complejo de sujetos: el empresario, el trabajador, las Asociaciones de Empresarios, los Sindicatos o las Administraciones Públicas. En los ficheros automatizados de personal de las empresas está contenida una gran cantidad de información relativa a los trabajadores, que incluye tanto datos relativos a la vida profesional de los mismos, titulación, puestos desempeñados, retribuciones, junto a otros relativos a la vida familiar como el estado civil o el número de hijos. También y sin abandonar la vida estrictamente laboral, nos encontramos ante otros datos especialmente protegidos como los datos de salud contenidos en las bajas laborales, enfermedades profesionales, etc. o incluso datos relativos a ideología, como la afiliación sindical a partir del descuento de las cuotas sindicales.

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 gestorías para la gestión de sus ficheros de personal, que actúan de 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 un otorgamiento genérico 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.

5.5.9.1. Cesiones obligatorias datos de AA.PP. a Organizaciones sindicales

Se solicita a la Agencia informe sobre la legalidad de que un sindicato pueda obtener de la Administración de una Comunidad Autónoma una relación con los nombres y direcciones de todos los empleados al servicio de esa Administración.

El artículo 1 del Real Decreto 1332/94 de 20 de junio de desarrollo de la Ley Orgánica 5/92 define cesión de datos como toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de los datos realizada por toda persona distinta de la afectada; por lo que facilitar los datos solicitados a un sindicato por parte de esa Administración sería un supuesto de cesión de datos de los previstos en la Ley Orgánica.

El artículo 11 de la citada ley regula las cesiones y establece con carácter general la necesidad del consentimiento del afectado para que sus datos puedan ser cedidos a un tercero. La única excepción a este principio general aplicable a este caso ha de estar prevista en una norma que tenga rango de Ley. En el caso de las Administraciones Públicas se insiste en el artículo 19, en que no obstante, lo establecido en el artículo 11.2.b) la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

Las excepciones de los derechos de las personas deben interpretarse siempre con un carácter restrictivo. Para poder determinar qué datos se pueden ceder habrá que analizar las previsiones que las diferentes leyes lleven a cabo a este respecto. Además la Exposición de Motivos de la Ley Orgánica pretende limitar, cuando no evitar, actividades como las descritas y se hace referencia al principio de consentimiento, o de autodeterminación, que otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el perfil personal, cuya obtención transgrediría los límites de la privacidad.

Teniendo en cuenta los preceptos y principios interpretativos indicados, se puede analizar en el ámbito del derecho sindical la existencia de una serie de normas en las que se prevén cesiones de datos de carácter personal a los sindicatos.

La Ley 9/1987 de 12 de junio, de Órganos de representación, Determinación de las Condiciones de Trabajo y Participación del Personal al servicio de las Administraciones Públicas establece en su artículo 9 la información que ha de entregarse a las Juntas de Personal y Delegados de Personal, sin que en dicho artículo se haga referencia a los datos que contempla la consulta.

Por lo que se refiere al artículo 11 de la Ley Orgánica de Libertad Sindical (LOLS), se prevé tan sólo que el empresario, o en su caso Administración, proceda al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia al sindicato a solicitud 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, y para los datos que excedan del cumplimiento de la misma será necesario además el consentimiento del trabajador así como la conformidad del empresario. En caso de cesión de los datos que excedan de los estrictamente necesarios el empresario podría estar incurriendo en una falta muy grave de acuerdo con el 43.4.b. de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal.

El conjunto de preceptos y principios citados determina que la cesión deberá ampararse en este caso en normas con rango de Ley, que caso por caso, podrán prever la cesión de modo individualizado y concreto, por lo que la solicitud planteada carece en principio de una habilitación legal concreta, lo que determinaría la vulneración de la Ley Orgánica.

5.5.9.2. Base de datos de sindicatos en el ámbito de la empresa

Se solicita información sobre la legalidad de crear una Base de Datos en la que consten los datos de los trabajadores facilitados por la propia Empresa. En ningún caso, figurarían datos que se puedan entender como especialmente protegidos, tales como raza, religión, sino los datos que facilita la empresa, como nombre, apellidos, fecha de alta en la empresa, categoría, etc. pretende usar dichos datos para hacer envíos personalizados internos y en ningún caso serían facilitados a ninguna empresa externa. En concreto, se plantea si sería necesario pedir autorización por escrito a cada empleado para la inclusión de estos datos dentro de la base de datos, y si este fichero se debe inscribir en el Registro General de Protección de Datos de la Agencia.

Con carácter general, el criterio determinante para proceder a la inscripción de un fichero es el tratamiento automatizado de los datos relativos a personas físicas; por lo que si tienen cualquier fichero informatizado que contenga datos de esta clase deberán proceder a la notificación del fichero en el Registro General de Protección de Datos de la Agencia.

No obstante lo anterior, por lo que se refiere a los datos de los afiliados sindicales, el artículo 2.2 de la Ley Orgánica relativo a las excepciones en ámbito de aplicación de la misma, establece que el régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex-miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

De lo anteriormente expuesto, se deduce que los ficheros relativos a afiliados no se encuentran regulados por la Ley Orgánica, salvo en lo relativo a las cesiones de datos.

Por el contrario, los datos de los trabajadores facilitados por la Empresa que no pertenecen al sindicato deben cumplir con la normativa vigente, dado que se encuentran dentro del ámbito de la Ley Orgánica.

Por último y tal y como se explica en el apartado anterior puede considerarse ajustada a la Ley la entrega de los datos indispensables para el cobro de la cotización sindical, pero no de aquellos otros como fecha de nacimiento, dirección (salvo que se refiera a la del centro de trabajo) o sexo, que no estarían amparados por ley alguna, lo que determinaría la vulneración de la Ley Orgánica. Deberán, por tanto, solicitar el consentimiento de los trabajadores para este fin.

5.5.9.3. Utilización de bases de datos para el control de productividad

Se solicita información sobre legalidad del control del trabajo mediante programa informático. El programa sirve para registrar y controlar los expedientes tramitados. Uno de los datos son las iniciales del trabajador que tramita el expe - diente. El jefe de la dependencia pide información sobre el número de expedientes tramitados por cada persona de la oficina, aunque nunca se informó de que ese dato iba a ser usado para medir la productividad.

En primer lugar, hay que señalar que la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos resulta de aplicación al caso, al tratarse de datos personales automatizados. Esta Ley exige como principio general el consen - timiento del afectado par el tratamiento automatizado de los datos. Una de las excepciones a este principio se prevé para aquellos supuestos en que los datos son necesarios para el mantenimiento de las relaciones laborales

En el ámbito de la relación jurídica que existe entre los empleados y la empresa en la que prestan sus servicios, debe entenderse adecuado que el empleador recabe los datos que sean precisos para el normal desenvolvimiento de la misma y, dentro de estos datos, parece adecuado que se recaben del empleado los correspondientes a su identidad a efectos de controlar el trabajo para que se pueda comprobar el grado de cumplimiento de las obligaciones que competen a los empleados. En este sentido, el Estatuto de los Trabajadores establece como una obligación del traba - jador el contribuir a la mejora de la productividad (artículo 5 letra e). Por su parte, el apartado 3º del artículo 20 del mismo Estatuto establece que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

El artículo 4.1 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal establece, efectivamente, que los datos sometidos al tratamiento automatizado no deben ser excesi - vos en relación con el ámbito y las finalidades legítimas para las que se han obtenido.

La Sentencia del Tribunal Constitucional de 22 abril 1993, en Recurso de amparo núm. 190/1991, excluye del ámbito de la intimidad, constitucionalmente amparado, a «los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada". 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".

En el artículo 5 de la LORTAD se establece una serie de extremos sobre los que se debe informar en el momento de recoger los datos, pero en el apartado 3º se excepciona de dicha obligación en los supuestos en que estos extremos se deduzcan del modo en el que han sido recogidos. En este sentido, la finalidad del control de la productividad está implícita en la propia relación laboral, por lo que se debe considerar sobreentendido este requisito en el momento de formalizar la relación laboral.

Como conclusión, hay que señalar que no parece que el comportamiento descrito contradiga por sí mismo los princi - pios de la legislación vigente, toda vez que la información personal se utiliza en el medio laboral exclusivamente y en el marco de una relación contractual para una finalidad intrínsecamente laboral y prevista como tal por el Ordenamiento Jurídico.

5.5.9.4. Control de los datos de conexión a internet en el ámbito de la empresa

Se plantea una consulta acerca de la legalidad del control por parte de la empresa del acceso a Internet por parte de los trabajadores, sin que se impongan a éstos restricciones de uso ni de seguimiento del uso que se realiza de la conexión. Se han limitado, sin embargo algunas funciones, email, chat, ftp, ... Parece ser que se proporciona a la Direc - ción un listado con las páginas a las que ha accedido cada empleado, que lo divulga y da a conocer según su criterio. Considera el consultante que mediante estos listados se tiene acceso a información íntima del tipo - tendencias sexua -

les - opiniones religiosas y políticas - enfermedades contagiosas - etc... de la persona que utiliza Internet. Sin desconocer la necesidad de limitar el uso del teléfono o del correo en el entorno laboral, se plantea si la intervención sin previo aviso es legal y sino podría considerarse análoga a regulación del registro de las taquillas personales.

Del Estatuto de los Trabajadores se desprende que las actuaciones por parte del empresario en el ámbito laboral pueden limitar los derechos fundamentales de los trabajadores. El empresario tiene en principio la potestad de controlar el cumplimiento de las obligaciones laborales, así como el uso profesional de los instrumentos de trabajo, como el uso del ordenador y de Internet. No parece, en principio, justificado que en el uso laboral de Internet se pueda revelar información íntima del tipo - tendencias sexuales - opiniones religiosas y políticas - enfermedades contagiosas - etc... de la persona que utiliza Internet. Se trataría más bien de un uso privado de medios laborales que el empresario puede controlar.

La tecnología de Internet permite el almacenamiento de información en el servidor del empresario. En este sentido, la distribución desde un servidor en la propia empresa forma parte del sistema de comunicación. En consecuencia, no es equiparable a las escuchas telefónicas, porque éstas exigen la intervención de las líneas de comunicación para la escucha de conversaciones, mediante aparatos que de suyo no forman parte de la instalación telefónica, y deben ser autorizadas por los Jueces y Tribunales. Tampoco es equiparable al registro de las taquillas del trabajador, dado que el acceso queda limitado al titular, y para registrar la taquilla sería necesario cumplir con ciertos requisitos preestablecidos.

De todo lo anterior, se deduce que dado las circunstancias del caso, no parece que la actuación sea contraria a los preceptos de la Ley Orgánica 5/92.

5.5.9.5. Cesión de nombre, teléfono particular de un trabajador para conceder una subvención para formación.

Se consulta sobre la legalidad de una cesión de datos personales con motivo de la realización de unas acciones formativas destinadas a mejorar el nivel técnico del personal. Estas acciones formativas están en parte pagadas por la empresa y en parte subvencionadas. Por otra parte existe un organismo que se encarga de tramitar estas subvenciones y al que los centros de formación deben demostrar que han impartido una serie de cursos a personas concretas.

Para que el centro de formación demuestre la participación en los cursos se solicita al trabajador que firme un cuestionario, que ha sido impreso por la empresa desde su sistema de nómina, en el que aparecen los siguientes datos: nombre y apellidos, DNI, Nº Seguridad Social, sexo, fecha de nacimiento, teléfono particular, teléfono de contacto (el de la empresa) y dirección de residencia.

El trabajador en cuestión eleva una queja formal a sus directores respecto a que se facilite al organismo su dirección y teléfono particulares, siendo informado de que éstos datos son imprescindibles para la solicitud de subvención y que la alternativa consiste en renunciar a participar en la acción formativa.

Algunos de los datos solicitados parecen ser excesivos para la finalidad de que se trata; en concreto, el teléfono particular y la residencia particular no parecen ser necesarios en principio para la realización de un curso formativo en el ámbito de la empresa.

La cesión de los datos solicitados (no sólo teléfono y domicilio particular), para esta finalidad no se encuentra prevista de modo específico por las normas, y dado que, de conformidad con el artículo 4.2. apartado b) del Estatuto de los Trabajadores, la formación profesional en el trabajo tiene el carácter de derecho y no de obligación, sería necesario solicitar el consentimiento del trabajador para la realización del curso, y, en ese momento, se le debería informar de que la aceptación implica necesariamente la cesión de sus datos a un tercer organismo.

5.5.10. EDUCACIÓN

5.5.10.1. Utilización de internet en el ámbito de las universidades.

Algunas Universidades desean facilitar un servicio de directorio que proporcione información acerca de su personal y de sus alumnos. La información que se ofrecería es la dirección de correo electrónico que facilita la universidad y, en el caso de personal, el número de teléfono del despacho. Esta información estaría disponible, a través de Internet, con carácter general.

Se plantean, por algunos afectados si tales datos constituyen información personal y si deben dar su consentimiento para publicarlos. Por su parte las universidades entienden, en principio, que la información de quiénes son sus trabajadores y estudiantes es pública y que el número de teléfono y la dirección de correo electrónico no tienen el carácter de dato personal, puesto que pertenecen a la Universidad.

Para esta cuestión se debe tener en cuenta el principio general de consentimiento del afectado establecido en el artículo 6 de la Ley Orgánica. Con este precepto, se establece el principio general del consentimiento del afectado y sus excepciones en relación con los usos posteriores de sus datos. Esta vinculación se refuerza con el principio de finalidad de los datos recogido en el artículo 4, relativo a calidad de los datos, que en su apartado segundo establece que 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.

La obtención o simple visualización por un tercero no autorizado, de datos de los alumnos o profesores al margen de la

relación administrativa necesaria sería contraria a la Ley Orgánica. Si la misma se debe a la autorización errónea de los accesos nos encontraríamos ante una cesión indebida.

Si se pretende ampliar la accesibilidad a los datos de los alumnos y empleados de la Universidad, con carácter general en Internet, más allá de lo que la relación académico administrativa y laboral, en su caso, pueda implicar de modo razonable, será necesario complementar la solicitud del consentimiento previamente informado de los afectados de estos extremos, cumpliéndose para ello con las previsiones del artículo 5 de la Ley Orgánica, relativo al derecho de información en la recogida de datos.

5.5.11. COLEGIOS PROFESIONALES.

5.5.11.1. Legalidad de la cesión de datos tributarios al Colegio de Abogados para la concesión de Justicia gratuita.

Plantea un ciudadano la legalidad de la solicitud de datos personales por parte del Colegio de Abogados, con motivo de la petición de la Asistencia Jurídica Gratuita, dado que considera que estos datos ya son conocidos por el Colegio referido al referir en su consulta que el Colegio dispondría de un terminal que se conecta con la Delegación de Hacienda.

En relación con la primera cuestión, sobre el carácter adecuado o no de la solicitud de sus datos para la concesión de Asistencia Jurídica Gratuita, hay que tener en cuenta los siguientes preceptos. En los artículos 4, 12 y 13 de la Ley 1/1996, que regula la Asistencia Jurídica Gratuita, se regulan algunos de los aspectos que se plantean en su consulta. En estos preceptos se establece lo siguiente:

Artículo 4. Exclusión por motivos económicos.

A los efectos de comprobar la insuficiencia de recursos para litigar, se tendrá en cuenta además de las rentas y otros bienes patrimoniales o circunstancias que declare el solicitante, los signos externos que manifiesten su real capacidad económica, negándose el derecho a la asistencia jurídica gratuita si dichos signos, desmintiendo la declaración del solicitante, revelan con evidencia que éste dispone de medios económicos que superan el límite fijado por la Ley.

La circunstancia de ser el solicitante propietario de la vivienda en que resida habitualmente, no constituirá por sí misma obstáculo para el reconocimiento del derecho, siempre que aquélla no sea suntuaria.

Artículo 12. Solicitud del derecho.

El reconocimiento del derecho a la asistencia jurídica gratuita se instará por los solicitantes ante el Colegio de Abogados del lugar en que se halle el Juzgado o Tribunal que haya de conocer del proceso principal para el que aquél se solicita, o ante el Juzgado de su domicilio. En este último caso, el órgano judicial dará traslado de la petición al Colegio de Abogados territorialmente competente.

Cuando haya concurrencia de litigantes en un proceso, el reconocimiento del derecho a la asistencia jurídica gratuita deberá ser instado individualmente por cada uno de los interesados.

Cuando con arreglo a las leyes procesales, los solicitantes deban litigar bajo una sola defensa o representación, deberán computarse, a efectos del reconocimiento del derecho, la totalidad de los ingresos y haberes patrimoniales de los solicitantes. En este caso, si se acreditara que los ingresos y haberes patrimoniales de cada uno de los solicitantes no sobrepasan el doble del salario mínimo interprofesional, se procederá a nombrar abogado y, en su caso, procurador del turno de oficio que deberán asumir la representación y defensa conjunta de todos ellos.

Si se acreditara que los ingresos y haberes patrimoniales de cada uno de los solicitantes superan el doble del salario mínimo interprofesional pero no alcanzan el cuádruple, la Comisión de Asistencia Jurídica Gratuita podrá determinar cuáles de los beneficios establecidos en el artículo 6 se otorgará a los solicitantes.

Artículo 13. Requisitos de la solicitud.

En la solicitud se harán constar, acompañando los documentos que reglamentariamente se determinen para su acreditación, los datos que permitan apreciar la situación económica del interesado y de los integrantes de su unidad familiar, sus circunstancias personales y familiares, la pretensión que se quiere hacer valer y la parte o partes contrarias en el litigio, si las hubiere.

De conformidad con estos preceptos, la solicitud de los datos patrimoniales para comprobar la situación económica del solicitante de asistencia jurídica gratuita, parece conforme con el artículo 4 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos.
Sin embargo, el acceso directo por parte del Colegio de Abogados a los ficheros de la Delegación de Hacienda, podría ser contrario a lo establecido en la Ley Orgánica 5/92, pero no ha quedado acreditado la existencia de tal acceso directo.

5.5.11.2. El carácter de fuente accesible al público de los listados de Colegiados

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 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 para otra finalidad.

MEMORIA DE 1998 - CÓDIGOS TIPO

1.- Introducción.

El artículo 31 de la Ley Orgánica 5/92, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), prevé la posibilidad de formular códigos tipo a los responsables de ficheros de titularidad privada, a través de acuerdos sectoriales o mediante decisiones de empresa, en los que se establezcan:

1. Condiciones de organización
2. Régimen de funcionamiento
3. Procedimientos aplicables
4. Normas de seguridad del entorno, programas o equipos
5. Obligaciones de los implicados en el tratamiento y uso de la información personal
6. Garantías, para el ejercicio de los derechos de las personas con respecto a la Directiva y las normas de desarrollo de los estados miembros
7. Medidas a adoptar por el incumplimiento del código

Estos códigos tienen el carácter de códigos deontológicos o de buena práctica profesional, y pueden ser depositados en el Registro General de Protección de Datos (RGPD), dónde se procederá a su inscripción, siempre que se ajusten a las disposiciones legales y reglamentarias sobre la materia, o bien se denegará tal inscripción, en caso contrario. En este último supuesto, previamente, los solicitantes son requeridos para que efectúen las correcciones necesarias.

2.- Análisis normativo

La ley Orgánica 5/1992, de 28 de octubre (LORTAD) contempló desde un primer momento la posibilidad de elaborar códigos de conducta (art. 31) para facilitar la correcta aplicación de las normas reguladoras de la protección del tratamiento automatizado de datos de carácter personal.

No ha sido, por tanto, necesario esperar a la aprobación de la Directiva 95/46/CE ni a su transposición al derecho interno para abordar la posibilidad de elaborar los citados códigos de conducta.

Ahora bien, a la vista de la regulación recogida en la LORTAD y en la Directiva 95/46/CE resulta conveniente plantear las cuestiones que a continuación se mencionan y que se refieren, particularmente, a los sujetos habilitados para la elaboración de códigos tipo.

La Ley española no menciona expresamente los sujetos habilitados para la elaboración de códigos de conducta limitándose a señalar el carácter o ámbito que pueden tener los acuerdos a través de los cuales se adoptan.

Sin embargo, de su literalidad se desprende que cabe una doble opción: acuerdos sectoriales y acuerdos de empresa.

La primera de ellas coincide plenamente con las previsiones del artículo 27 de la Directiva 95/46/CE.

Por el contrario, la segunda posibilidad, es decir, la elaboración de Códigos de conducta por una sola empresa va más allá de las previsiones de la de la Directiva.

En efecto, los artículos 27.1 y 2 de la Directiva prevén que la elaboración de códigos de conducta tengan carácter sectorial, al señalar el apartado 1 que deben adaptarse a las peculiaridades de cada sector y, referir en su apartado 2 que los sujetos habilitados al efecto sean "las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos".

Sin embargo, la posibilidad contemplada en la norma española puede resultar apropiada, al menos, por las siguientes razones:

- La fuerza ejecutiva en el seno de una empresa puede ser más intensa que en el ámbito de una asociación sectorial. Así se aprecia en la experiencia española en la que códigos de conducta adoptados por una empresa contemplan sanciones más contundentes (falta laboral grave) que las previstas en los códigos de asociaciones sectoriales.

- La competencia entre empresas que operan en un mismo sector estimula la adopción de códigos tipo más estrictos, puesto que los mismos se están convirtiendo en un elemento económico relevante para ganar o conservar cuota de mercado (sector de la solvencia patrimonial y de los registros de morosidad).

Admitida la posibilidad de que los códigos de conducta puedan ser adoptados en el ámbito de una sola empresa, debe considerarse qué criterios han de aplicarse para conseguir que su aprobación suponga un valor añadido respecto de la protección derivada de la norma nacional. En este sentido, la Agencia de Protección de Datos considera que deben utilizarse, al menos, los siguientes:

- El número de datos personales que son objeto de tratamiento por parte de la empresa. De este modo puede conse-

guirse que los principios de protección de datos personales se apliquen de forma efectiva respecto de un número relevante de usuarios.

- El número de empleados vinculados a la empresa. Con ello se pretende conseguir que los principios propios de la protección de datos personales sean conocidos y asumidos por un número importante de personas que los recaban o tratan.

Ambos criterios han sido aplicados en la única experiencia práctica en la que se ha elaborado un código de conducta en el ámbito de una sola empresa. En efecto, el Código de conducta fue elaborado por la empresa Telefónica de España S.A., que solicitó su inscripción en el Registro General de Protección de Datos, siendo, en aquel momento, la única operadora de telefonía fija y móvil. Concurrían, por tanto, no sólo el hecho de tratar datos personales de un número elevado de clientes, sino también el hecho de contar con una considerable plantilla de empleados.

- La segunda particularidad de la normativa española en relación a los sujetos habilitados para la adopción de códigos de conducta consiste en que únicamente se admiten respecto de operadores privados, quedando excluidas las distintas modalidades organizativas que adoptan las Administraciones Públicas.

En esta materia el artículo 27 de la Directiva 95/46/CE permite interpretar que cabe la posibilidad de que los códigos de conducta pudieran ser adoptados en el ámbito de las Administraciones Públicas en la medida en que no exige expresamente que se trate de ficheros de titularidad privada. Junto a ello, el artículo citado contempla como sujetos habilitados, además de a las asociaciones profesionales, a "las demás organizaciones representantes de otras categorías de responsables del tratamiento". Bajo esta rúbrica pueden incluirse las distintas Administraciones Públicas y las organizaciones en que se agrupan (v. gr. las federaciones de entes locales de distintos ámbitos territoriales).

La posibilidad de que puedan elaborarse códigos de conducta por las Administraciones Públicas debe considerarse de interés con el fin de facilitar el conocimiento de la normativa reguladora de la protección de datos personales, armonizar sus actuaciones en esta materia y favorecer su cumplimiento. Máxime si se tiene en cuenta que las citadas Administraciones son operadores que tratan automatizadamente un volumen ingente de datos personales de los ciudadanos.

En relación con esta cuestión, la conveniencia de someter a reglas comunes a los ficheros de titularidad pública y privada, está siendo debatida por los Grupos Parlamentarios en la transposición de la Directiva 95/46/CE.

3.- Experiencias prácticas

En lo que se refiere a la experiencia práctica sobre códigos de conducta, los supuestos en que se ha producido han sido los siguientes:

Solicitante: TELEFONICA DE ESPAÑA S.A.

Presentación: 1994

Objeto y ámbito de aplicación

Este código es desarrollado por Telefónica, que lo adopta mediante una decisión de empresa, con el fin de ceñirse en su gestión a la más estricta legalidad. Se desarrolla por medio de una normativa interna, que articula las prescripciones de la LORTAD en los diversos procesos de gestión empresarial de forma unitaria y homogénea.

El código se establece como una normativa de obligado cumplimiento para todas las Unidades de la Empresa y, en particular, para aquéllas que intervienen en la recogida, tratamiento y entrega de los datos de carácter personal obrantes en ficheros automatizados de Telefónica, así como para los directivos titulares de las Unidades designadas como responsables operativas de dichos ficheros.

Inscripción: 1994

"CODIGO ETICO DE PROTECCION DE DATOS PERSONALES DE LAS EMPRESAS DE SERVICIOS COMERCIALES"

Solicitante: ASOCIACION DE EMPRESAS DE SERVICIOS DE INFORMES COMERCIALES (ASEICO)

Presentación: 1995

Objeto y ámbito de aplicación:

ASEICO, consciente de la importancia de la labor de sus miembros, reconoce la necesidad para el sector de elaborar este Código Etico, con el fin de prevenir las violaciones de la privacidad de las personas que pudieran resultar del tratamiento de los datos personales.

El código se aplica a las relaciones que mantienen las empresas asociadas a ASEICO con los comerciales o profesio-

nales sobre los que se elaboran informes comerciales, con los usuarios de los mismos, así como a las relaciones que dichos asociados pueden mantener entre sí y con terceras personas, empresas, entidades u organismos relacionados de forma directa o indirecta con el ejercicio de la actividad de información comercial.

Inscripción: 1995

"REGLAMENTO DEL FICHERO HISTORICO DE SINIESTRALIDAD DE CONDUCTORES"

Solicitante: UNION ESPAÑOLA DE ENTIDADES ASEGURADORAS Y REASEGURADORAS (UNESPA)

Presentación: 1998

Objeto y ámbito de aplicación:

El Fichero Histórico de Siniestralidad de Conductores, se fundamenta jurídicamente en el artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados que permite a las entidades aseguradoras establecer ficheros comunes tanto para la colaboración estadística como en la prevención del fraude en la selección de riesgos y en la liquidación de siniestros. El reglamento de regulación de este fichero pretende la adecuación a la LORTAD, especialmente en todo lo previsto en cuanto a garantizar los derechos de las personas cuyos datos son tratados en el mismo, formulándolo como código tipo.

Se constituye desde la Comisión Técnica de Seguro de Automóviles de UNESPA, titular del fichero, y es de aplicación en todas las entidades aseguradoras adheridas a este fichero.

Inscripción: Se encuentra en trámite

"CODIGO ETICO DE PROTECCION DE DATOS PERSONALES EN INTERNET"

Solicitante: FEDERACION ESPAÑOLA DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECEMD)

Presentación: 1998

Objeto y ámbito de aplicación:

Este código surge a través de la Asociación Española de Comercio Electrónico (AECE), actualmente FECEMD, que reconoce la necesidad de regular unas normas de compromiso voluntario por parte de las empresas que operan en Internet, con el fin de proteger la intimidad de las personas en el tratamiento automatizado de los datos de carácter personal en Internet.

Pueden adherirse al Código todas aquellas empresas que comercializan productos o servicios en Internet y tratan datos personales.

El código dedica un capítulo a establecer unos principios adicionales aplicables a las actividades on-line dirigidas principalmente a menores, los cuales en comparación con los adultos, pueden no entender la naturaleza de la información que se les pide o los usos a los cuales se puede destinar la información.

Inscripción: 1998

"CODIGO ETICO DE PROTECCION DE DATOS PERSONALES DE LA ASOCIACION DE PUBLICIDAD DIRECTA Y BASES DE DATOS PD&BD"

Solicitante: ASOCIACION DE PUBLICIDAD DIRECTA Y BASES DE DATOS PD&BD

Presentación: 1999

Objeto y ámbito de aplicación:

Tiene por objeto la regulación del uso de las tecnologías de la información y singularmente de la informática, en su aplicación al tratamiento informatizado de los datos personales por parte de las empresas miembro de la PD&BD, desarrollando en este código términos establecidos en la LORTAD.

Quedan sujetas a este Código cualesquiera actividades de tratamiento automatizado de datos personales, ya sea de naturaleza principal o accesoria e incluso las previas o posteriores al tratamiento automatizado propiamente dicho,

realizadas por los asociados a la PD&BD.

Inscripción: En trámite

De ellos merece una consideración específica el reciente Código Etico de Protección de Datos Personales en INTERNET elaborado por la Asociación Española de Comercio Electrónico. Sus aspectos más destacables son los que a continuación se mencionan.

- Pese a la denominación de la Asociación promotora del Código, éste no contempla la globalidad de cuestiones relacionadas con el comercio electrónico, sino que se ocupa, fundamentalmente, del marketing por E-mail.

Aún con esta acotación, presenta un interés específico por referirse a relaciones que se desarrollan en INTERNET, ámbito en el que la protección del tratamiento automatizado de datos personales ofrece dificultades adicionales a las que se producen cuando la actividad publicitaria se desarrolla a través de sistemas convencionales.

- La Asociación que lo ha elaborado incluye empresas muy significativas de diversos sectores como el bancario, los medios de comunicación audio visual y escrita, correos y telégrafos, grandes establecimientos comerciales, edición y distribución de libros, informática, telecomunicaciones, marketing, consultoría y asesoramiento jurídico y empresarial.

- En la promoción del Código ético han participado tres de las principales asociaciones de consumidores, así como la Asociación para el Autocontrol de la Publicidad, organismo de carácter privado que actúa como autorregulador en el ámbito de la publicidad ilícita.

De este modo se ha pretendido que el contenido del Código no se limite a tener en cuenta el criterio de las empresas, sino también la problemática e intereses de los consumidores.

Su presencia no se ha limitado a participar en la elaboración del Código sino que tiene un carácter estructural y permanente. En efecto, de los 10 miembros que integran el Comité de Protección de Datos de la AECE, órgano que tiene atribuida la competencia de control del cumplimiento del Código ético, 4 son representantes de asociaciones de consumidores y 1 de la Asociación de Autocontrol de la Publicidad.

- El derecho de información a los afectados de que sus datos han sido recabados o capturados por los anunciantes encuentra su primera manifestación en la obligación que se impone a éstos de informar en su página web, mediante un aviso, de que se está produciendo dicho tratamiento de datos.

A tal efecto, la página de inicio (home page) debe incluir el sello de garantía de la Asociación, cuya selección proporcionará al consumidor un acceso a pantallas donde se detalla el aviso.

El aviso deberá ser de fácil comprensión y contener como mínimo:

- Una dirección de E-mail, postal u otro sistema de comunicación a través de los que se puedan ejercer los derechos de acceso, rectificación y cancelación, así como la especificación de las finalidades para las que se autoriza el uso de los datos.

La información mínima debe incluir también las posibles cesiones de datos indicando la finalidad a que pueden destinarse.

En el caso de que se produzca la posibilidad de ceder los datos deberá informarse de la finalidad a la que se destinarán.

Finalmente, en relación con la captación de información y el tipo de información captada, el anunciante deberá incluir en la información mínima del hecho de la colocación de "cookies".

- El anuncio en el web del anunciante, como se ha señalado anteriormente, constituye la vía para el ejercicio de los derechos de acceso, rectificación y cancelación.
- El consumidor podrá oponerse, total o parcialmente, a:

- El tratamiento de datos, excepto cuando resulte necesario para la ejecución de contratos celebrados.

- La utilización de datos para algunas de las finalidades sobre las que se le ha informado.

- El consumidor podrá, también, seleccionar o excluir finalidades para las que consiente que sean destinados sus datos. Si las empresas pretenden utilizarlos para finalidades distintas de las consentidas deberán advertirlo expresamente y otorgar un plazo para oponerse.

- En el caso de terceros deberá informársele sobre la identidad de los cesionarios y sobre las finalidades perseguidas con la cesión. El derecho de oposición puede ejercerse mediante un sistema "on-line".

En todo caso, deberá facilitarse una dirección postal u otro sistema de comunicación que no suponga gastos ni inco-

modidades superiores a aquélla.

- La remisión de publicidad a grupos de noticias (newsgroup), tablón de anuncios (bulletin boards) y foros de charlas (chats) debe ser coherente con las políticas declaradas en el seno del foro en cuestión, a cuyo efecto, los operadores de los foros adheridos deberán publicar las políticas aplicables a las posibles ofertas en su foro y, los anunciantes, antes de dirigir ofertas por E-mail, deberán consultarlas y respetar la oposición colectiva manifestada a través del moderador.

Los anunciantes asumen, asimismo, tanto la obligación de informar sobre los riesgos de captación de la información por empresas no adheridas al Código, como la de apoyar iniciativas sobre como educar al consumidor para proteger su intimidad en la red.

- En el caso de utilización de la técnica del SPAM, las ofertas deberán identificarse de modo que puede reconocerse inmediatamente su carácter publicitario, identificando al anunciante en el "subjet" del E-mail.

Adicionalmente, deberán informar sobre la posibilidad de oponerse al envío de ofertas posteriores y proporcionar un mecanismo para ejercitar tal derecho a través de E-mail o de otro medio de comunicación.

- En las relaciones con terceros contratantes las empresas involucradas en la cesión de datos para realizar ofertas por E-mail deberán garantizar que cumplen los principios del Código ético. La misma exigencia se aplica, con carácter contractual, a los anunciantes que alquilen sus listados.

- De utilizarse listados de direcciones electrónicas elaborados a partir de fuentes accesibles al público, los anunciantes o los terceros que las hayan elaborado, deberán asegurarse o exigir contractualmente que los consumidores afectados han podido oponerse a la utilización de sus direcciones y no incluyen las de los que se hubieran opuesto al uso para el que se pretenden utilizar.

- En relación al tratamiento de datos sobre menores, ante la dificultad de conocer cuándo un menor facilita datos, se aplican garantías indirectas que tratan de evitar los riesgos que afectan a tales usuarios.

En primer lugar se trata de que las comunicaciones "on-line" que, por su contenido, tengan presuntamente como destinatarios a menores, se adecuen a las características objetivas del público al que se dirigen.

En segundo lugar, se concede a los padres la posibilidad de que, preventivamente, puedan ejercer los derechos de acceso, cancelación y rectificación, debiendo respetarse el aviso de los padres contrario a la solicitud de información o publicidad. A tal efecto los anunciantes deberán animar a los menores para que consulten con sus padres.

Finalmente, no podrán cederse los datos ni utilizarse para campañas inadecuadas a la edad de los menores.

- El Código ético crea un sello de garantía para las empresas adheridas que tiene por objeto constituir una marca distintiva colectiva, impidiendo que puede usarse como marca propia de la empresa usuaria o como garantía de los productos ofrecidos. Su finalidad queda, por tanto, circunscrita al cumplimiento del Código de conducta, debiendo las empresas usuarias aplicar sin demoras ni reservas las instrucciones de utilización que les sean comunicadas por la Asociación.

- El control del cumplimiento del Código ético se atribuye al Comité de Protección de Datos de la Asociación, cuya composición se ha mencionado con anterioridad.

El propio Comité tiene la obligación de velar por la evaluación del cumplimiento del Código a través de un programa anual de auditorías sistemáticas y al azar.

- Los consumidores que consideren que se ha infringido el Código ético pueden dirigirse a la empresas responsable del fichero o a la Junta Directiva de la Asociación. Si el responsable del fichero no justifica su actuación en el perentorio plazo de 5 días, el consumidor podrá dirigirse al Comité de Protección de Datos.

- Las sanciones previstas en el Código comprenden la advertencia, la amonestación y la retirada temporal o definitiva del sello de garantía.

A ellas se añaden la propuesta de expulsión de la Asociación y, potestativamente, la posibilidad de publicitar la sanción impuesta.

- Finalmente, se prevé la posibilidad de que la Asociación colabore con las empresas adheridas a través del Servicio de Asesoría de Protección de Datos, así como mediante la elaboración de un "software" que facilite la creación de una política de privacidad "on-line" de la empresa.

- Con el fin de mantener actualizado el Código se prevé su evaluación cada dos años para adecuarlo tanto a las inno - vaciones tecnológicas, como a la propia práctica del sector. La revisión se someterá a la Agencia de Protección de Datos con carácter previo a su inscripción.

Como valoración del citado Código ético, el juicio de la Agencia de Protección de Datos es el de que constituye una primera e interesante aproximación a los problemas que suscita el tratamiento de datos personales en Internet. Tales

problemas se centran fundamentalmente en la posibilidad de captar datos personales sin consentimiento ni conocimiento del afectado, pudiendo tratarse automatizadamente para configurar perfiles personales vinculados a una dirección electrónica.

A juicio de la Agencia, la colaboración de los operadores en Internet debe valorarse positivamente, máxime si se tienen en cuenta las dificultades de todo tipo que se producirían en el paso de mantener una conducta de desinterés en esta materia.

De ahí que, aún pudiendo considerarse otras alternativas, se entienda que debe seguirse un proceso gradual que estimule un mejor cumplimiento de las normas de protección. Ello no excluye, en modo alguno, que las infracciones que se produzcan sean perseguidas y sancionadas.

En esta misma línea de facilitar la protección en el ámbito de Internet, la Agencia de Protección de Datos publicó en 1997 unas "Recomendaciones" dirigidas a concienciar a los usuarios sobre las posibilidades de que los datos personales pueden utilizarse de forma irregular, y de las precauciones que deben adoptar para evitarlo.

En dicho proceso resultará necesario intensificar las acciones de evaluación interna y externa del Código de conducta, quedando siempre abierta la posibilidad de proceder a su revocación si se acredita que no cumple las previsiones a las que se dirige.

MEMORIA DE 1998 - ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES DE LOS DISTINTOS PAÍSES EN MATERIA DE PROTECCIÓN DE DATOS.

1. UNIÓN EUROPEA. GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES CREADO POR LA DIRECTIVA 95/46/CE

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo aprobaron la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (designada en lo sucesivo "la Directiva"). El artículo 29 de la Directiva ha creado el grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Este grupo tiene la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal en la Comunidad y en terceros países.

El Grupo de Trabajo se compone de representantes de las autoridades nacionales independientes encargadas de la protección de datos y un representante de la Comisión e incluirá un representante de la autoridad responsable de las cuestiones relacionadas con la protección de datos dentro de las instituciones europeas, a partir de la fecha de la institución de esta autoridad.

Al compartir la experiencia de las autoridades nacionales, el Grupo de Trabajo impulsa la aprobación de una estrategia coherente para la aplicación de los principios generales enunciados en la Directiva y aconseja a la Comisión sobre las cuestiones relacionadas con la protección de datos. Su función consiste especialmente en formular dictámenes sobre el nivel de protección en la Unión y en los terceros países, y en emitir recomendaciones sobre toda cuestión referente a la protección de las personas con respecto al tratamiento de datos de carácter personal.

El Grupo de Trabajo se reunió por primera vez el 17 de enero de 1996. Este comienzo de los trabajos fue a instancia de las autoridades nacionales responsables de la protección de datos. Desde la entrada en vigor de las legislaciones griega e italiana sobre la protección de datos personales, el Grupo de Trabajo reúne desde ahora a las autoridades de control de todos los Estados miembros. A lo largo de 1998 el Grupo se ha reunido en 10 ocasiones.

El Grupo ha venido efectuando un seguimiento en materia de transposición de la Directiva 95/46 constante cada vez que se ha reunido. Se ha constatado dentro del mismo una doble preocupación: por un lado, tratar de cumplir el plazo legal establecido para la transposición que, conforme al artículo 32 de la Directiva, finalizó 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.

En cuanto al cumplimiento del plazo fijado para la transposición de la Directiva, la mayoría de los países integrantes del Grupo han superado ya el plazo previsto para dicha transposición, aun a pesar de haberse iniciado en tiempo y forma el proceso parlamentario. Esto se debe en parte a 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 al derecho interno la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones, y también en algunos países, como es el caso de Suecia, en donde ha sido necesaria una modificación constitucional para poder adoptar la Directiva, e incluso tras la transposición de la misma el Gobierno considera necesaria una nueva modificación de la Ley de Protección de Datos.

La Agencia de Protección de Datos española forma parte de este Grupo de Trabajo, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Como fruto de este trabajo y en el ejercicio de las competencias atribuidas por la Directiva el Grupo de Trabajo del Artículo 29 ha elaborado los siguientes documentos durante 1998:

1. Documento de trabajo: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero? Adoptado por el Grupo de Trabajo el 14 de enero de 1998 (DG XV D/5057/97 final WP 7)

2. Documento de trabajo: Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países Aprobado por el Grupo de Trabajo el 22 de abril de 1998 (DG XV D/5005/98 final WP 9).

3. Recomendación 1/98 sobre los sistemas informatizados de reserva de las líneas aéreas (SIR) Aprobada por el Grupo de Trabajo el 28 de abril de 1998 (XV D/5009/98 final WP 10).

4. Dictamen 1/98 sobre la Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS) Adoptado por el Grupo de Trabajo el 16 de junio de 1998 (XV D/5032/98 WP 11).

5. Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE Aprobado por el Grupo de Trabajo el 24 de julio de 1998 (DG XV D/5025/98 WP 12).

6. Documento de Trabajo: Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo Aprobado el 10 de septiembre de 1998 (DG XV D/5004/98 WP 13).

Los conclusiones más relevantes de los documentos se van a agrupar en cuatro apartados. En primer lugar, se tratarán los parámetros y criterios que, a juicio del Grupo de Trabajo, se deben tener en cuenta para valorar el nivel adecuado de protección de los terceros países a los que se realizan transferencias de datos. En segundo y tercer lugar se abordará el análisis de los Códigos de Conducta y las cláusulas contractuales como medios idóneos para garantizar un nivel de protección adecuado en los terceros países. Por último, se tratará el tema de Internet en otro apartado, uniendo las actuaciones del Grupo junto con las actuaciones de la Unión Europea y del Consejo de Europa en esta materia.

1.1. NIVEL ADECUADO DE PROTECCIÓN

El objetivo de la protección de datos es ofrecer asistencia a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU (1990). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince estados de la Comunidad.

Es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas. En Europa las legislaciones han incluido en general las normas de procedimiento como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos relativos al procedimiento están plasmados en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones.

Fuera del ámbito comunitario es menos común encontrar estos medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos. Los signatarios del Convenio 108 deben incorporar los principios de la protección de datos en su legislación, pero no se requieren mecanismos complementarios tales como una autoridad de control. Las directrices de la OCDE sólo exigen que "se tengan en cuenta" en la legislación nacional y no prevén procedimientos para garantizar que las directrices deriven en una protección efectiva de las personas físicas.

Por otro lado, las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento y de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. El grado de riesgo que, en el caso de una transferencia internacional, supone para el interesado será un factor importante para determinar los requisitos concretos de un caso determinado.

1.1.1. Principios fundamentales de la protección de datos

Principio de limitación de objetivos (finalidad) - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por alguna de las razones expuestas en el artículo 13 de la Directiva.

Principio de proporcionalidad y de calidad de los datos - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

Principio de transparencia (información en la recogida de los datos) - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2, 3 y 13 de la Directiva.

Principio de seguridad - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

Derechos de acceso, rectificación y oposición - el interesado debe tener derecho a obtener una copia de todos los datos relativos a su persona, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento sus datos personales. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

Restricciones respecto a transferencias sucesivas a otros terceros países -únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.

Además, deben aplicarse otros principios adicionales a tipos específicos de tratamiento como a los **datos sensibles, la publicidad directa** - con la posibilidad de negarse a transferencias de datos cuyo fin sea la publicidad directa, o la **decisión individual automatizada** - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

1.1.2. Objetivos de un sistema de protección de datos

Los objetivos de un sistema de protección de datos son básicamente tres:

1. Asegurar un **nivel satisfactorio de cumplimiento** de las normas. Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2. 2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello, es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3. 3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

1.1.3. Aplicación a los miembros del Convenio 108 del Consejo de Europa

El Convenio 108 es el único instrumento internacional existente con poder vinculante en el área de la protección de datos, aparte de la Directiva. La mayoría de los signatarios del Convenio también son Estados miembros de la Unión Europea (actualmente cuenta con la ratificación de los 15) o países, como Noruega e Islandia, donde en cualquier caso la Directiva es vinculante en virtud del acuerdo del Espacio Económico Europeo. Como conclusión es posible permitir la mayoría de las transferencias de datos personales a países que han ratificado el Convenio 108 al amparo del artículo 25.1 de la Directiva a condición de que el país en cuestión:

- también disponga de mecanismos adecuados para garantizar el cumplimiento, ayudar a las personas físicas y facilitar la reparación (como, por ejemplo, una autoridad de control independiente dotada de las competencias apropiadas);

- y sea el destino final de la transferencia y no un país intermediario a través del cual transitan los datos, excepto cuando las transferencias sucesivas se dirigen de nuevo a la UE o a otro destino que ofrezca una protección adecuada.

1.2. CÓDIGOS DE CONDUCTA

En este apartado se distingue entre una Doctrina General del Grupo de Trabajo, que se va plasmando a lo largo de los distintos documentos, y por otro lado la valoración, en concreto, de un proyecto de Código de Conducta de las Compañías Aéreas.
El nivel de protección de datos de un determinado país puede verse acrecentado además de por las normas de Derecho, por las normas de autorregulación profesionales y sectoriales. En este sentido, se pueden considerar los Códigos Tipo como un conjunto de normas de protección de datos aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por los miembros del sector industrial o profesional en cuestión.
1.2.1. Valor añadido del Código Tipo
Para poder evaluar la validez de un Código Tipo es necesario tener en cuenta el plus de efectividad su aprobación implica en relación con los principios fundamentales de la protección de datos que se han expuesto en el apartado referido a los criterios que deben tomarse en consideración a la hora de evaluar si un país ofrece un nivel de protección adecuada.

1.2.2. ¿Es el organismo responsable del código representativo del sector?
La fuerza ejecutiva de un código es fundamental, por lo que resultan básicos tanto el carácter representativo del organismo responsable del código en el sector, como la fuerza de la asociación en cuanto a su capacidad para imponer sanciones a sus miembros por incumplimiento del código.
Un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código de protección de datos, resulta confuso para el consumidor. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos son objeto de tratamiento.
En sectores tales como la publicidad directa pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de

ambigüedad en cuanto a la naturaleza de las normas aplicables, y también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

1.2.3. La evaluación de la autorregulación

El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos debe tener en cuenta los siguientes aspectos:
1. el examen del contenido del instrumento,
2. la evaluación de su eficacia,
3. el nivel de cumplimiento general,
4. el apoyo y la ayuda a las personas cuyos datos sean objeto de tratamiento,
5. la reparación adecuada (incluida la compensación, cuando corresponda).

1.2.4. Evaluación del contenido de un instrumento de autorregulación

Se trata de garantizar que estén presentes los "principios de protección de datos" anteriormente expuestos. Es una evaluación objetiva en la que se trata de ver cuál es el contenido del código.
En este punto, el que un sector industrial haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante, aunque si en su desarrollo se han tenido en cuenta las opiniones de las personas cuyos datos son objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje fielmente los principios básicos necesarios para la protección de datos.
La transparencia del código es un elemento crucial; en particular, el código debería redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones.
Además, el código deberá prohibir la comunicación de datos a empresas que no pertenezcan al sector y que no se rijan por aquél, a menos que se prevean otras medidas adecuadas de protección.

1.2.5. Evaluación de la eficacia de un instrumento de autorregulación

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas para garantizar la adhesión al código y para resolver los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales antes referidos de eficacia de la protección para considerar que un código de autorregulación proporciona una protección adecuada.

1.2.6. Un buen nivel de cumplimiento general

Un código profesional o industrial se desarrollará por un organismo representativo del sector industrial o profesional en cuestión, y se aplicará a los miembros de dicho organismo representativo específico. El nivel de cumplimiento del código dependerá del:
1. grado de conocimiento de la existencia del código y su contenido por parte de sus miembros,
2. de las medidas que se adopten para garantizar la transparencia del código a los consumidores con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz,
3. de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y,
4. De la naturaleza y la aplicación de las sanciones en caso de incumplimiento.
Por tanto, son importantes las siguientes preguntas:
1. ¿Qué medidas adopta el organismo representativo para asegurarse de que sus miembros conocen el código?
2. ¿Exige el organismo representativo a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
3. ¿Presentan dichas pruebas las propias empresas o proceden de una fuente exterior (tal como un auditor acreditado)?
4. ¿Investiga el organismo representativo las supuestas o presuntas violaciones del código?
5. ¿Es el cumplimiento del código una condición para formar parte del organismo representativo o es dicho cumplimiento meramente "voluntario"
6. En caso de que un miembro incumpla las disposiciones del código, ¿con qué tipo de sanciones disciplinarias cuenta el organismo representativo (expulsión u otras)?
7. ¿Es posible para una persona o empresa continuar trabajando en la profesión o sector industrial concreto después de haber sido expulsado del organismo representativo?
8. ¿Puede hacerse cumplir el código mediante otros procedimientos, por ejemplo, en los tribunales o en un tribunal especializado?

Por lo que se refiere a las sanciones cabe distinguir:
* sanciones "reparadoras" que, en caso de incumplimiento, únicamente exige al responsable del tratamiento la modificación de sus prácticas con el fin de adecuarlas a lo establecido en el código, y
* sanciones "punitivas" que tienen repercusión en el comportamiento futuro de los responsables del tratamiento al proporcionar un incentivo para que se cumpla sistemáticamente el código.
La falta de sanciones auténticamente disuasorias y punitivas es una carencia importante en un código. Sin dichas sanciones, es difícil entender cómo puede lograrse un nivel satisfactorio de cumplimiento general, a no ser que se establezca un sistema riguroso de control exterior (como una autoridad pública o privada competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

1.2.7. Apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento

Un requisito esencial para un sistema de protección de datos adecuado y eficaz consiste en el apoyo institucional a los

afectados. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:
- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Supone el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez es un punto clave. Idealmente, el árbitro debería ser ajeno a la profesión o sector en cuestión, dado que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya infringido el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

1.2.8. Reparación adecuada

Probada la infracción del código de autorregulación, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (por ejemplo, corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, prever el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico y/o moral que se cause.
Por lo tanto, podrían plantearse también las siguientes preguntas:
- ¿Es posible comprobar si un miembro que haya vulnerado el código, ha modificado después sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación en virtud del código, y en caso afirmativo, de qué manera?
- ¿Equivale la vulneración del código a una ruptura de contrato, o es susceptible de sanción en virtud del Derecho público (por ejemplo, protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

1.2.9. Recomendación 1/98 sobre los sistemas informatizados de reserva de las líneas aéreas (SIR) (XV D/5009/98 final WP 10).

Los destinatarios de esta recomendación son la Comisión Europea, el Parlamento Europeo, el Consejo de la Unión Europea y el Comité Económico, en relación con una Propuesta de Reglamento (CE) del Consejo por el que se modifica el Reglamento (CEE) nº 2299/89 del Consejo relativo a un código de conducta para los sistemas informatizados de reserva (SIR)1.
Habida cuenta de las características específicas de las reservas en líneas aéreas, y de las recientes iniciativas de la Comisión a este respecto, el Grupo de Trabajo decidió crear un subgrupo para el estudio de los sistemas informatizados de reserva (SIR). El subgrupo se reunió en dos ocasiones y decidió someter los resultados de sus debates al Grupo de Trabajo con vistas a la adopción de la presente recomendación.
El sector del transporte aéreo se caracteriza por un uso muy desarrollado de los sistemas informáticos. Existen bases de datos que contienen datos personales en muchos contextos, y en particular en las compañías aéreas, las agencias de viajes y los sistemas informatizados de reserva. Algunas de las bases de datos (en especial, aunque no de forma exclusiva, las de los SIR) están ubicadas fuera de la Comunidad.
Dado el carácter internacional de la transporte aéreo, las soluciones de tipo general son, en principio, las más adecuadas. Considerando lo anterior, el Grupo de Trabajo recomienda sobre la propuesta de Reglamento por el que se modifica el Reglamento 2299/89 del Consejo, relativo a un código de conducta para los sistemas informatizados de reserva, que se complete con las siguientes disposiciones:
– Una obligación clara de facilitar información al consumidor acerca del tratamiento de datos personales en el SIR. Esta información, que podría facilitarse (por ejemplo, mediante folletos estándar), debería incluir la denominación y dirección del vendedor del sistema, la finalidad del tratamiento, el plazo de conservación y los procedimientos por los cuales el interesado puede ejercer el derecho de acceso a los datos.
– La obligación para los abonados (p.ej., las agencias de viajes) y las compañías aéreas de obtener el consentimiento expreso de los interesados para recoger datos sensibles (pasajeros minusválidos, comidas aptas para musulmanes, etc.). Si el SIR incluye un sistema de expedición directa de billetes, el vendedor del sistema debería quedar sujeto a tal obligación.
– La obligación para las partes antes mencionadas de responder rápidamente a una solicitud de **acceso** presentada por un pasajero que desea ver sus propios datos.
– La exigencia para los SIR de que todos los datos personales obtenidos se archiven fuera de línea en un plazo no superior a 72 horas tras la conclusión del viaje y se destruyan en un plazo máximo de 3 años. El acceso a tales datos únicamente debe autorizarse a efectos de la resolución de litigios en materia de facturación. No obstante la obligación de destruir los datos en el plazo de 3 años, los datos personales podrán conservarse durante el tiempo que resulte necesario para zanjar una demanda de daños y perjuicios o para dar cumplimiento a un requisito legal (p.ej., normas contables y fiscales).
– La exigencia de que se efectúen las modificaciones oportunas para ampliar el ámbito de aplicación de la auditoría prevista en el artículo 21 bis.
– Que se estudien, además, con carácter prioritario los problemas específicos planteados por las reservas en línea efectuadas al margen de los SIR (p.ej., agencias de viajes o compañías aéreas que expiden directamente billetes por Internet) y que la Comisión proponga sin demora soluciones adecuadas. A este respecto, se invita a la Comisión a precisar si la Directiva 97/66/CE es aplicable a este extremo y en qué medida.

1.3. LAS CLÁUSULAS CONTRACTUALES COMO MEDIO PARA GARANTIZAR UN NIVEL DE LA PROTECCIÓN ADECUADO DE EN LAS TRANSFERENCIAS INTERNACIONALES A TERCEROS PAÍSES

En el contexto de las transferencias a terceros países, el contrato es un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Comunidad (y, por tanto, fuera del ámbito de aplicación de la Directiva y, de hecho, del marco general del Derecho comunitario), a un país en que el nivel general de protección no sea suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección general adecuada mediante inclusión de los elementos esenciales de la misma que no existen en una situación determinada.
En la Comunidad se utilizan contratos para determinar el reparto de responsabilidades en materia de protección de datos entre el responsable del tratamiento y el subcontratista encargado de llevarlo a cabo. Cuando se utilice un contrato en relación con transferencias de datos a terceros países, éste debe abarcar mucho más: ha de ofrecer a la persona a la que se refieran los datos salvaguardas adicionales, puesto que el receptor establecido en el tercer país no está sujeto a una serie de normas obligatorias que garanticen un nivel de protección adecuado. Para ello se deberán tener en consideración los siguientes extremos:
1. Idoneidad: Para evaluar la idoneidad de las salvaguardas ofrecidas por una solución contractual debe partirse de la misma base que para evaluar el nivel general de protección en un tercer país. Una solución contractual debe contener todos los principios básicos para la protección de datos y ofrecer los medios necesarios para que pueda velarse por su observancia.
2. Contenido del contrato: El contrato debe fijar minuciosamente la finalidad, los medios y las condiciones del tratamiento de los datos transferidos, así como la forma en que se aplicarán los principios básicos de protección de datos. Los contratos que limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma ofrecen una mayor seguridad jurídica. Por consiguiente, en la medida de lo posible, el contrato debería servir para atribuir al remitente de los datos el poder decisorio sobre el tratamiento efectuado en el tercer país.
3. Reparto de responsabilidades entre el responsable y el encargado del tratamiento: De acuerdo con la Directiva, una entidad, el "responsable del tratamiento", debe asumir la responsabilidad principal del cumplimiento de los principios sustantivos de protección de datos. La segunda entidad, el "encargado del tratamiento", sólo es responsable de la seguridad de los datos. Una entidad se considera responsable del tratamiento si está capacitada para decidir sobre la finalidad y los medios del mismo, en tanto que el encargado del tratamiento es simplemente el organismo que presta materialmente el correspondiente servicio. La relación entre ambos se rige por lo dispuesto en el artículo 17.3 de la Directiva, en el que se establece que la realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular, que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento y que las obligaciones del apartado 1 (las normas sustantivas sobre seguridad de los datos), tal como las define la legislación del Estado miembro en el que esté establecido el responsable, incumben también a éste.
Se desarrolla así el principio general enunciado en el artículo 16, con arreglo al cual toda persona que esté bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, deberá abstenerse de procesar datos personales salvo cuando reciba instrucciones del responsable (o cuando lo exija la ley).
En caso de transferencia de datos a terceros países, también intervendrá, en general, más de una entidad. En este caso, se establece una relación entre la entidad que transfiere los datos (el "remitente") y la que los recibe en el otro país (el "receptor").
En tal contexto, una de las finalidades del contrato debe seguir siendo la de determinar el reparto de responsabilidades entre ambas partes en lo que atañe a la protección de datos. No obstante, el contrato no debe limitarse a este aspecto, sino que ha de ofrecer garantías adicionales para los interesados, por el hecho de que el receptor del país no comunitario no está sujeto a una serie de normas obligatorias de protección de datos que proporcionen garantías adecuadas.
4. Grado de autonomía del receptor: Si el receptor disfruta de cierta autonomía en relación con el tratamiento de los datos transferidos, la situación es más compleja y es posible que un simple contrato entre las partes de la transferencia no siempre permita a las personas a las que se refieren los datos ejercer sus derechos. Puede resultar necesario un mecanismo por el cual el remitente establecido en la Comunidad conserve la responsabilidad por los daños que pudieran derivarse del tratamiento llevado a cabo en el tercer país.
5. Prohibición de cesión a terceros: El contrato debería excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente por el receptor a organismos u organizaciones no vinculados por el contrato, a menos que pueda obligarse a terceros, mediante disposiciones contractuales, a respetar los mismos principios de protección de datos.
6. Verificación externa del cumplimiento: La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación.
7. Reclamaciones del afectado: En el supuesto de que la persona a la que se refieren los datos se encuentre con algún problema, como consecuencia, en su caso, del incumplimiento de las cláusulas sobre protección de datos contenidas en el contrato, resulta, en general, difícil asegurarse de que la queja del interesado se investiga convenientemente. Las autoridades supervisoras de los Estados miembros experimentarán dificultades de orden práctico a la hora de llevar a cabo tales indagaciones.
8. Carácter apropiado de las soluciones contractuales: Las soluciones contractuales resultan probablemente más adecuadas para las grandes redes internacionales (tarjetas de crédito, reservas de billetes de avión), que se caracterizan por un elevado volumen de transferencias repetitivas de datos similares y, y por la existencia de un número relativamente reducido de grandes empresas que operan en sectores ya sujetos a supervisión y regulación públicas. Otro caso en el que la utilización de contratos presenta un potencial considerable es el de las transferencias de datos entre distintas sucursales o empresas del mismo grupo.
9. Exclusión de países que no garantizan los derechos humanos: Los países en los que las prerrogativas con las que

cuentan los poderes públicos para acceder a la información son más amplias de lo que autorizan las normas sobre protección de los derechos humanos aceptadas en el ámbito internacional, no constituyen un destino seguro para las transferencias basadas en cláusulas contractuales.

2. CONSEJO DE EUROPA

En 1981 se firmó el Convenio 108 para la protección de los individuos en relación con el tratamiento automatizado de datos. Este Convenio establece el libre flujo de datos personales entre los Estados que son parte del mismo, flujo que sólo puede impedirse en los supuestos en que las Partes dejen de ser parte del Convenio, o en el caso de que la protección datos en el país en cuestión no sea equivalente, o si los datos se transfieren a un tercer Estado no miembro.

El Convenio establece un Comité Consultivo (T-PD) que se compone de los representantes de los Estados que son parte en el Convenio y que es el encargado de la interpretación de las normas, así como de cerciorarse del cumplimiento del mismo. Este Comité estudió el tema de las cláusulas contractuales como instrumento para facilitar las transferencias internacionales entre los Estados Parte y los que no son Parte, junto con la Unión Europea y la Cámara Internacional de Comercio

Desde 1981 la sociedad se ha automatizado del tal modo que en la actualidad el ordenador es un instrumento muy extendido que permite tanto a un individuo como a una organización el tratamiento de los datos. En este contexto, el individuo se convierte en un agente activo de la sociedad de la información, mientras que por otra parte, su privacidad se ve sometida a un número de interferencias cada vez mayores por los numerosos sistemas de información tanto públicos como privados.

Los principios del Convenio deben adaptarse e interpretarse en función de los diferentes sectores implicados. El Consejo de Europa ha preferido, a este respecto, la utilización de las Recomendaciones como instrumento legal para este fin, dado que su procedimiento de adopción es mucho más sencillo y se adaptan mejor a las circunstancias cambiantes de la protección de datos, a pesar de carecer de obligatoriedad son una referencia obligada para los Estados.

Con el fin de elaborar estas recomendaciones el Comité de Ministros creó en 1976 un Comité de Expertos sobre protección de datos, que se convirtió después en el Grupo de Proyectos sobre protección de datos (CJ-PD). Este Comité se compone de expertos de los 40 Estados Miembros responsables de la protección de datos en sus respectivos países.
Durante estos años el CJ-PD no sólo ha creado una serie de Recomendaciones, sino que también ha publicado estudios sobre temas específicos en el ámbito de la protección de datos. La Agencia de Protección de Datos española forma parte de este Comité, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

A lo largo de 1998 se ha trabajado en una Recomendación sobre la Vida Privada en Internet, que finalmente ha sido adoptada por el Comité de Ministros en febrero de 1999. A lo largo de 1999 está previsto que el CJ-PD que se continúe con el estudio de una recomendación de datos de carácter personal recogidos y procesados para los seguros y sobre una recomendación sobre servicios financieros. También se estudiarán los datos para los usos policiales para evaluar los nuevos desarrollos en este ámbito. Por otra parte, se abordará la incorporación las directrices sobre Internet con vistas a su integración en Códigos Tipo. Por último, se prevé continuar los trabajos ya iniciados sobre las tarjetas inteligentes y la vigilancia electrónica.

En el Anexo de la Memoria de 1998 se incluye la Recomendación R (97) 18 y Exposición de Motivos del Comité de Ministros a los Estados Miembros relativa a la protección de datos de carácter personal, recogidos y tratados con fines estadísticos. Esta Recomendación no se incluyó en la Memoria de 1997 por no estar traducida al castellano.

La Recomendación sobre la Vida Privada en Internet se va a comentar en el apartado siguiente relativo al fenómeno Internet, que dada su importancia merece un tratamiento conjunto con las actuaciones en el ámbito de la Unión Europea, y separado del resto de los temas.

3. EL FENÓMENO INTERNET.

La globalización de la sociedad de la información gracias en gran medida al fenómeno Internet, ha concienciado a todos los organismos internacionales con competencias en la materia, sobre la necesidad de establecer una serie de normas tendentes a obtener una regulación uniforme de sus efectos jurídicos. No obstante, estos esfuerzos para efectuar una regulación derivada de la naturaleza de los derechos que pueden resultar afectados topan con 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 la territorialidad de las leyes, produciendo un casi absoluto vacío legal.

Todas las actuaciones llevadas a cabo por los Estados y expresadas en los foros internacionales llevan a tres conclusiones fundamentales a la hora de abordar la regulación de Internet:

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 autorregulaciones 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 de que son muchos los sectores implicados, 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.

Se van a analizar por su especial importancia la Propuesta de la Comisión de un Plan plurianual de acción comunitaria para fomentar la seguridad en la utilización de Internet y el Dictamen del Grupo del Artículo 29 1/98 sobre Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS) y la Recomendación sobre la Vida Privada en Internet del Consejo de Europa.

3.1. PROPUESTA DE LA COMISIÓN DE UN PLAN PLURIANUAL DE ACCIÓN COMUNITARIA PARA FOMENTAR LA SEGURIDAD EN LA UTILIZACIÓN DE INTERNET

Es necesario 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 Europea2 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 ella 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 (Plataform 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.

3.2. DICTAMEN DEL GRUPO DEL ARTÍCULO 29 1/98 SOBRE PLATAFORMA DE PREFERENCIAS DE PRIVACIDAD (P3P) Y NORMA DE PERFILES ABIERTA (OPS) 3

El Consorcio World Wide Web ha querido poner a punto un vocabulario único a través del cual se puedan articular las preferencias del usuario y las prácticas del sitio Internet. El Proyecto de Plataforma de Preferencias de Privacidad (P3P por Platform for Privacy Preferences) concibe la privacidad informática y la protección de datos como algo que debe ser objeto de un acuerdo entre el usuario de Internet cuyos datos se recaban y el sitio Internet que registra dichos datos.
La filosofía parte de la idea de que el usuario da su consentimiento para que un sitio Internet registre sus datos personales (el objetivo de la Norma de Perfiles Abierta -conocida por su sigla en inglés OPS por Open Profiling Standard- es garantizar la transmisión segura de un perfil normalizado de datos personales), a condición de que las prácticas en materia de privacidad informática declaradas por el sitio como, por ejemplo, el propósito para el cual se registran los datos y si estos datos se utilizan o no para fines secundarios o se ceden a terceros, satisfagan las exigencias del usuario.
Estas decisiones en materia de política informática hacen prever que la puesta en práctica de la P3P y de la OPS en la Unión Europea dará lugar a una serie de problemas concretos que se abordan a continuación:

* Una plataforma técnica para la protección de la intimidad no bastará por sí sola para proteger la intimidad personal en la Red. Es necesario aplicarla en un contexto de normas de protección de datos que sean ejecutables y deparen a todas las personas un nivel mínimo y no negociable de protección de la intimidad. Esta concepción presenta el riesgo de pasar la responsabilidad de protegerse del 'controlador de datos al usuario. Tal inversión de responsabilidades también presupone un nivel de conocimientos sobre los riesgos que el tratamiento de datos entraña para la intimidad de las personas, algo que no resulta realista esperar de la mayoría de los ciudadanos.
* ?Existe el riesgo de que la P3P, una vez puesta en práctica en la próxima generación de software de navegación, pueda llevar a los operadores radicados en la UE a creer erróneamente que podrían quedar eximidos de algunas de sus obligaciones legales y podría causar confusión no sólo entre los operadores en cuanto a sus obligaciones, sino también entre los usuarios de Internet en cuanto a la naturaleza de sus derechos de protección de datos.
* Para los usuarios radicados en la UE que entren en contacto con sitios Internet establecidos en países extracomunita-

rios, la preocupación principal es que la organización a la que comunican sus datos personales no esté sujeta a la directiva europea o a ninguna normativa de protección de datos efectivamente aplicada
* ?Dada la escasa probabilidad de que la mayoría de los usuarios de Internet modifiquen los parámetros preconfigurados de su navegador, la posición "por defecto" sobre las preferencias de privacidad de un usuario tendrá una enorme incidencia en el nivel general de protección de la intimidad en línea.
* La P3P y las OPS deben integrarse en la tecnología de navegación con posiciones por defecto que reflejen el interés del usuario por disfrutar de un nivel elevado de protección de su intimidad (incluida la capacidad de navegar por los sitios de la Red de forma anónima) sin verse bloqueado o sufrir molestias por su intento de acceder a los sitios.
* Cuando un operador exija que se le facilite un perfil de datos identificables como condición para acceder a su sitio Internet, habrá que pedir cada vez el consentimiento del usuario para proporcionar dicha información al sitio en cuestión. Cuando el sitio no requiera tal información, el acceso puede efectuarse sin solución de continuidad. Los principales fabricantes de software de navegación tienen la responsabilidad de aplicar la P3P y las OPS de forma que aumenten en lugar de disminuir los niveles de protección de la intimidad.
* El Grupo de Trabajo anima a que se desarrolle un software de Internet que se ajuste a las normas en materia de protección de datos aplicables en la Unión Europea, y considera que sería apropiado poner a punto los mecanismos que permitan verificar la conformidad del software de Internet a este respecto. A finales de 1998 el Grupo elaboró borrador de recomendación sobre el tratamiento automático e invisible en Internet, que previsiblemente se aprobará a comienzos de 1999.

3.3. EL PROYECTO DE RECOMENDACIÓN DE LA VIDA PRIVADA EN INTERNET DEL CONSEJO DE EUROPA

Por lo que se refiere al proyecto de Recomendación de la Vida Privada en Internet, 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 los datos que revelan la personalidad e incluso las inclinaciones íntimas del afectado.
* 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 la dirección de correo electrónico es un dato de carácter personal.
* Evitar que se soliciten muchos datos de carácter personal.
* Exigir información acerca de qué datos personales son conservados por el suministrador de servicios o por un tercero en Internet: modificarlos si son inexactos o hacerlos suprimir si son excesivos o están desfasados.
* No enviar correos malintencionados, ya que pueden volverse contra el remitente, con consecuencias jurídicas adversas.
* Recordar que la dirección de correo electrónico u otros datos de carácter personal pueden ser incluidos en guías o anuarios.

Para los suministradores de servicios de Internet se establecen, entre otros, las siguientes recomendaciones:

* 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) Desarrollo y puesta en marcha en el mercado sus propios servicios si el usuario ha dado su consentimiento explícito a que sus datos sean utilizados con fines de marketing.
* Se recomienda no 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 superior a 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 la página en cuestión, 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 cuánto 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) respetar el deseo de los usuarios, tanto de los que 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 el cifrado (técnicas criptográficas) 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 establezcan las salvaguardas oportunas.

1 COM (97) 246 final de 9 de julio de 1997
2 (véase Diario Oficial de las Comunidades Europeas 13 de febrero de 1998)
3 Adoptado por el Grupo de Trabajo el 16 de junio de 1998 (XV D/5032/98 WP 11).

4. SISTEMA DE INFORMACIÓN SCHENGEN

El objetivo del Convenio de Aplicación del Acuerdo de Schengen es permitir la supresión de los controles en las fronteras comunes en la circulación de personas entre los Estados miembros (en la actualidad Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos y Portugal), manteniendo en el interior del territorio Schengen creado un nivel de seguridad al menos igual al que ya existía. Entre las medidas compensatorias previstas en el Convenio que persiguen este objetivo, se encuentran la armonización de la política en materia de expedición de visados, una política común en materia de determinación del Estado responsable del examen de la solicitud de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico ilegal de estupefacientes, la armonización del nivel de control de las fronteras exteriores del territorio Schengen y la creación del Sistema de Información Schengen (SIS).
El principal objeto del SIS es, con la ayuda de la información que se transmite en el sistema, preservar el orden y la seguridad públicos, incluida la seguridad del Estado, así como la aplicación de las disposiciones previstas en el Convenio relativas a la circulación de personas en los territorios de los países que conforman el territorio Schengen. El SIS consta de una parte nacional (NSIS) en cada uno de los países que aplican el Convenio y de una unidad de apoyo técnico central ubicada en Estrasburgo (CSIS), estableciéndose de esta forma una conexión entre todos los Estados miembros que permite a los usuarios del sistema la posibilidad de disponer en tiempo real de la información necesaria para sus misiones. Esta información está disponible al efectuar controles en la frontera, así como cuando se realizan otros controles de policía y de aduanas; en el caso de los extranjeros, la información está disponible a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de aquéllos en el marco de la aplicación de las disposiciones sobre la circulación de personas.
En el Capítulo Tercero del Título IV del Convenio se establecen los principios y mecanismos destinados a garantizar

una adecuada protección de los datos de carácter personal 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 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 de Protección de Datos, encomienda a ésta el ejercicio del control aquí mencionado.
Por otra parte, el artículo 115 del Convenio establece la creación de una Autoridad de Control Común (ACC) encargada del control de la unidad de apoyo técnico del SIS; esta autoridad está compuesta por dos representantes de cada autoridad nacional de control. También el artículo 10 del Real Decreto mencionado establece que el Director de la Agencia designará a los dos representantes que formarán parte de la Autoridad de Control Común.
Durante el año 1998 la ACC ha celebrado siete reuniones plenarias, seis de ellas en Bruselas y una en Lisboa, así como reuniones técnicas para la preparación de una inspección de control que se va a realizar en la unidad de apoyo técnico central ubicada en Estrasburgo durante el año 1999 y para analizar un estudio preliminar que se está confeccionando y que define los requisitos del nuevo Sistema de Información Schengen (SIS II). A continuación se presentan los aspectos más relevantes relativos al SIS español, a los temas tratados en las reuniones de la ACC y a las repercusiones que han tenido en el trabajo desempeñado por esta Agencia las decisiones tomadas por la ACC.

4.1. DATOS INTRODUCIDOS POR LAS AUTORIDADES ESPAÑOLAS

El SIS incluye exclusivamente las categorías de datos que proporciona cada uno de los Estados miembros y que son necesarios para los fines previstos en el Convenio. Las categorías de datos introducidos corresponden a personas descritas, vehículos (cilindrada superior a 50 c.c. o remolques y caravanas de peso en vacío superior a 750 Kg. que hayan sido robados, sustraídos u ocultados fraudulentamente) y objetos (armas de fuego, documentos vírgenes y documentos de identidad expedidos que hayan sido robados, sustraídos u ocultados fraudulentamente, así como billetes de banco registrados). En el caso de las personas descritas se distinguen entre otros los siguientes fines por los que dichos datos pueden ser introducidos por las autoridades competentes: personas buscadas para su detención a efectos de extradición, extranjeros incluidos en las listas de no admisibles, datos de personas desaparecidas o que deban ser puestas a salvo provisionalmente (otorgarles protección, prevención de amenazas, menores de edad), datos de testigos o de personas que deban comparecer ante las autoridades judiciales.
Según los datos disponibles a fecha de 1/1/99, las autoridades españolas habían introducido en el SIS los datos de 20.085 personas, lo cual representaba el 2'53% del total de datos que se habían introducido relativos a personas. Los datos de estas personas se distribuían por finalidad de la siguiente forma: 489 (detención a efectos de extradición), 13.283 (no admisibles), 3951 adultos y 2.191 menores de edad (desaparecidos o que deban ser puestos a salvo provisionalmente), 150 (testigos y personas que deban comparecer ante las autoridades judiciales) y 17 (otras categorías).

4.2. INSPECCIÓN DE LAS OFICINAS SIRENE

Como consecuencia de una fuga de información y documentos que se produjo en la Oficina SIRENE belga (unidad encargada de gestionar los intercambios complementarios de información entre los diferentes países), la ACC decidió con fecha de 12 de diciembre de 1997 proceder a una verificación de las medidas de seguridad existentes en cada una de las Oficinas SIRENE de cada uno de los países que aplicaban el Convenio, por lo que encomendó dicha revisión a cada una de las Autoridades Nacionales de Control1.
Durante el año 1998 cada una de las Autoridades procedió a efectuar los diferentes controles sobre las Oficinas SIRENE, elaborándose los respectivos informes que recogían el resultado de los trabajos realizados. La ACC elaboró un documento síntesis en el que se recogían diferentes recomendaciones cuya implantación mejoraría el nivel de seguridad de las Oficinas SIRENE y que debían adoptarse en los casos en que todavía no se estuvieran aplicando. De las recomendaciones emitidas cabe destacar: el mantenimiento de la seguridad física a su máximo nivel; la creación de un sistema de auditoría de las operaciones que se efectuaran sobre las bases de datos y la explotación regular de los ficheros de trazado resultantes para la detección de anomalías; limitar y controlar el acceso a los archivos manuales de los expedientes; reforzar las medidas de control de acceso lógico a la información verificando regularmente los motivos por los que se realizan las consultas; designar a un responsable de seguridad y definir normas de seguridad comunes a las diferentes Oficinas SIRENE de aplicación a su personal; impedir la generación de impresiones de pantalla conteniendo información de las bases de datos; fomentar la organización de cursos de formación para los usuarios de las Oficinas SIRENE centrados en la seguridad de la información; la elaboración periódica de informes relativos al estado de la seguridad de los NSIS y de las Oficinas SIRENE.
De estas recomendaciones, así como de las propias que elaboró esta Agencia, se dio traslado al Ministerio del Interior, entendiendo que muchas de las medidas técnicas propuestas por la ACC ya se estaban aplicando en la Oficina SIRENE española.

4.3. CAMPAÑA DE INFORMACIÓN

En el año 1997 la ACC decidió lanzar una campaña que informara a los ciudadanos de la existencia del SIS y de la posibilidad que tienen de ejercer los derechos que el Convenio les reconoce, teniendo en cuenta que se había constatado que el ejercicio de esos derechos era muy reducido. Estos derechos son básicamente el de acceso a la información registrada en el SIS, el de rectificación en caso de que los datos se hayan registrado basándose en un error de hecho o de derecho, el de emprender una acción ante los Tribunales o las instancias competentes para obtener la rectificación o supresión de la información errónea o una indemnización y del de solicitar la comprobación de los datos registrados y la utilización que de ellos se hace.
Con el fin de que la campaña pudiera llevarse a cabo en todo el territorio Schengen, la ACC elaboró, con cargo a su presupuesto, unos modelos de cartel y de folletos explicativos dirigidos al público en general con el fin de que pudieran ser posteriormente impresos y distribuidos en cada uno de los países. Para su consecución solicitó la colaboración de las Autoridades Nacionales de Control, de las instancias Schengen y de las autoridades competentes de los Estados.
Esta Agencia consideró que era 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, por lo que procedió a la edición de los folletos y los carteles, contratando dicho trabajo a una empresa externa. El número de carteles y folletos que se imprimieron fue de 400 y 50.000 respectivamente. Para la distribución de los carteles se solicitó la colaboración del Ministerio de Asuntos Exteriores y del Ministerio del Interior, con el fin de que fueran difundidos en las oficinas consulares y en los puestos fronterizos exteriores (aéreos, marítimos o terrestres) del territorio Schengen.
A finales del año 1998 dicha campaña sólo se había iniciado en los países de Alemania, Grecia y Portugal, además de España, comprobándose que en algunos casos se había producido un incremento en el número de solicitudes que realizaban los ciudadanos en el ejercicio de los derechos que el Convenio les reconoce.

4.4. INSPECCIÓN DEL CSIS

Durante el año 1998 la ACC decidió formar un grupo de trabajo, en el que participó la delegación española, encargado de definir la lista de controles que debían verificarse en una próxima inspección que se realizaría en la unidad de apoyo técnico central (CSIS) durante el año 1999. La realización de este control se justificaba debido al tiempo que había transcurrido desde que se efectuó el último (octubre de 1996) y a que en el año 1998 se habían incorporado tres nuevos países: Austria, Grecia e Italia.
Durante ese año este grupo de trabajo se reunió en diferentes ocasiones y se discutieron dos notas elaboradas por la delegación española en la que se presentaban los controles a efectuar. En la primera de ellas se detallaba el plan de trabajo a seguir para analizar las medidas de seguridad implantadas en el CSIS y con ello el cumplimiento del artículo 118.1 del Convenio de Schengen. Además, este plan podrá ser aprovechado por cada Autoridad Nacional de Control en las revisiones que realicen en los NSIS y en las Oficinas SIRENE, con el fin de homogeneizar los resultados de esos trabajos en todos los países. La segunda nota definía un plan de trabajo para verificar el cumplimiento de las medidas específicas contenidas en el Convenio y que no están relacionadas directamente con medidas de seguridad.
Aprobadas ambas notas en el seno del grupo de control se presentaron a la ACC y ésta decidió su fusión en un solo documento; este documento constituye una base de referencia para las futuras revisiones que se vayan a realizar en el CSIS y para las que efectúen las autoridades nacionales de control de sus sistemas de información Schengen nacionales.

4.5. PRESUPUESTO PROPIO DE LA ACC

La asignación de una dotación presupuestaria propia y suficiente para la ACC es una de las peticiones que ha reiterado esta Autoridad desde su establecimiento, entendiendo que dicha asignación es imprescindible para la eficiencia de su actividad y para el ejercicio de sus competencias de una forma independiente. Otras consideraciones que apoyan esta petición son que el personal de apoyo de la Secretaría de Schengen con el que se cuenta es simplemente una persona a tiempo parcial, que el presupuesto asignado a la ACC para 1998 fue el 0'012% del presupuesto global de Schengen y que esta autoridad está compuesta de representantes de autoridades nacionales independientes cuyas dotaciones presupuestarias son también reducidas. Hasta la fecha la ACC no ha recibido de los organismos ejecutivos (constituidos por representantes de los diferentes países que aplican el Convenio) una respuesta positiva a su petición, lo cual es considerado por esta autoridad como una forma de limitar su independencia en el ejercicio de sus funciones.

4.6. FUTURO DE LA ACC Y DEL SIS

Durante el año 1999 entrará en vigor el Tratado de Amsterdam, con lo que el marco institucional del funcionamiento de Schengen quedará modificado, debatiéndose todavía en el seno de la Unión los cambios en el funcionamiento de los sistemas de información policiales y de su respectivo control independiente. En este sentido, la ACC considera que la integración del SIS en la estructura comunitaria debe ir acompañada de la continuidad del control independiente de la ACC y que por ello su actividad no debe verse afectada por dicha integración.
El SIS y principalmente su unidad de apoyo técnico central (CSIS) también sufrirá modificaciones durante el año 1999, en concreto, se pretende que a primeros del año 2000 entre en funcionamiento un nuevo sistema (SIS1+), que resolverá los problemas planteados por el efecto 2000 y la integración de los países nórdicos, así como las deficiencias de administración y operación que presenta el actual sistema.
Hay que esperar también que durante el año 1999 se presenten las bases de lo que será la futura generación del SIS (SIS II), el cual entrará en funcionamiento previsiblemente en un plazo de unos cuatro o cinco años. Este sistema resolverá los problemas de la actual arquitectura en estrella del SIS que no se han podido acometer con la puesta en funcionamiento del SIS1+ y que presumiblemente se verán agravados con la incorporación de nuevos países a dicho sistema de información.

1 Véase él apartado de "Fuerzas y Cuerpos de Seguridad" en el Capítulo de "Inspección de Datos" de esta memoria.

5. EUROPOL

En el año 1998 se ha continuado en el seno de este grupo la discusión y negociación del Reglamento Interno de la Autoridad Común de Control (ACC-Europol) establecida por el Convenio Europol, habiéndose llegado a un texto que contaba con el consenso general en la reunión mantenida el día 8 de septiembre en Bruselas. Esta reunión la podemos calificar como "mixta", puesto que fue convocada desde el seno del Grupo de Trabajo pero a ella asistieron ya los miembros que habían sido designados informalmente como representantes de las Autoridades Nacionales de Control en la ACC-Europol.
Con carácter previo a esta reunión, se habían celebrado otras tres los días 20 de enero, 11 de febrero y 10 y 11 de junio de 1998, todas ellas con objeto de cerrar un texto aceptable para todas las partes, centrándose las discusiones, como ya se explicó en la Memoria del año anterior, en la forma de abordar los distintos puntos de vista existentes respecto de la naturaleza del Comité de Recursos y de las garantías de independencia y de las capacidades de sus miembros.
Como resultado del proceso de negociación y de la mediación del Grupo de Redacción del borrador del Reglamento Interno, compuesto por los representantes de Alemania, Irlanda y Países Bajos, se fueron aproximando posturas y se

llegó a una solución de compromiso que permitió la aprobación del texto. En dicha solución no se especifica la naturaleza del Comité de Recursos ni como órgano jurisdiccional ni como órgano administrativo, pero se introducen toda una serie de garantías en el procedimiento por el que se regirá dicho Comité que lo hacen aceptable para aquellas delegaciones que planteaban problemas constitucionales respecto al mismo.

En el año 1998, pues, ha tenido lugar la constitución de la Autoridad Común de Control (ACC-Europol) que establece en su artículo 24 el Convenio Europol (Ver anexo). La misión que a dicha Autoridad encomienda el Convenio es la de revisar las actividades de Europol para garantizar que los derechos de las personas en relación con el almacenamiento y tratamiento de los datos personales que dicha institución realice.

Esta Autoridad está constituida por un número máximo de dos representantes de cada Autoridad Nacional de Protección de Datos. Esta autoridad, en el caso español, es la Agencia de Protección de Datos, habiendo sido designada como tal, a los efectos previstos en el artículo 23 del Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una Oficina Europea de Policía (Convenio Europol), por Acuerdo del Consejo de Ministros de fecha 25 de septiembre, en el que se establece que el Ministerio de Asuntos Exteriores notificará esta designación al Secretario General del Consejo de la Unión Europea en cuanto depositario del Convenio Europol. La Autoridad Común de Control puede establecer en su seno diversos comités. De hecho, el Convenio establece también en su artículo 24 la existencia de un Comité de Recursos, que tendrá como misión conocer de las reclamaciones respecto de la denegación de los derechos de acceso, rectificación y cancelación a los ficheros de Europol.

La ACC-Europol se reunió dos veces a lo largo de 1998. La primera, el día 9 de octubre de 1998 en Bruselas. En dicha reunión se procedió a la aprobación provisional (deberá ser ratificado por el Consejo de la Unión Europea) y por unanimidad del Reglamento Interno de la ACC-Europol. Este texto se había venido negociando en el seno del Grupo de Trabajo sobre Ficheros Policiales a lo largo de los años 1997 y 1998, según se mencionó en la Memoria correspondiente a 1997.

En esta primera reunión se decidió comenzar a aplicar el Reglamento con carácter provisional, haciéndose cargo de la Presidencia de la ACC- Europol el miembro de mayor edad de la misma, M. René Faber, representante de Luxemburgo.

Posteriormente, el Presidente convocó la próxima reunión en la que se procedería a elegir al Presidente y Vicepresidente de la ACC-Europol y del Comité de Recursos.

Esta segunda reunión tuvo lugar en La Haya, el día 23 de noviembre de 1998. En ella, aparte de realizar determinadas precisiones respecto de la interpretación de algunos puntos del Reglamento que habían sido solicitadas por el Consejo de la Unión Europea, se procedió a la elección de Presidente y Vicepresidente de la ACC, siendo votados para ambos cargos Mr. Fergus Glavey, representante de la Autoridad Nacional de Irlanda y Mr. René Faber, representante de la Autoridad Nacional de Luxemburgo.

Por lo que respecta a la elección de Presidente y Vicepresidente del Comité de Recursos, fueron elegidos Mr. Peter Huxtinx, representante de la Autoridad Nacional de los Países Bajos y Mr. Mário Manuel Varges Gomes, representante de la Autoridad Nacional de Portugal.

Está previsto que la ACC-Europol mantenga una nueva reunión en el primer trimestre de 1999, una vez que se hayan ratificado en todos los Estados parte del Convenio Europol todos aquellos protocolos relativos al personal de Europol necesarios para la puesta en marcha de dicha institución. En la agenda de dicha reunión figurará, entre otros puntos, la elaboración de un dictamen de la ACC-Europol sobre el documento preparado por el Consejo de Administración de Europol sobre transferencia de información desde Europol a terceros países.
Una vez finalizada la elaboración del Reglamento Interno de Europol, está previsto que el Grupo de Trabajo sobre Ficheros Policiales pueda recobrar su funcionamiento habitual, caracterizado por el estudio de diversos temas relacionados con la protección de datos personales en el tratamiento de los mismos en la investigación policial y la toma de postura respecto de aquellas iniciativas que se produzcan en este campo. Por ello, está planificada la celebración de una reunión del Grupo en el mes de enero de 1999.

6. PARTICIPACIÓN EN OTROS GRUPOS DE TRABAJO DE ÁMBITO INTERNACIONAL.

6.1. Grupo de protección de datos en telecomunicaciones iwg (international working group on data protection in telecommunications.)

En 1998 ha habido dos reuniones del grupo de trabajo de protección de datos en telecomunicaciones, celebrándose la de primavera en Hong Kong y la de otoño en Berlín. En ambas reuniones se han producido nuevas incorporaciones de delegaciones de países del sudeste asiático y del este europeo. De la incorporación de los nuevos países se desprende el interés con que es seguido el desarrollo normativo que ha tenido lugar en la UE respecto de la protección de datos en general y de la directiva 95/46 en particular, cuya transposición tenía como fecha límite octubre de 1998.

La reunión de Hong Kong fue especialmente fructífera al aprobarse cuatro posiciones comunes (Ver anexo) y que fueron presentadas a la reunión de Autoridades de Protección de Datos celebrada en Santiago de Compostela también en 1998. La reunión sirvió también de colofón para el primer foro sobre privacidad y protección de datos en los países de Asia y del Pacífico celebrado en los días previos también en Hong Kong.

En la reunión de Berlín se realizó un seguimiento de la transposición que en cada país de la UE se ha realizado de la

Directiva 97/66, relativa a la protección de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. También se ha realizado un seguimiento del estado actual, en cada uno de los diferentes países, sobre legislaciones específicas de diversos temas, entre los que se encuentran el comercio electrónico, los servicio multimedia (Internet), el cifrado, etc. En este sentido cabe destacar los siguientes aspectos:
- España publicó, en abril de 1998, la nueva Ley General de Telecomunicaciones que además de liberalizar el sector ha introducido nuevos aspectos relativos a la privacidad y a la protección de datos. La nueva Ley, transponiendo en parte la Directiva 97/66/CE, garantiza el secreto de las comunicaciones al establecer que solo con orden judicial las fuerzas y cuerpos de seguridad podrán interceptar los contenidos de las comunicaciones. También se reconoce el derecho de los ciudadanos a utilizar el cifrado, si bien, el estado se reserva el derecho a requerir las claves y el algoritmo, mediante el depósito en un organismo público. Este último aspecto queda pendiente de un desarrollo reglamentario posterior.

En septiembre de 1998 se ha completado la transposición de la Directiva 97/66/CE, de protección de datos en el sector de las telecomunicaciones. De la misma cabe destacar los siguientes aspectos: Se establece que los datos de tráfico deben ser cancelados al terminar la comunicación, pudiendo mantenerse únicamente los datos necesarios para la facturación. Se reconoce el derecho del abonado a no recibir la factura detallada, en este sentido se prevé que a través de una orden ministerial se especifiquen las formas en que se podrá hacer anónimo, en la factura, la identificación del abonado llamado. Respecto de los repertorios telefónicos se establece que solo se incluirán los datos necesarios, y que si éstos son ampliados se deberá contar previamente con el consentimiento del abonado. Se reconoce el derecho del abonado a no aparecer en el repertorio y a que se borre parte de su dirección. Se reconoce también el derecho del abonado a que se marquen sus datos en el repertorio para que éstos no se utilicen con fines de marketing directo.

Finalmente, se establece que para las llamadas no solicitadas con fines de venta directa y efectuadas mediante sistemas automáticos se requerirá el consentimiento previo del afectado. Este consentimiento no será requerido si se utilizan sistemas no automáticos, aunque en este caso se reconoce el derecho de exclusión.

- La Comisión Europea esta trabajando en un borrador de Directiva relativa al Comercio Electrónico, que contendrá regulaciones relativas a la responsabilidad de publicar contenidos ilegales o nocivos por medios electrónicos. También tiene muy avanzada una directiva sobre firma digital que contempla la utilización de seudónimos como forma de mantener el anonimato.
- Alemania cuenta desde 1997 con una Ley de Servicios de Comunicación e Información (conocida como Ley de servicios multimedia) que ha de ser informada de nuevo en 1999 encontrándose actualmente en fase de valoración. En este contexto una comisión ha elaborado unas recomendaciones que consideran que la futura ley debería contemplar de forma global los servicios de Internet, los servicios móviles y los prestados vía satélite y la repercusión en ellos de la protección de datos, así como la búsqueda de soluciones a nivel internacional.
- La agencia de protección de datos francesa (CNIL) ha elaborado un registro específico para los servidores Web con datos personales en Internet. En dicho formulario se recogen entre otros aspectos los siguientes: la identificación del responsable, la dirección para ejercicio de los derechos de acceso, rectificación y cancelación, las cesión de datos y categorías de datos cedidos, la fuente de los datos y la forma de recolección, las medidas de seguridad (integridad, autenticación, cifrado, firma digital, tercero de confianza que tiene en depósito las claves, organismo que ha certificado la Web), los tratamientos que se realizan con los datos relativos a la conexión. El cuestionario incluye ejemplos de información a facilitar a los usuarios de los diferentes servicios ofrecidos por Internet.
- En Holanda se está discutiendo un borrador de ley que pretende legislar diferentes aspectos relativos a Internet. Según este borrador, únicamente podrían ser perseguidos por difundir a través de sus ordenadores contenidos ilegales o nocivos quienes sean efectivamente conscientes de dichos contenidos y tengan los medios suficientes para detener dicha difusión y no lo hagan.
- El Gobierno del Reino Unido ha elaborado un borrador de norma para la transposición de la Directiva 97/66/CE, de protección de datos en telecomunicaciones. La norma se encuentra ahora en periodo de consulta. El artículo 12.2 de la Directiva deja a potestad de cada estado miembro el optar entre dos esquemas en relación con la recepción de llamadas no solicitadas para venta directa. Según una opción no se permiten dichas llamadas si no existe consentimiento previo de los afectados (requiere listado de los que quieren recibir tales llamadas), según la otra opción las llamadas son posible siempre que el abonado no haya expresado su rechazo a la recepción de dichas llamadas (requiere una lista de los que no quieren recibir tales llamadas). El Reino Unido ha optado por la segunda opción pero se reserva el derecho de optar por la primera opción si la práctica demuestra que no existe una protección efectiva. Dada la opción elegida se ha establecido la creación de una lista oficial de los que no quieren recibir tales llamadas mantenida bajo la jurisdicción del Ministerio de Telecomunicaciones. En relación con los abonados corporativos, el Gobierno ha decidido no regular ninguna restricción en relación con llamadas de marketing no solicitadas, pero ha introducido también un mecanismo similar al de personas físicas en relación con la recepción de faxes con fines de marketing directo (listado de los que no quieren recibir faxes de este tipo).
- Tras la reciente aprobación de la ley de protección de datos por el Parlamento Polaco, en agosto de 1998 se ha constituido la Agencia de Protección de Datos en dicho país. La Ley polaca sigue las directrices de la Directiva 95/46 de protección de datos. Con la aprobación de dicha ley, Polonia se convierte en el primer país del antiguo bloque del Este en disponer de legislación sobre protección de datos. Otros países del entorno, como es el caso de Lituania, se encuentran ya tramitando sus respectivos proyectos de ley.

6.2. Encuentro hispanoholandés sobre estándares de inspección

Con motivo de la celebración en Santiago de Compostela de la XX Conferencia Internacional de Autoridades de Control en materia de protección de datos, la Agencia de Protección de Datos presentó una ponencia relativa a estándares de inspección y a los métodos y procedimientos de la Inspección de Datos española.
Como resultado de la misma, los representantes del Registratiekamer, Autoridad de Control de los Países Bajos, mostraron su interés en compartir experiencias sobre la materia para tratar de llegar a métodos y procedimientos de

inspección comunes. La cada vez mayor internacionalización de los tratamientos de datos y la entrada en vigor de la Directiva 95/46/CE hacen que sea previsible que, cada vez con mayor frecuencia, sea necesario recurrir a actuaciones coordinadas entre las inspecciones de varias autoridades.
Establecidas estas premisas, se pensó por ambas partes que un primer paso en esta colaboración sería la celebración de un encuentro entre representantes de ambas inspecciones. El citado encuentro tuvo lugar en Madrid, en el mes de noviembre de 1998, un encuentro de dos días de duración, en el que se expusieron los métodos de trabajo de ambas inspecciones.
A la finalización del mismo, se constató que, aun existiendo diferencias de enfoque y tipos distintos de inspección en cada uno de los países, era posible establecer un conjunto importante de similitudes que podían servir como base de un trabajo común.
Para continuar dicho trabajo, se acordaron dos líneas de acción. La primera de ellas fue la de presentar en la próxima Conferencia de Primavera de Autoridades de Protección de Datos, que está previsto celebrar en Helsinki, en el mes de abril de 1999, un informe con el resultado del encuentro y, en su caso, ampliar los trabajos a todas aquellas autoridades que muestren interés en el tema.
La segunda línea de acción consistió en el lanzamiento del proyecto de una inspección coordinada entre ambas autoridades, utilizando métodos y documentos similares acordados previamente, para así poder analizar los resultados y avanzar en el establecimiento de estándares comunes.
Ambas actividades está previsto que se desarrollen a lo largo de 1999, dándose cuenta de su resultado en la próxima Memoria de la Agencia.

7. OTRAS ACTIVIDADES

7.1. CONFERENCIA DE PRIMAVERA DE AUTORIDADES DE PROTECCIÓN DE DATOS EN DUBLIN (DÍAS 24 Y 25 DE ABRIL EN DE 1998)

La Conferencia de Primavera de los Comisionados Europeos de Protección de Datos se compone los Comisarios de la Unión Europea, así como de los representantes de Noruega e Islandia. Su misión consiste principalmente en analizar los problemas de la protección de datos en el ámbito europeo, con vistas a elaborar una posición común para la Conferencia Mundial Anual.

En la Conferencia de 1998 se trataron los siguientes temas:

* Misión, organización y actividades actuales de las Oficinas de Protección de Datos.
* Policía, aduanas y cuestiones afines: Europol, Shengen, Eurodac y el sistema de información aduanera.
* El papel de las auditorías de confidencialidad, la comprobación previa y un planteamiento basado en la adopción de estándares en la consecución de una protección de datos eficaz.
* Procesamiento de datos personales y la libertad de expresión: el periodismo y el artículo 9 de la Directiva.
* Estudio del tratamiento automatizado de datos personales por parte de las entidades del sector financiero.
* Cuestiones relativas al crédito al consumo.
* Código de Conducta respecto a los programas informáticos para Internet.
* Marketing para Internet.
* Evolución de las tecnologías de la Información y de su regulación en el ámbito internacional.
* El Papel de Internet como apoyo al trabajo desempeñado por las autoridades competentes en materia de protección de datos.

La Delegación Española además de participar activamente en el debate, presentó un proyecto de cooperación entre las diversas Agencias consistente en conectar las diferentes páginas web de la Agencias, con vistas a facilitar una mayor coordinación entre las diferentes autoridades de control y una mayor información por parte de los ciudadanos.

7.2. CONFERENCIA MUNDIAL DE AUTORIDADES DE PROTECCIÓN DE DATOS CELEBRADA EN SANTIAGO DE COMPOSTELA (DEL 16 AL 18 DE SEPTIEMBRE DE 1998)

La Agencia de Protección de Datos Española fue la autoridad encargada de organizar esta Conferencia que reune a las Autoridades de protección de datos a nivel mundial entre los días 16 al 18 de septiembre. El programa de la Conferencia, consensuado con las autoridades de los países participantes trató de diversos temas de máxima actualidad sobre la materia, que fueron desarrollados por prestigiosos miembros de aquellas Autoridades y por otros especialistas en la materia.

En primer lugar, intervino el Director de la Agencia Española en su condición de anfitrión, desarrollando el *tema "El derecho a la privacidad y su frontera en los demás derechos humanos*". La siguiente ponencia, a cargo del representante de la Comisión Europea, versó sobre *"El escenario internacional y la Directiva Europea sobre Protección de Datos".* El representante de la Agencia Francesa se encargó de la titulada *"La aplicación de las reglas de la protección de datos a datos públicos o accesibles al público*", interviniendo como participantes el representante de la Agencia de Nueva Zelanda y el catedrático español D. Carlos Lema. Posteriormente fue abordado el tema "*Protección de datos y road pricing". Utilización de nuevas tecnologías para la vigilancia en las carreteras*", del que fue ponente el representante de la Agencia de los Países Bajos, participando también un Magistrado español. Más tarde fue objeto de estudio un tema de tanta actualidad como "*Internet: correo electrónico, venta electrónica, códigos deontológicos*" a cargo de dos miembros de la Agencia de Italia, participando los representantes de las Agencias de Ontario y de Hong Kong.

La segunda jornada comenzó con el análisis de las "*Transferencias internacionales y métodos para reforzar la cooperación internacional*" bajo la ponencia del profesor Reidenberg de la Universidad de Fordham (USA), participando sobre el mismo tema representantes de las Agencias Suiza y Portuguesa de Protección de Datos. A continuación se abordó el tema *"Medidas de seguridad de las bases de datos: desarrollo reglamentario*" del que fue ponente una representante de la Agencia Española de Protección de Datos y participaron miembros de la Agencia del Reino Unido y de la Agencia Alemana de Berlín. El "*Tratamiento de datos de solvencia patrimonial y el análisis de los riesgos financieros*" corrió también a cargo de un representante de la Agencia de Protección de Datos de España, con la participación de un miembro de la Agencia Francesa. Finalmente se abordó el tema "*Concienciación del individuo en la protección de sus datos personales*" bajo la ponencia de un representante de la Agencia Alemana (Hamburgo), participando el Presidente de la Asociación Española de Usuarios de Servicios Bancarios. Todas las sesiones se enriquecieron con animado coloquio e importantes aportaciones por parte de los asistentes.

Por último, el 18 de septiembre y en sesión cerrada para las autoridades de protección de datos de la Unión Europea, se abordaron los temas: "*Determinación de estándares de inspección*" y "*Datos especialmente protegidos*" con la intervención como ponentes de representantes de la Agencia Española y Alemana respectivamente.

Dada la gran calidad de las ponencias y las aportaciones de los participantes, la Agencia de Protección de Datos ha decidido su publicación íntegra, con la convicción de que con ello se contribuirá a una mayor difusión y conocimiento de los importantes temas abordados en la XX Conferencia Internacional.

MEMORIA DE 1998 - ANÁLISIS Y VALORACIÓN DE LOS DIVERSOS PROBLEMAS DE LA PROTECCIÓN DE DATOS EN ESPAÑA

1. INTRODUCCIÓN

Don Juan Manuel Fernández López, fue nombrado Director de la Agencia de Protección de Datos el 3 de abril de 19981. El 27 de mayo de 1998 compareció el Director de la Agencia de Protección de Datos a petición propia ante la Comisión Constitucional del Congreso, para informar sobre la situación y orientación de la actuación futura como Director del citado órgano, así como en respuesta a tres peticiones de comparecencia, todas ellas solicitadas por el Grupo Mixto.

Concretamente se trataba de una solicitud para informar de las actuaciones de la Agencia de Protección de Datos en relación con las denuncias efectuadas contra la Compañía Telefónica Nacional de España, S. A., por la presunta venta de los datos de carácter personal de sus abonados sin contar con su consentimiento expreso, solicitud de comparecencia para informar de las líneas generales, es decir, en este sentido redundante con la petición a solicitud del Director, pero con mención específica de las actuaciones que piensa llevar en relación con la cesión por el Ministerio de Defensa a la empresa que resulte adjudicataria del concurso para la campaña publicitaria de tropa profesional de un listado con los nombres y direcciones de dos millones de jóvenes españoles en soporte informático.

La aplicación de la Ley Orgánica 5/1992, de 29 de octubre, en el año 1998, puso de manifiesto una serie de problemas jurídicos, algunos ya tratados en Memorias anteriores, tal como el de los ficheros de solvencia patrimonial o el marketing directo. En la comparecencia del Director de la Agencia ante la Comisión Constitucional del Congreso se plantean algunos de estos problemas de modo especifico, por lo que se van a analizar a continuación, así como las líneas generales de actuación futura de la Agencia expresadas por el nuevo Director en su comparencia. A continuación se van a tratar las respuestas dadas a las cuestiones planteadas en relación con los procedimientos abiertos a Telefónica, así como los problemas suscitados por el Ministerio de Defensa y el Marketing Directo.

En otro apartado se abordará el desarrollo normativo, en relación con la transposición de las Directivas 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en el tratamiento de datos personales y la libre circulación de éstos y la Directiva 97/66/CE relativa al tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones, la reforma del Reglamento Hipotecario, así como la Instrucción 1/98 del Director de la Agencia.

2. COMPARECENCIA EN EL CONGRESO: LÍNEAS MAESTRAS DE SU ACTUACIÓN AL FRENTE DE LA AGENCIA DE PROTECCIÓN DE DATOS

El Director de la Agencia de Protección de Datos manifestó en su comparecencia de 27 de mayo de 1998 ante la Comisión Constitucional, las siguientes líneas maestras de su programa de actuación al frente de la Agencia de Protección de Datos del modo siguiente:

2.1. PROMOCIÓN DEL DESARROLLO NORMATIVO

El Director ha considerado una de sus prioridades principales impulsar la transposición de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en el tratamiento de datos personales y la libre circulación de éstos.

También ha considerado de primera magnitud la necesidad de informar preceptivamente aquellas normas sectoriales que tengan incidencia sobre la protección de datos personales automatizados. Aunque, en principio, podría pensarse que el artículo 36.h) de la Ley Orgánica de Protección de Datos no exige el informe preceptivo de la Agencia más que en las disposiciones generales que desarrolle la misma, el espíritu de la norma y las exigencias de racionalidad legislativa determinan que la Agencia pueda y deba informar normativas sectoriales que afectan a la protección de datos. A este respecto hay que señalar nuevamente que el artículo 5 apartados a) y b) del Estatuto de la Agencia establece que los proyectos de disposiciones generales de desarrollo de la Ley Orgánica, así como cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica deberán ser informados preceptivamente por la Agencia.

Con este fin, se han realizado las gestiones pertinentes en el Ministerio de Justicia para poder tener información y manifestar el criterio de la Agencia sobre cualquier disposición de carácter general que afecte directa o indirectamente a la protección de datos.

En el ámbito del debate sobre la configuración jurídica de la Agencia se suscitó la cuestión relativa a la posibilidad de que ésta pueda formular iniciativas a los Parlamentos o a otras Instituciones Públicas. Esta cuestión fue abordada por el Director de la Agencia en sentido afirmativo, considerando necesaria la atribución a la Agencia de competencias en este aspecto, de un modo análogo a cómo sucede en otros organismos de la Administración, como el Tribunal de Defensa de la Competencia.

Para analizar más en profundidad este tema hay que remitirse al apartado de Desarrollo Legislativo al final de este epígrafe.

2.2. NECESIDAD DE DAR A CONOCER LA LEY ORGÁNICA 5/92 DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONALA pesar de la labor desarrollada hasta ahora por la Agencia, dado lo relativamente reciente de la ley, no es suficientemente conocida por los ciudadanos a los que ampara ni por las entidades públicas y privadas que deben cumplirla. A este respecto se prevén las siguientes líneas de actuación:

- Potenciar el servicio de atención al ciudadano. Para saber el grado de conocimiento de la ley por parte de los ciudadanos, se está considerando la posibilidad de que realice una encuesta el Centro de Investigaciones Sociológicas.
- Llevar a cabo una campaña de publicidad, dentro de los límites presupuestarios de la Agencia, insertando anuncios en periódicos y prensa sectorial, así como la presentación pública de la memoria anual.
- Participación y organización de seminarios, jornadas y cursillos para los sectores empresariales y administraciones públicas, en particular para las corporaciones locales.
- Publicaciones específicas de la Agencia, divulgativas, en particular en el ámbito de las nuevas tecnologías y de los derechos de los ciudadanos en este campo. (Véase el apartado del Premio de la Protección de Datos).

En este ámbito se pueden observar el importante incremento de actividad en el Área de Atención al Ciudadano debido a estos esfuerzos,), con un crecimiento del 15,4 % de las consultas presenciales, un incremento del 30% en las llamadas telefónicas, y del 44% de las consultas escritas.

Por lo que respecta a la difusión publicitaria, cabe destacar la realización de una campaña publicitaria general, y otra específica sobre Schengen, como se detalla en las actividades de la Secretaría General. También se ha abordado el proyecto de realización de una encuesta por parte el Centro de Investigaciones Sociológicas; esta encuesta tendría por objeto averiguar el nivel de conocimiento de los ciudadanos españoles de la protección de datos. Se prevé que esta campaña se pueda llevar a cabo en los primeros meses de 1999.

El Director de la Agencia ha participado en numerosos foros de debate entre los que destacan los relacionados con el Marketing Directo, el funcionamiento de la propia Agencia, la confidencialidad en los Sistemas de Información Clínica, protección de datos en el sector financiero y bancario, así como temas relacionados con la Seguridad en el tratamiento de datos en el sector público.

Asimismo ha mantenido numerosas reuniones con representantes de los sectores públicos y privados entre los que cabe destacar dentro del sector privado las entidades financieras, empresas aseguradoras, marketing directo, telecomunicaciones, asociaciones de consumidores y usuarios, así como diversas asesorías y consultorías; en el ámbito público se han mantenido reuniones con los representantes de Departamentos Ministeriales y otros organismos de la Administración Central, de la Administración Autonómica, Universidades y representaciones diplomáticas de otros países.

2.3. ESTIMULAR LA ADOPCIÓN DE CÓDIGOS TIPO DE CARÁCTER SECTORIAL

Otra de las prioridades es estimular la adopción de códigos tipo de carácter sectorial que, de un lado, potencien la protección del ciudadano y, de otro, fijen para los asociaciones y organizaciones de un mismo sector empresarial un marco jurídico conforme con la ley, facilitando así su mejor cumplimiento. Por su importancia merece destacarse que, a lo largo de 1998, se ha trabajado con la Asociación Española de Marketing Directo en la confección de un código deontológico para actividades de venta y promoción por medio de Internet. Como resultado de este esfuerzo conjunto se ha depositado en la Agencia este Código (ver apartado relativo a Códigos Tipo y el anexo correspondiente).

2.4. COORDINACIÓN CON OTRAS INSTITUCIONES

En el ámbito de la coordinación con otras Instituciones, es preciso destacar en especial el Defensor del Pueblo, que también recibe quejas sobre incumplimiento de la ley, cuyo artículo 45.4 obliga al Director de la Agencia a comunicar las infracciones que puedan cometer las Administraciones Públicas. A este respecto merece una mención especial la reunión mantenida con el Adjunto del Defensor del Pueblo durante el mes de julio, así como la cooperación obtenida de dicha Institución y del Defensor del Menor de la Comunidad de Madrid en relación con el código ético de control de la publicidad en Internet; también merecen especial mención los contactos mantenidos con la Agencia de Protección de Datos de la Comunidad de Madrid, en el marco de la cooperación entre la Agencia y las autoridades de protección de datos de las Comunidades Autónomas previstas en el artículo 40 de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal y artículo 12 del Real Decreto 1332/94 que desarrolla la anterior.

En el ámbito de las Corporaciones Locales los principales esfuerzos para difundir y garantizar el cumplimiento de la Ley se han llevado a cabo a través de sus principales organizaciones, tales como la Federación Española de Municipios (FEM) y la representación de las entidades en el Consejo Consultivo. Dicha actividad se ha complementado con una actividad específica dirigida por la Subdirección del Registro para promover y facilitar la inscripción de sus ficheros en el Registro General de Protección de Datos.

2.5. PLANES DE INSPECCIÓN

Habiéndose realizado con anterioridad la inspección sectorial de ficheros de los hospitales públicos, Fuerzas y Cuerpos de Seguridad, tanto del Estado como autonómicos y locales, y el proceso de recogida de datos de las encuestas de población de las Comunidades Autónomas, se lleva a cabo en la actualidad o está programada para un futuro inmediato la revisión del sistema Schengen en España, de las salas de juego, del sector de las telecomunicaciones, el de la solvencia patrimonial, también del sector del seguro y los grandes ficheros públicos, en especial el de la Agencia Tributaria y el de la Seguridad Social. (a este respecto véase la parte de la Memoria correspondiente a la Inspección).

De ellos se han culminado en 1998 los planes de Inspección relativos a Schengen, Salas de Juego, los ficheros de información sobre solvencia patrimonial y crédito y seguros, habiéndose iniciado la relativa a telecomunicaciones, y encontrándose en fase preparatoria las Inspecciones de los grandes ficheros públicos. Sobre el cumplimiento de estas previsiones en detalle se puede consultar el apartado de esta Memoria dedicado a la protección de datos.

2.6. EJERCICIO DE LA POTESTAD SANCIONADORA

Otra de las líneas de actuación es la aplicación estricta de la ley a los infractores, en especial a los reincidentes. Lo deseable es que el grado de cumplimiento de la ley haga disminuir el número de estos procedimientos. La sanción es,

en cierto modo, el fracaso del Derecho, pero la sanción también es un medio de defensa del Estado de Derecho. Lo deseable en este caso es la disminución de las sanciones basada a su vez en la disminución de las infracciones, lo que denotaría un mayor nivel de cumplimiento de la Ley por parte de los obligados (a este respecto véase la parte de la Memoria correspondiente a la Inspección).

2.7. PROMOVER LA ACTIVIDAD DEL CONSEJO CONSULTIVO

Para el desarrollo de las funciones del Director de la Agencia de Protección de Datos, la ley ha previsto el Consejo Consultivo como órgano de asesoramiento, en el que están representados los principales estamentos de la sociedad: Congreso, Senado, Universidades, Administraciones Central, Autonómica y Local, Real Academia de la Historia, Consejo de Consumidores y Consejo Superior de Cámaras. La primera sesión con el nuevo Director al frente de la Agencia tuvo lugar el día 20 mayo de 1998, con un apretado orden del día.

Se considera necesario estimular en la medida de lo posible el funcionamiento del Consejo Consultivo, dado que por su composición multidisciplinar puede realizar importantes aportaciones a una comprensión más cabal y completa de los complejos problemas que plantea la protección de datos. Ya en la primera reunión el Consejo se ha mostrado seriamente interesado en los temas sometidos a consideración y el Director desea manifestar que ha recibido un apoyo importante desde el primer momento. (Para mayor información véase el apartado correspondiente al Consejo Consultivo).

2.8. PARTICIPACIÓN ACTIVA EN LOS FOROS INTERNACIONALES

Asimismo, la Agencia de Protección de Datos ha de continuar presente en los foros internacionales, en los que viene obligada a participar como los del Grupo de Trabajo del Artículo 29 dentro de la Comisión Europea, o en el Grupo de Expertos del Consejo de Europa, Schengen, y puesta en marcha de la Autoridad de Control Común de Europol, entre otros. A este respecto, es de destacar que la Agencia española fue encargada de organizar la XX Conferencia Internacional de Autoridades de Protección de Datos, que tuvo lugar en Santiago de Compostela del 16 al 18 de septiembre de 1998. (Para mayor información ver el apartado relativo a relaciones internacionales).

RESPUESTAS A LAS SOLICITUDES DE INFORMACIÓN PLANTEADAS POR LOS GRUPOS PARLAMENTARIOS EN LA COMPARECENCIA
PROCEDIMIENTOS DE INVESTIGACIÓN A TELEFÓNICA

El Grupo Parlamentario Mixto del Congreso planteó una cuestión específica relativa a la utilización comercial por Telefónica de datos personales sin contar con el consentimiento expreso de los afectados. Dada la alarma social que han originado estas acciones, y respondiendo a las solicitudes del Grupo Mixto del Congreso relativas a las actuaciones previstas por la Agencia de Protección de Datos, el Director de la Agencia ha contestado del modo que se expone a continuación.

Ya en el año 1996 se recibieron varias denuncias en las que se puso de manifiesto la recepción en los nuevos domicilios de los afectados de propaganda procedente de diversas entidades. Esta publicidad contenía sus datos personales que habían sido cedidos por la filial de Telefónica, Telefónica Publicidad e Información (TPI), a través del producto Coditel.

En la Agencia de Protección de Datos se abrió un procedimiento contra Telefónica de España por cesión de datos a su filial TPI, por tratamiento de datos sin consentimiento por parte de TPI y por cesión de datos por TPI a terceros. Se declararon probados la cesión de datos de Telefónica a TPI, así como también el tratamiento y posterior cesión de estos datos a empresas para realizar campañas de marketing.

Por resolución de 6 de junio de 1997 se sanciona a Telefónica de España con 50.000.001 pesetas por cesión de los datos a TPI. Se sanciona también a TPI con 10.000.001 pesetas por tratamiento de datos sin consentimiento de los afectados y se sanciona con 50.000.001 pesetas a TPI por cesión de datos a terceros.

Posteriormente, en 1997 varias denuncias de ciudadanos manifiestan no estar de acuerdo en la forma en que Telefónica de España estaba procediendo a recabar el consentimiento de los abonados, mediante una circular, para proceder a la cesión de sus datos a otras empresas del grupo. Se acuerda la apertura del procedimiento por cesión de datos de Telefónica a terceros y por falta de información en la recogida de esos datos. Se declaran probados tanto la cesión como la falta de información en la recogida de datos.

Por resolución de 3 de abril de 1998 se sanciona a Telefónica con 30 millones de pesetas por falta de información en la recogida de datos y no se le sanciona por la cesión de datos al habérsele impuesto ya sanción por este motivo en el anterior expediente al que he hecho referencia. Por una sola denuncia en que el afectado dice que se han utilizado sus datos personales para publicidad, después de haber solicitado expresamente que no fueran utilizados para esta finalidad, se abre un nuevo procedimiento sancionador contra Telefónica por tratamiento de datos sin el consentimiento del afectado. Se declara como hecho probado el tratamiento sin consentimiento y por resolución de 11 de este mes se sanciona a Telefónica en la cuantía de 10.000.001 pesetas.

Se han abierto otros procedimientos por dos denuncias por no haber proporcionado TPI -la filial de Telefónica- toda la información sobre el derecho de acceso, sino solamente parte de los mismos. También de oficio, se abrió otro proce-

dimiento a Telefónica que remitió a sus abonados una circular informativa solicitando su consentimiento para la cesión de datos a empresas del grupo y a terceros. Se ha acordado la apertura del procedimiento por falta de información para la cesión de datos. Como consecuencia de todas estas actuaciones, además de las sanciones mencionadas Telefónica ha comunicado a sus abonados que no va a ceder los datos a terceros. Por su parte, TPI comunica a la Agencia de Protección de Datos la destrucción de sus ficheros y la correspondiente supresión de la inscripción de los ficheros en el Registro General de Protección de Datos.

También se ha planteado si las multas que impuestas a Telefónica resultan disuasorias para evitar la infracción, o dicho en otros términos,*"si resulta barato el infringir"*. A este respecto, se puede contestar en el sentido del estudio que ha realizado la Agencia con motivo de la transposición de la Directiva: para evitar estas situaciones una de las propuestas consiste en que las multas puedan llegar hasta el 10 por ciento de la cifra de facturación de las empresas, en términos similares a lo que ocurre en la Ley de Defensa de la Competencia.

Por otro lado, otro medio adecuado podría consistir en obligar, como una sanción más, a dar publicidad a las resolu - ciones que dicte la Agencia, de forma ejemplarizante y, también, para que los ciudadanos conozcan las posibilidades que la Ley y la Agencia les facilitan.

CAMPAÑA PUBLICITARIA DEL MINISTERIO DE DEFENSA PARA LA CAPTACIÓN DE TROPA PROFESIONAL

El Grupo Parlamentario Mixto del Congreso planteó otra cuestión específica relativa a la adjudicación del concurso para la campaña publicitaria de tropa profesional de un listado con los nombres y direcciones de dos millones de jóvenes en soporte informático a una empresa privada. Este proyecto ha tenido un importante eco en los medios de comunicación social, con la consiguiente alarma social y la consiguiente petición de información sobre las acciones emprendidas por la Agencia mediante comparecencia ante la Comisión Constitucional del Congreso

Apareció en la prensa esta noticia referida con anterioridad al nombramiento del Director actual de la Agencia. Toda vez que el anterior Director ya había cesado, y antes de la toma de posesión del actual Director, éste intervino de inmediato para comprobar el alcance de dicha información, poniéndose en contacto con el Subsecretario del Ministerio de Defensa.

Se recibió información de que se pensaba llevar adelante una campaña publicitaria para informar del acceso a la categoría de tropa profesional, que comprendía no sólo la confección y distribución del *mailing* sino también anuncios en prensa y en televisión, manifestando el Subsecretario de Defensa la disposición de aquel departamento para cumplir en todo con la legalidad vigente, por lo que tenían decidido realizar una consulta por escrito a la Agencia de Protección de Datos. En dos ocasiones se ha dirigió el Ministerio de Defensa a la Agencia, que ha respondido a sus consultas en fechas 3 y 22 del mes de abril de 1998.

En definitiva, el problema principal radica en si los datos que se recaban para una concreta finalidad, en este caso el reclutamiento, pueden ser utilizados por el responsable del fichero directa o indirectamente para una finalidad distinta de la que permitió recabar los datos y tratarlos informatizadamente, lo que está prohibido por el artículo 4.2 de la Ley Orgánica de Protección de Datos. Resulta secundario el hecho de la entrega del fichero a un tercero para la prestación de un servicio, ya que ello es posible sin consentimiento del afectado siempre que no se cedan los datos a terceros ajenos al contrato, que se destruyan los datos una vez prestado el servicio y que no se apliquen a fin distinto del que figura en el contrato de servicios.

Se han recibido también en la Agencia escritos relacionados con el asunto: por un lado, del Partido Democrático de Nueva Izquierda, instando las actuaciones oportunas para evitar la operación de cesión y, por otro, de la Asociación de Consumidores de la Plataforma de opinión reivindicativa, en los que se denuncian posibles infracciones de la Ley Orgánica de Protección de Datos.

En este sentido, alguno de los reclamantes ha manifestado su preocupación sobre la actuaciones realizadas o que piensa llevar a cabo el Ministerio de Defensa en relación con la cesión de datos relativos a dos millones de ciudadanos españoles de entre 18 y 24 años, potenciales aspirantes a soldado profesional. Esta preocupación se manifiesta en el valor que esta información podría tener para cualquier empresa. También manifiesta que los datos en cuestión no son obtenidos por el Ministerio de Defensa, sino por los entes reclutadores, fundamentalmente consulados y sobre todo ayuntamientos, que realizan una actividad previa al reclutamiento, para que, luego, el Ministerio de Defensa, con la tropa y la marinería, desarrolle las actividades de encuadramientos, sorteos, etcétera, y que son datos que se obtienen por estas entidades con una finalidad concreta, que es la prestación del servicio militar y no cualquier otra, aunque esté conectada con el Ministerio de Defensa.

Una tercera comunicación se ha recibido del Defensor del Pueblo, en la que, dentro de sus facultades institucionales, solicita informes sobre las actuaciones realizadas por la Agencia de Protección de Datos en este asunto. Se recibió el día 6 de mayo de 1998 y el día 7 se ha dado respuesta al Defensor del Pueblo dándole traslado de los escritos que se han dirigido al Ministerio de Defensa.

Para concluir, hay que señalar la colaboración que la Agencia ha recibido del Ministerio de Defensa en este asunto ha sido ejemplar. Desde el primer momento, se atendió la petición de información con gran diligencia. Se han remitido dos informes por parte de la Agencia y finalmente no se ha llevado a cabo esta campaña, atendiendo a las opiniones que al respecto ha manifestado la Agencia sobre este asunto.

MARKETING DIRECTO

Finalmente, en el marco de la comparecencia se suscitaron cuestiones relacionadas con el marketing directo y la obtención de datos por partes de las empresas de este sector. A este respecto, hay un tema preocupante porque podía dejar a las empresas del sector del marketing y de la publicidad en nuestro país en situación peor que sus homólogas en los países de la Unión Europea, donde pueden tener más facilidad de acceso a este tipo de datos que se obtienen del censo y que sólo en el momento en que el ciudadano dice que no quiere recibir publicidad se puede negar a ello. La realidad es que en el resto de los países europeos estas empresas están trabajando con datos accesibles al público y tal vez el hecho de que no puedan hacerlo en nuestro país determinará que lo hagan desde otros países, con la pérdida de los correspondientes puestos de trabajo.

Hay que dar la mayor protección que pueda ofrecerse a los ciudadanos, pero no establecer una legislación restrictiva respecto de la que pueda existir en otros países de la Unión Europea que pueda perjudicar a determinadas empresas en el ámbito del desarrollo comercial de estos datos.

Existe un problema serio en que cierto comercio, que es lícito y que se practica en el resto de los países de la Unión Europea, podría tener ciertas dificultades, sobre todo en cuanto al acceso a datos que proceden del Censo Electoral y que la Ley de Ordenación del Comercio Minorista expresamente permite, pero en cambio la Ley Orgánica Electoral General prohibe expresamente, con lo que se produce una contradicción legislativa lamentable.

A este respecto, y dentro de procedimientos sancionadores, el anterior Director de la Agencia realizo una consulta a la Junta Electoral Central y recibió la contestación de la prevalencia de la Ley Orgánica General Electoral, por su carácter orgánico, sobre la Ley de Ordenación del Comercio Minorista, por su carácter de simple ley; además y a pesar de su posterioridad, hacía imposible que pudieran utilizarse estos datos por las empresas de marketing. En cualquier caso, éste será el criterio de la Agencia al respecto en tanto que los Tribunales de Justicia no se pronuncien sobre este tema.

DESARROLLO LEGISLATIVO
LA TRANSPOSICIÓN DE LA DIRECTIVA 95/46/CE

El 31 de Agosto de 1998 se publica en el Diario del Congreso de los Diputados el Proyecto de Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal. Ya el 27 de febrero anterior la Agencia remitió a la Secretaría General Técnica del Ministerio de Justicia el Informe preceptivo sobre el borrador del Anteproyecto de Ley Orgánica por el que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que tiene por objeto la adaptación al Derecho español a la Directiva 95/46/CE. Toda vez que el trámite de audiencia pública modificó el texto del Anteproyecto, la Agencia de Protección de Datos volvió a emitir un nuevo informe el 31 de mayo de 1998.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo establece como fecha límite para la transposición de la misma al derecho interno el 24 de Octubre de 1998. Por lo que se refiere a la transposición de la Directiva al Ordenamiento Jurídico Español hay que tener en cuenta que la actual Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal, ya ha incorporado con carácter previo a la aprobación de esta Directiva, muchos de sus principios, habida cuenta que la actual redacción de la Ley se inspira en un proyecto anterior de Directiva. Toda vez que nuestra Ley Orgánica, cuando fue redactada, tuvo en cuenta la entonces propuesta de Directiva, las adaptaciones necesarias son pequeñas.

Existen algunas razones que pueden ser la causa del retraso que sufre la transposición de la Directiva. Entre otras, se pueden considerar los cuatro recursos de inconstitucionalidad aún no resueltos por el Tribunal Constitucional que pesan sobre la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal.

Ya en la Comisión de Justicia del Congreso en junio del año 1996 se planteó, qué se pensaba hacer con la transposición de esta Directiva y se instaba a reconducir el asunto de la transposición junto con la finalización de los cuatro recursos de inconstitucionalidad que están pendientes en esta materia, ya que uno de ellos estaba planteado por el Defensor del Pueblo, otro por 50 diputados del Grupo Popular, y los otros dos lo eran por cuestiones competenciales, interpuestos por el Consejo ejecutivo de la Generalidad y por el Parlamento catalán. El objetivo era que con la nueva redacción que de la Ley fuera posible el desistimiento en estos procedimientos. Hubiera sido deseable que el nuevo proyecto hubiera nacido sabiéndose a ciencia cierta cuál era el ámbito normativo que rige en esta materia, no teniendo la pendencia de cuatro posibles sentencias del Tribunal Constitucional.

Por parte de la Agencia se han propuesto, en consonancia con lo declarado por el Director de la misma ante el Congreso, una mayor flexibilización de las multas, dado que adolecen de una falta de flexibilidad para sancionar adecuadamente conductas diferenciadas. También se ha propuesto una mayor cuantificación, hasta el límite del 10 por ciento de la cifra de facturación, dado que en el debate parlamentario se puso de relieve que, para ciertas empresas, la cuantía de las multas puede no resultar disuasoria. Por otro lado, parece que un medio adecuado podría consistir en obligar, como una sanción más, a dar publicidad a las resoluciones que dicte la Agencia, de forma que sirvan como ejemplo y, también, para que los ciudadanos conozcan las posibilidades que la Ley y la Agencia les facilitan.

La nueva Ley debe resolver la contradicción existente en la actualidad entre la Ley Orgánica General Electoral y la Ley de Ordenación del Comercio Minorista, clarificándose así si algunos datos del Censo Electoral se pueden considerar fuentes accesibles al público para fines de marketing directo.

3. LA TRANSPOSICIÓN DE LA DIRECTIVA 97/66/CE DE TELECOMUNICACIONES

La Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y el Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones, incorpora, entre otras, la Directiva 97/66/CE, del Parlamento Europeo y el Consejo de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad.

El Real Decreto 1736/1998 incorpora en su articulado cuestiones relativas a las guías telefónicas, restringiendo de la publicación en las mismas a los abonados que hayan manifestado su deseo de oposición para que se les excluya de las guías públicas. En las guías de servicios de telecomunicaciones se podrán publicar otros datos personales de los abonados siempre que éstos hayan dado su consentimiento inequívoco2. Los abonados podrán exigir a los operadores, sin coste alguno, que se les excluya de las guías, o que se indique que sus datos personales no pueden utilizarse para fines de venta directa o que se omita parcialmente su dirección.

El Título V recoge la mayor parte de las previsiones relativas a la protección de los datos personales en la prestación de los servicios de telecomunicaciones. Establece sobre el alcance y sujetos obligados las normas de carácter técnico, en relación a la protección de datos en la explotación de redes y prestación de servicios de telecomunicaciones.

El ámbito de aplicación de estos preceptos se refiere al tratamiento de datos personales en :
- la prestación de servicios de telecomunicaciones disponibles al público,
- explotación de redes públicas de telecomunicaciones,

Se exceptúa del ámbito de aplicación del Título V, cuando de conformidad con la normativa vigente sea necesario adoptar medidas para:

- la protección de la seguridad pública.
- Seguridad del Estado.
- Aplicación del derecho penal.
- Interceptación legal de las telecomunicaciones.

Por lo que se refiere al Régimen Jurídico de estos datos, se hace una referencia expresa a la aplicación de la Ley Orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal a la protección de los datos personales vinculados a las redes y servicios de telecomunicaciones se regirá por lo dispuesto en la misma (de conformidad con el artículo 50 de la Ley General de Telecomunicaciones). Establece además que los operadores con licencia individual o con autorización general para la prestación de servicios de telecomunicaciones disponibles al público o los que exploten redes públicas de telecomunicaciones, deberán garantizar la protección de datos personales en el ejercicio de su actividad. También los operadores prestadores de servicios deberán tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios. Estas medidas se tendrán que adoptar en colaboración con el operador de la red pública.

Todo abonado que haya solicitado su exclusión de las guías, tendrá que ser informado por los operadores con una comunicación en la que se explique con mayor detalle las facilidades de identificación de línea llamante y de la línea conectada y de cómo su utilización puede afectar a la protección de su intimidad.

Se establece además que dentro de las llamadas no solicitadas para fines de venta directa**,** sólo podrán realizarse las llamadas automáticas (sin intervención humana3) o fax, con fines de venta directa, a aquellos abonados que hayan dado su consentimiento. Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas no automatizados, podrán efectuarse salvo las dirigidas a aquellos que hayan manifestado su deseo de oposición.

Establece la obligación con carácter general del responsable de tratamiento que cuando exista un riesgo concreto de violación de la seguridad de la red el prestador del servicio, deberá informar al abonado sobre dicho riesgo y las posi - bles soluciones **,** indicando su coste.

Los datos personales sobre tráfico y facturación sólo se podrán tratar datos personales por los operadores con la única finalidad de gestión de facturación y pagos de interconexiones, destruyéndose los datos personales cuando haya pasado el plazo legal para impugnar las facturas o exigir el pago.

También se podrán tratar estos datos para la promoción comercial de sus propios servicios de telecomunicaciones cuando el abonado haya dado su consentimiento4, salvo cuando dicho tratamiento se haya iniciado antes de la entrada en vigor del Reglamento.

Prevé el Reglamento la protección de los datos personales en la facturación detallada, concediendo a los abonados el derecho tanto a recibir facturas no detalladas, como a la supresión de un determinado número de cifras en la factura de los números a los que se ha llamado, al igual que a la no aparición en la factura de los números a los que se llama cuando el pago se haga con tarjeta de crédito.

En el Real Decreto se incorporan también importantes previsiones sobre la presentación y restricción de la línea

llamante y línea conectada, debiendo los operadores facilitar a la Agencia de Protección de Datos, con una antelación de quince días a la fecha de su envío, copia de la comunicación que vayan a utilizar para informar a sus abonados de las facilidades de identificación y restricción de la línea llamante y línea conectada.
La supresión en origen por línea de la identificación de la línea llamante, debe ofrecer las posibilidades, de que cualquier abonado pueda suprimir de forma automática en todas sus llamadas la identificación de su línea. Los abonados podrán, de manera gratuita, activar o desactivar dicha supresión automática dos veces en los seis meses siguientes de recibir la información referida en el apartado anterior.

La supresión en origen llamada a llamada se desarrolla además por la Resolución de 2 de diciembre de 1998. B.O.E. nº 312 de 30/12/98, por la que se atribuye el código "067", al servicio de supresión en origen llamada a llamada de identificación de la línea llamante.

No obstante, la regla anterior queda excepcionada cuando el destino de las llamadas corresponda a entidades autorizadas para la atención de urgencias (llamadas al 112), se tendrá que eliminar las marcas de supresión en origen de la identificación de la línea llamante; o ciertos destinos de las llamadas asociadas a determinados servicios, se podrá establecer por el Ministerio de Fomento, que no dispongan de la facilidad de identificación de la línea llamante.

Por último, se prevé la responsabilidad de los Operadores que tengan sus redes interconectadas en el caso de que faciliten información sobre la línea llamante a países, distintos de la relación que con este fin se establecerá por la Secretaría General de Comunicaciones, previo informe de la Agencia de Protección de Datos.

4. REFORMAS DE LOS REGLAMENTOS DEL REGISTRO HIPOTECARIO Y DEL REGISTRO MERCANTIL

Antes de valorar las modificaciones introducidas en el Reglamento Hipotecario y en el Reglamento del Registro Mercantil que pueden afectar a la protección de datos de carácter personal, introducidas ambas por el Real Decreto 1807/1998, de 4 de septiembre, se considera necesario analizar brevemente la Instrucción de la Dirección General de los Registros y del Notariado de 17 de febrero de 1998 (BOE 27/02/1998), ya que en cierta forma es el antecedente de la regulación contenida posteriormente en el artículo 332.6 del Reglamento Hipotecario pues viene a modificar la concepción de fuente accesible al público que tiene el Registro de la Propiedad.

Como se señala en la propia Instrucción, la misma se dicta, ante la disparidad de criterios seguidos por los Registradores de la Propiedad y Mercantiles en orden a la expedición o no de publicidad formal en los casos de peticiones masivas de notas simples respecto de datos consignados en sus archivos, partiendo para ello a su vez, de lo establecido en el articulo 607 del Código Civil respecto del Registro de la Propiedad y del artículo 23.1 del Código de Comercio respecto del Registro Mercantil, artículos que regulan con carácter general la publicidad formal de ambos Registros.

El Objeto de la referida Instrucción es establecer por la Dirección General de los Registros y del Notariado los principios generales de publicidad formal y actuación de los Registradores de la Propiedad y Mercantiles en caso de petición en masa.

Se establece en principio, dentro del punto quinto de la Instrucción, la prohibición con carácter general de que los Registradores de la Propiedad y Mercantiles no expedirán la publicidad formal cuando el objeto de la solicitud sea su incorporación masiva a bases de datos, registros paralelos, etc., sin responder en consecuencia a mandato alguno por parte del interesado en la información suministrada.

No obstante lo anterior se excepcionan de dicha prohibición, las solicitudes de publicidad formal que encajen en alguno de los siguientes supuestos:

1. Si se hacen en cumplimiento de alguna disposición legal que faculte la realización de estudios estadísticos.
2. Si su objetivo satisface un interés público como la realización de estudios sectoriales o de planificación económica por la Administraciones Públicas, Corporaciones de Derecho Publico, o instituciones publicas o privadas sin ánimo de lucro a estos efectos.
3. Si derivan de un Convenio de colaboración suscrito con el Colegio de Registradores de la Propiedad y Mercantiles de España, que es a quien por vía normativa corresponde la publicación de estadísticas con referencia a las bases de datos de los registros.

En estos casos, y, a pesar de que la solicitud encaje en alguno de los supuestos anteriores, la propia instrucción contempla, de una parte, que el solicitante se comprometerá por escrito a que el tratamiento y publicación de los datos se realizará mediante agregación de los mismos, salvaguardando el derecho a la intimidad y a la privacidad, y, de otra parte, obliga a los propios Registradores a hacer constar en la publicidad que expidan, que existe la prohibición de incorporar los datos obtenidos a ficheros o bases informáticas para la consulta individualizada de personas físicas o jurídicas, incluso expresando la fuente de información.

Esta prohibición que posteriormente se verá recogida en la modificación del articulo 332 del Reglamento Hipotecario, en concreto en su apartado 6, es importante destacarla dado que cambia la concepción de fuente accesible al público del Registro de la Propiedad, perdiendo éste dicha concepción siempre que se este considerando el tratamiento masivo de datos, necesitando por tanto el consentimiento de los afectados para poder realizar dicho tratamiento en el supuesto de que se pretendiese incorporar a cualquier tipo de ficheros.

Posteriormente a la instrucción anterior y como consecuencia de la reforma de la Ley Hipotecaria llevada a cabo por la Ley 7/1998 sobre condiciones Generales de la Contratación, se exige un cambio de redacción de los preceptos del Reglamento Hipotecario y del Reglamento del Registro Mercantil para su adecuación a la referida Ley, a la normativa sobre protección del consumidor y a la legislación sobre protección de datos de carácter personal, en especial a la norma general contenida en el articulo 4.2 de la LORTAD.

Dicho cambio se ha llevado a efecto por el Real Decreto 1867/1998, de 4 de septiembre, por el que de un lado se modifican determinados artículos del Reglamento Hipotecario, y de otro, se añaden cinco nuevos apartados al articulo 12 del Reglamento del Registro Mercantil, a través de la disposición adicional única de dicho Real Decreto.

4.1. REGLAMENTO HIPOTECARIO

Respecto al Reglamento Hipotecario sólo señalar que existen tres disposiciones que se refieren al tratamiento de datos y que son:

El artículo 332.2 cuando establece que se prohibe el acceso directo, por cualquier medio, al núcleo central de la base de datos del Archivo del Registrador, que responderá de su custodia, integridad y conservación, así como su incorporación de la base de datos para su comercialización o reventa.

El artículo 332.5 al prevenir que la nota simple informativa consistirá tan solo en un extracto sucinto del contenido de los asientos, consistente en la identificación de la finca, del titular o titulares de derechos inscritos, extensión, naturaleza y límites de los derechos y, en su caso, prohibiciones o restricciones que afecten a los titulares o a los derechos inscritos.

El art. 332.6 al establecer que los registradores no atenderán las solicitudes en masa o indiscriminada.

Por lo que se refiere a esta última prohibición se plantea como problema fundamental la cuestión ya avanzada anteriormente, de si el Registro de la Propiedad puede ser o no considerado como una fuente accesible al público en los términos empleados por la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, en concreto por lo previsto en su artículo 28.1 cuando establece que quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento.

En este sentido conviene precisar que la LORTAD garantiza en su artículo 4.2 que 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, por lo que debe entenderse que si la finalidad buscada por la Ley Hipotecaria es garantizar la seguridad del trafico inmobiliario, advirtiendo, a quienes se interesen por el estado y cargas de una finca de dichas circunstancias, y garantizando, fundamentalmente en el artículo 34, que quien adquiere del titular inscrito una finca o derecho, goza de la protección registral, de modo que, una vez inscrito su derecho, este resulta invulnerable por cualquier otro derecho que no constara en el registro, ello conlleva a considerar que, las consultas masivas de los datos del registro no sirven a la finalidad de la seguridad del tráfico inmobiliario, sino para otros fines distintos de este, y en consecuencia conforme prohibe el artículo 4.2 de la LORTAD, al apartarse de la propia finalidad, el Registro de la Propiedad en estos supuestos no podría ser considerado como fuente accesible al publico.

Finalmente y por lo que se refiere a las otras disposiciones contenidas en el Reglamento Hipotecario, relativas a la prohibición de acceso directo a los libros del registro; y, a la información que deben contener las notas simples informativas, únicamente señalar que tienen su apoyo legal en el artículo 222 apartados 2 y 5 de la Ley Hipotecaria, en la redacción dada por la disposición adicional segunda de la Ley 7/1998 de 13 de abril, sobre Condiciones Generales de Contratación, y su finalidad está directamente vinculada con la protección de privacidad que se garantiza en el articulo 18.4 de la Constitución y se desarrolla en la LORTAD.

De esta manera se evita que información distinta a la estrictamente necesaria para garantizar la seguridad en el tráfico inmobiliario se ponga a disposición de terceras personas, con lo que se cumple con el principio de que los datos no sean excesivos en relación con el ámbito y las finalidades para las que se han obtenido, que se establece en el articulo 4.1 de la LORTAD.

4.2. REGLAMENTO DEL REGISTRO MERCANTIL

Ante todo ha de señalarse que los sujetos objeto de inscripción en el Registro Mercantil son todos ellos empresarios, en una gran mayoría sociedades. Toda vez que según señala el artículo 1 de la LORTAD el objeto de la Ley es "....garantizar el honor, la intimidad personal y familiar de las personas físicas ...." aquellos que accedan al Registro Mercantil quedaran fuera de la protección que otorga dicha Ley sin perjuicio de que otras normas amparen los derechos de los empresarios y puedan ejercitar las correspondientes acciones en vía jurisdiccional.

Por lo que se refiere a la modificación del articulo 12 del Reglamento del Registro Mercantil introducida por la disposición adicional única del Real Decreto 1867/1998, conviene señalar que en el anteproyecto presentado a la Agencia para informe se contenía un apartado 5 del tenor literal siguiente:

"Se reconoce la posibilidad de incorporación de la información así obtenida mediante consultas a bases de datos para su comercialización siempre que los datos objeto de tratamiento automatizado se incorporen a bases registradas en la Agencia de Protección de Datos para realizar informes jurídicos o económicos en los que la publicidad formal no sea la única fuente de los mismos. Se excluye la publicidad engañosa".

Este era el único apartado que afectaba al régimen de protección de datos y en el informe emitido por la Agencia de Protección de Datos sobre el anteproyecto de redacción propuesto por la Dirección General de los Registro y del Notariado, se consideró como mas conveniente que no se realizara regulación alguna respecto del régimen de la privacidad, en atención a al publicidad formal del Registro Mercantil, salvo la que ya se encuentra regulada en el articulo 12.3 del Reglamento, en donde se deja a la responsabilidad del Registrador Mercantil la atención a consultas en masa o a la publicidad en general de datos personales.

Atendiendo a lo señalado en su informe por la Agencia de Protección de Datos, de la redacción final de la referida disposición adicional ha desaparecido el proyectado apartado 5.

5. INSTRUCCIONES DEL DIRECTOR DE LA AGENCIA

Al principio de 1998 el Director de la Agencia de Protección de Datos dictó la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. Las Instrucciones del Director de la Agencia se dictan al amparo de lo dispuesto en el artículo 36.c) de la Ley Orgánica 5/92 que atribuye al Director de la Agencia la función de "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 presente Ley".

Por lo que se refiere al objeto de la Instrucción 1/98, es aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales. Para ello, la Instrucción recoge la regulación de dichos derechos de acuerdo con la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio, y realiza una interpretación unitaria de los preceptos teniendo en cuenta la totalidad de principios legales.

La Ley Orgánica 5/1992 dedica los artículos 14 y siguientes a los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados. Dichos derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

El ejercicio de los derechos de acceso, rectificación y cancelación aparece regulado no sólo en la Ley Orgánica 5/1992, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos procedimentales de la citada Ley.

En las normas primera, segunda y tercera de la Instrucción se detallan los requisitos que deben cumplirse en el ejercicio de los derechos con carácter general. Sin embargo, las particularidades que presentan los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con fines de publicidad exigen tratarlos de un modo especial en las normas cuarta y quinta, respectivamente. (Ver anexo).

Dada la situación actual en lo que se refiere a la Transposición de la Directiva 95/46/CE, el Director actual de la Agencia ha decidido posponer la elaboración de Instrucciones en tanto no se apruebe el proyecto actual de modificación de la Ley Orgánica 5/92, por considerar que la solución e interpretación de algunos aspectos de la ley actual pueden quedar zanjados de modo definitivo por este procedimiento.

1 Nombrado mediante Real Decreto 498/98 de 27 de marzo.

2 Cuando el abonado se dirija al operador por escrito solicitándole que amplíe sus datos personales que figuran en la guía o cuando el operador solicite del abonado su consentimiento y éste le responda en el plazo de un mes dando su aceptación.

3 Aparatos de llamada automática.

4 Consentimiento tácito cuando se informa no se procede a dejar sin efecto de modo expreso. Ver Disposición Transitoria Séptima.

6. Análisis de algunas Sentencias dictadas por la jurisdicción contencioso-administrativa durante 1998 y que afectan a procedimientos sancionadores y procedimientos de tutela de derechos.

Durante 1998 han recaído 13 sentencias de la jurisdicción contencioso administrativa que han venido a resolver los correspondiente recursos contencioso administrativos interpuestos contra las resoluciones dictadas por la Agencia de Protección de Datos. Dichas resoluciones se corresponden con 11 procedimientos sancionadores y 2 expedientes de tutela de derechos.

Como primera nota a destacar es necesario resaltar que únicamente en un caso se ha revocado la resolución dictada por la Agencia, caso que mas adelante se comenta, y en el resto han sido confirmadas las resoluciones en todos sus términos. Ello es significativo de que los criterios de aplicación de la LORTAD utilizados por la Agencia han sido criterios conformes a derecho.

Del total de procedimientos resueltos y atendiendo a una distribución por sectores se desprende el siguiente cuadro:

Entidades financieras	2
Solvencia patrimonial y crédito	5
Publicidad Directa	3
Otros	3

De las sentencias dictadas y atendiendo al objeto de los recursos interpuestos se pone de relieve por su trascendencia los criterios mas importantes que han sido confirmados por la Jurisdicción Contenciosa.

6.1 Datos procedentes del Censo Electoral.

El criterio mantenido por la Agencia respecto a que los datos procedentes del censo electoral y del padrón municipal no son fuentes accesible al público ha sido confirmado por tres sentencias del Tribunal Superior de Justicia de Madrid.

Estas sentencias que han recaído en el sector de publicidad directa, han considerado el censo y el padrón municipal como una fuente no accesible al público y en consecuencia los datos que en ellos figuran no pueden ser utilizados para su comercio ni venta sin el consentimiento de las personas afectadas.

En los tres casos se utilizaron los datos del censo o del padrón para mandar publicidad de diversas entidades a un grupo extensos de personas.

La utilización de estos datos se consideran análogos tanto los obtenidos del padrón municipal como los del censo, puesto que en definitiva la inscripción y el registro de los datos en uno y otro caso es la misma.

La ley Orgánica 5/92 de Régimen Electoral General prohibe en su articulo 41.2 la información particularizada sobre los datos contenidos en el censo electoral. Asimismo el artículo 39 de la Ley que regula la exposición de las listas electorales a efectos de que los particulares puedan formular reclamaciones sobre sus datos censales y únicamente a estos efectos.

Por otra parte la redacción del articulo 16 de l Ley 7/85, de 2 de abril, de Bases del Régimen local, dada por la Ley 4/96, de 10 de enero, que pone de relieve el carácter confidencial de los datos del padrón municipal a los efectos previstos en la Ley Orgánica 5/92, no constituye sino una adaptación concreta de dicha norma que no altera tal carácter confidencial de los datos del padrón pues ya la propia ley 7/85 garantizo el respeto de los derechos fundamentales reconocidos en la constitución Española y concretamente en su artículo 18 lo que debe ponerse en relación con el Convenio del Consejo de Europa de 28 de enero de 1981, ratificado por España el 27 de enero de 1984, para la protección de las personas respecto del tratamiento formalizado de datos de carácter personal. Todo lo cual viene a confirmar la voluntad del legislador de extender el tratamiento de los actos censales a los actos contenidos en el padrón municipal.

Por tanto en todo caso, el uso que se haga de los datos censales debe estar circunscrito a las finalidades propias de las elecciones, o del régimen electoral y asi lo ha entendido la Agencia de Protección de Datos al considerar prohibida la información particularizada sobre datos censales fuera de dicha finalidad, considerando en consecuencia que los datos censales no constituyen fuente o documento accesible al público en el sentido previsto en los artículos 6 y 29 de la LORTAD y en consecuencia la inclusión, utilización y tratamiento de dichos datos en un fichero de publicidad vulneran dichos preceptos siendo sancionables tales conductas por infracción grave de las previstas en el articulo 43.3 d) de dicha norma.

6.2 Actuaciones de inspección no forman parte del procedimiento sancionador.

Es este otra de la particularidades y criterios que por su importancia convienen destacar habida cuenta que viene a confirmar la actuación de la Agencia de Protección de Datos en es este sentido.

El Tribunal Superior de Justicia de Madrid en el procedimiento objeto de análisis en el que por parte de la entidad denunciada no se posibilito el acceso a la inspección de la Agencia al objeto de llevar a cabo su actuación siendo en consecuencia sancionada por obstrucción a la labor inspectora, ha puesto de relieve en su sentencia que, dicha función no formaba parte del procedimiento y que en consecuencia no necesitaba previamente la existencia de un acuerdo para poder ser llevada a cabo pues perdería su efectividad.

Razona en este sentido el Tribunal considerando que parece claro que la recurrente no facilito precisamente la actuación de la Agencia de Protección de Datos. Así, cuando informada de la denuncia formulada, se le requirió para que informaran sobre el origen o procedencia de los datos personales del denunciante y de todos los registro relativos a su persona, respondió con evasivas, sin facilitar la información solicitada. Ello motivo, sin duda, la visitas de inspección para las que no se requiere acuerdo de ninguna clase. La Agencia esta apoderada por ley para realizar esta función que, por lo demás, nunca se enmarca en el curso de un procedimiento sancionador, teniendo una finalidad de control de la aplicación de la LORTAD, sin perjuicio de que, en ocasiones y como consecuencia de los resultados de una visitas de inspección, se inicie un procedimiento sancionador.

Si como pretende la parte, para girar una visita de inspección, la Agencia hubiera de comunicarlo con antelación, especificando los datos a inspeccionar, se frustraría la finalidad de la visitas, pues los afectados lógicamente borrarían la huella de cualquier actuación que pudiera comprometerles. Por eso el factor sorpresa es consustancial a toda actuación inspectora.

Dice la parte que el hecho de que se haya iniciado una inspección sin incoarse previamente el procedimiento sancionador le ha originado indefensión, pero como puede pretender que se incoe un procedimiento sancionador cuando no se conoce o no se ha producido la conducta que motivara posteriormente su iniciación.

En los autos objeto de análisis A la actora no se la ha sancionado por tener registrados los datos del denunciante sino por su conducta obstruccionista al no suministrar la información requerida ni permitir que los inspectores de la Agencia visualizaran directamente el fichero de datos.

6.3 Por último es importante realizar un breve análisis sobre la única sentencia de las dictadas en 1998 que no ha confirmado el criterio mantenido por la Agencia en su resolución.

Los hechos que dieron motivo a la sanción en el procedimiento analizado en resumen consistieron en que por parte de una entidad bancaria se facilitó el saldo de una cuenta corriente determinada a una persona que con anterioridad había sido titular de la referida cuenta, pero que en la actualidad no. Dichos hechos fueron calificados como graves y muy

graves de conformidad con lo dispuesto en los artículos 10 y 11 de la LORTAD, por vulnerar el deber de secreto por parte de la entidad financiera y por ceder datos sin consentimiento del titular de los mismos.

Después de la instrucción de procedimiento se considero por el instructor del mismo que los hechos denunciados y probados eran constitutivos de una infracción muy grave de conformidad con lo dispuesto en el artículo 43.4.b), y, posteriormente la resolución del Director de la Agencia considero que la actuación de la entidad no cabría calificarla como una cesión ilícita, no porque no haya existido transmisión del dato a un tercero, sino por cuanto que aquella lleva implícito un animo de cesión que no concurre en el caso examinado y así se vino a considerar en la resolución que en la gestión o tratamiento de los datos no se han observado los deberes formales o documentales precisos, que obligaría a la entidad a efectuar una verificación del poder o autorización del tercero para acceder a los datos de la cuenta corriente. En definitiva se trataría de una infracción leve tipificada en el artículo 43.2.d), fundamentando dicho cambio en una interpretación de la norma más favorable al infractor.

El Tribunal Superior de Justicia vino a considerar en sentido afirmativo que la comunicación de un saldo de una cuenta corriente a una persona no autorizada vulnera la LORTAD, lo cual coincide con el criterio mantenido por la Agencia, dado que si bien es cierto como afirma la parte actora que del saldo existente en una cuenta corriente sin mas, no se desprende ni se puede conocer el perfil de una persona, no es menos cierto que si ese dato se liga con otros, como en las presentes actuaciones en las que el solicitante del dato conocía de antemano el numero de la cuenta y la identidad de su titular, se consiguió tener un mayor conocimiento del perfil personal de la titular mediante la comunicación llevada a cabo por la entidad bancaria y esa conducta precisamente es la que prohibe la LORTAD.

El Tribunal Superior de Justicia sin embargo no se muestra conforme con el cambio de calificación que por parte de la Agencia se realiza al resolver el procedimiento y por eso lo anula.

El Tribunal en efecto no muestra su conformidad con el actuar administrativo, dado que los tipos sancionados en los artículos 43.2.d), 43.3g) y 43.4.b) no presuponen los mismos hechos. Es decir, en esos preceptos no se tipifica el mismo hecho atendiendo al grado de intencionalidad. Eso podrá ocurrir en relación con las infracciones graves o muy graves pero no en cuanto a la infracción leve en la que no se tipifica ni el quebranto de deber de secreto ni la cesión de datos, sino cualquier incumplimiento de índole formal o documental, no pudiendo considerarse tal, el suministro de información que debió quedar reservada en la entidad bancaria.

Este cambio es importante destacarlo habida cuenta que en las presentes actuaciones si bien lo que se trato fue de rebajar la sanción por la falta e intencionalidad, dicha rebaja no se podía formalizar dado que la tipicidad de la infracción cometida e imputada al responsable no esta en ningún caso prevista como leve y si como grave o muy grave según los datos estén o no especialmente protegidos

MEMORIA DE 1998 - OTRAS ACTIVIDADES

1.- XX CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS CELEBRADA EN SANTIAGO DE COMPOSTELA.

En el ejercicio de sus competencias, la AGENCIA DE PROTECCION DE DATOS española ha sido designada para organizar la XX Conferencia Internacional de Autoridades de Protección de Datos que tuvo lugar en Santiago de Compostela los días 16 - 18 de septiembre de 1998.

En la Conferencia se abordaron los siguientes temas:

* "El derecho a la privacidad y su frontera en los demás derechos humanos". Agencia española.
* *"El escenario internacional y la Directiva Europea sobre Protección de Datos: cinco semanas antes de su entrada en vigor". Unión Europea.*
* *La aplicación de las reglas de la protección de datos a datos públicos o accesibles al público (listas electorales, repertorios telefónicos). Su relación con la publicidad y el marketing. Agencia francesa.*
* *Protección de datos y "road pricing". Utilización de nuevas tecnologías para la vigilancia en las carreteras. Agencia holandesa.*
* *Internet: Correo electrónico, venta electrónica, códigos deontológicos. Agencia italiana.*
* *Transferencias internacionales y métodos para reforzar la cooperación internacional. Estados Unidos.*
* *Medidas de seguridad de las bases de datos: Desarrollo reglamentario. Agencia española.*
* *Tratamiento de datos de solvencia patrimonial. Análisis de riesgos financieros. Ficheros de solvencia positivos y negativos. Agencia española.*
* *Concienciación del individuo en la protección de sus datos personales. Agencia alemana.*
* *Informe sobre las actividades del Grupo 21 de Trabajo sobre Telecomunicaciones y Protección de Datos .*
* *Determinación de standards de Inspección: Experiencia de la Agencia de Protección de Datos Española. Agencia española.*
* D*atos especialmente protegidos: Datos sociales y de salud. Agencia alemana.*

Al finalizar la Conferencia se aprobó una declaración conjunta de los asistentes en relación con un proyecto del Gobierno de Islandia consistente en la creación de una base de datos con información genética de todos los habitantes de Islandia. El contenido de la declaración se transcribe a continuación:
"*Se ha puesto en conocimiento de los Comisionados para la Protección de Datos de los países pertenecientes a la Unión Europea y al Espacio Económico Europeo, reunidos en Santiago de Compostela, del 16 al 18 de septiembre de 1998, para celebrar la 20º Conferencia Internacional sobre Protección de Datos, por parte de sus compañeros escandinavos, la propuesta del Gobierno de Islandia de crear una base de datos electrónica de carácter centralizado que contendrá los archivos sanitarios y otros datos conexos, incluyendo información genética, en principio atinente a todos los ciudadanos de Islandia, con el fin de controlar el uso de los servicios médicos y de productos farmacéuticos. A este respecto, los Comisionados hacen hincapié en los siguientes aspectos:*
-Debe ser plenamente respetado el principio de consentimiento libre y espontáneo del interesado para el almacenamiento y el procesamiento de sus datos. Debe también reconocerse el derecho que asiste al sujeto de los datos a retirarlos de la base una vez sus datos hayan sido incorporados a la misma. Únicamente serían aceptables excepciones a estos principios por razones excepcionales y siempre que se ofrezcan garantías suficientes acerca del uso correcto de los datos.
-Específicamente, debe quedar clara la definición de lo que se entiende por "datos personales" y debe ser eficaz el método para asegurar el anonimato. En un país con una población relativamente pequeña, es probable que la información atinente a aspectos genéticos indique la ascendencia biológica y revele la identidad de los interesados. En todo caso, la utilización de un código para reemplazar los datos identificadores no es suficiente para asegurar el anonimato.
-Los intereses mercantiles del usuario no pueden inducir a una ampliación de la finalidad originaria del registro.

Expresan su seria preocupación acerca del asunto y recomiendan a las autoridades de Islandia que reconsideren su proyecto a la luz de los principios fundamentales consagrados en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, del Convenio 108 relativo a la Protección de Datos y la Recomendación (97) 5 referente a datos médicos, ambos del Consejo de Europa, y la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
(*) Esta declaración cuenta con el apoyo de los Comisionados para la Protección de Datos de Alemania, Austria, Bélgica, Dinamarca, *España, Finlandia, Francia, Grecia, Irlanda, Italia, Luxemburgo, Noruega, Portugal, Reino Unido.*

Asimismo, los asistentes adoptaron un acuerdo sobre la utilización de Internet. En dicho acuerdo se ponía de manifiesto que, sobre la base de los principios de protección de datos personales ya establecidos en muchos países y aplicables a Internet, todos los estados y en particular aquellos que hacen un mayor uso de nuevas tecnologías, deben adoptar y reforzar las medidas de protección de datos personales y promover la cooperación internacional, basada en el reconocimiento de principios universales para asegurar que el creciente uso de Internet no produce consecuencias incompatibles con la protección de datos personales y la privacidad.

2.- PREMIO PROTECCIÓN DATOS PERSONALES 2ª EDICIÓN.

Se ha convocado la 2ª edición del premio Protección de Datos Personales con una dotación de 1.000.000 pesetas, con la finalidad de profundizar en el estudio del desarrollo del artículo 18.4 de la Constitución.

Se otorgó el premio a la obra: "La protección de los datos de carácter personal en el ámbito de la investigación penal", presentada por el Profesor Asociado de Derecho Procesal de la Universidad del País Vasco D. José Francisco Etxeberría Guridi.

La obra premiada aborda las siguientes materias:
* La protección de los datos de carácter personal y la atenuación de las garantías como consecuencia de la investigación penal
- Introducción
- El derecho a la autodeterminación informativa
- La atenuación de las garantías sobre la protección de datos personales en el marco de la investigación penal
- La garantía del principio de legalidad o previsión legal
*Diligencias de investigación que inciden especialmente en el derecho de autodeterminación informativa
- Introducción
- Naturaleza jurídica de las diligencias
- Análisis de las concretas diligencias de investigación
- El ADN y la investigación criminal: la creación de ficheros o bancos de datos con perfiles de ADN
- Búsqueda entrecruzada de rasgos distintivos
- La comparación o contraste de datos
- La preservación de los datos personales obtenidos con ocasión de la intervención de las comunicaciones telefónicas
- La protección de los datos de carácter personal procedentes de la colocación de videocámaras o artilugios análogos
- La medida de vigilancia policial

Dada la calidad de las obras presentadas, el Jurado decidió por unanimidad conceder un accésit dotado con 100.000 pesetas a la obra titulada: "La responsabilidad civil del responsable del fichero en la LORTAD", presentada por el Profesor Titular de la Universidad de las Islas Baleares D. Pedro Grimalt Servera.

3. PARTICIPACIÓN DEL DIRECTOR DE LA AGENCIA EN DIFERENTES CONFERENCIAS, SEMINARIOS Y JORNADAS

Fecha	Ciudad	Título	Organizada por
5-6-98	Madrid	Mesa redonda: ***"Las claves para una correcta aplicación de la LORTAD en Marketing Directo"***	AEMD
10-6-98	Barcelona	Participación en el Programa de Doctorado y Master "Justicia Constitucional, Tutela Judicial y Derechos Fundamentales" Exposición: ***"Examen de la Organización y Funcionamiento de la APD"***	ESADE(Facultad de Derecho)
26-6-98	Madrid	Jornada sobre sistemas de Información en salud mental Exposición: ***"La Garantía de confidencilidad en los sistemas de información clínica)***	Consejería de Sanidad y Servicios Sociales
10-08-98	S. Lorenzo del Escorial	Jornadas sobre Intimidad y Asedio Informático Exposición: ***"La Agencia de Protección de Datos"***	Asociación Profesional de la Magistratura
1ª Semana de Sepbre.	Madrid	Conmemoración Revista AUSBANC nº 100 Artículo**:*"Contribución de Ausbanc a la garantía de la intimidad de los usuarios de los servicios bancarios*"**	Ausbanc
16-18/9-98	Santiago de Compost.	XX Conferencia Internacional de Autoridades de Protección de Datos Exposición: ***"El derecho a la privacidad y su frontera en los demás derechos humanos"***	Agencia de Protección de Datos
Octubre	Madrid	Presentación del Premio Protección de Datos Personal.Segunda edición	Agencia de Protección de Datos
30-10-98	Salamanca	TECNIMAP Mesa redonda **- "Seguridad y Garantías en la utilización de los TIC**	MAP
1/12/98	Madrid	Conferencia **. "El tratamiento automatizado y la transmisión de los datos personales y económicos en la operativa Bancaria y Financiera"**	AUSBANC
2/12/98	Barcelona	Universidad Autonoma de Barcelona. Conferencia: **"Principios que garantiza la LORTAD y funciones de la APD"**	U.A.B
9-10/12/98	Castellón	Jornadas sobre Informática y Derecho **"El proyecto de Ley Orgánica de modificación de la LORTAD"**	Universidad Jaume I

4. PARTICIPACIÓN EN DIVERSAS ACTIVIDADES DE ÁMBITO NACIONAL.

4.1. Subcomité ISO/IEC JTC 1/SC 27 - Information technology - Security Techniques

El Subcomité ISO/IEC JTC 1/SC 27 (en adelante, SC 27) forma parte del Comité Técnico de Normalización 71 (en adelante, CTN 71) de la organización internacional ISO/IEC (International Standards Organization/International Electrotechnical Comission). El ámbito de trabajo del CTN 71 son las Tecnologías de la Información, y dentro del mismo, el Subcomité SC 27 se especializa en las Técnicas de Seguridad de los sistemas basados en las Tecnologías de la Información. Por su especial interés en los aspectos relacionados con las medidas de seguridad aplicadas a los ficheros automatizados que contienen datos de carácter personal, a las que se refiere el artículo 9 de la Ley Orgánica 5/92 de 29 de octubre, la Agencia de Protección de Datos participa desde 1996, en las actividades de la sección española del subcomité SC-27, la cual está integrada por expertos pertenecientes a las principales empresas y entidades nacionales dedicadas a la seguridad de la información, tanto del sector privado como del sector público.
Las actividades generales que el subcomité desarrolla, se pueden resumir en los siguientes aspectos:

* 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).
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.
A lo largo del año 1998, han tenido lugar un total de siete reuniones plenarias de la sección española del subcomité SC 27.
Entre las habituales actividades de revisión, votación y análisis de normas y procedimientos elaborados en el seno del subcomité SC-27 a nivel internacional y de los que se presenta una relación en el Cuadro 1, cabe destacar las siguientes actividades desarrolladas en el seno de la sección española:

* **Preparación de la reunión internacional plenaria del Subcomité SC-27, en Madrid, del 19 al 23 de abril de 1999.**
Para la organización, elaboración de agendas de trabajo, disposición de centros de reunión, etc., la sección española del subcomité ha desarrollado a lo largo de 1998 una intensa actividad. Esta reunión cuenta con el apoyo de las organizaciones miembro de la sección española del subcomité, de las que algunas son patrocinadoras.

* **Propuesta de un nuevo proyecto de trabajo sobre fechado electrónico**
Los miembros de la sección española del subcomité SC-27 han propuesto un nuevo proyecto de trabajo relativo al fechado electrónico (time-stamping), con el objetivo de elaborar un estándar sobre este mecanismo, denominado "Time Stamping Services and Protocols". Esta propuesta tiene su origen en el proyecto PKITS (Public Key Infrastructure with Time Stamping Authority) del Programa INFOSEC-ETS II (European Trusted Services) de la Unión Europea, en el que participan el Ministerio de Administraciones Públicas, la Fábrica Nacional de Moneda y Timbre, el organismo empresarial Correos y Telégrafos y la Universidad Politécnica de Cataluña.

Grupo de Trabajo	**Norma Internacional** (DIS: Borrador de norma internacional)	**Título**
Grupo de Trabajo 1 (WG1) – Requisitos, Servicios de Seguridad y Directrices	ISO/IEC 13335 (13335-1,13335-2,13335-3)	Guidelines for de Management of IT Security Part 1. Concepts and models for IT Security Part 2. Managing and Planning IT Security Part 3. Techniques for the management of IT Security
	ISO/IEC 14980	Code of practice for information security management
Grupo de Trabajo 2 (WG2) – Técnicas y mecanismos de seguridad	ISO 8372	Information processing, modes of operation for a 64-bit block cipher algorithm
	ISO 9160	Information processing, Data encipherment, Physical Layer
	ISO/IEC 9796 (9796-2)	Digital signature schemes giving message recovery Part 2: Mechanisms using a hash function
	ISO/IEC 9797 ISO/IEC DIS 9797-I	Data integrity mechanism using a cryptographic check function employing a block cipher algorithm Message authentication codes, Part 1: Mechanism using a block cipher
	ISO/IEC 9798 9798-1, 9798-2 DIS 9798-3 9798-4 DIS 9798-5	Entity authentication Part 1: General Model Part 2: Mechanisms using symmetric encirphement algorithms Part 3: Mechanisms using digital signatures techniques Part 4: Mechanisms using a cryptographic check function Part 5: Mechanisms using zero Knowledge techniques
	ISO/IEC DIS 9979	Procedures for the registration of cryptograhic algorithms
	ISO/IEC 10116	Modes of operation for a n-bit block cipher algorittm
	ISO/IEC 10118 10118-1 10118-2 10118-3 DIS 10118-4	Hash functions Part 1: General Part 2: Hash-functions using a n-block cipher algorithm Part 3: Dedicated hash-functions Part 4: Hash functions using modular arithmetic
	ISO/IEC 11770 11770-1 11770-2 DIS 11770-3	Key management Part 1: Framework Part 2: Mechanisms using symmetric techniques Part 3: Mechanisms using asymmetric techniques
	ISO/IEC 13888 13888-1 13888-2 13888-3	Non-repudiation Part 1: General Part 2: Mechanisms using symmetric techniques Part 3: Mechanisms using asymmetric techniques

Cuadro 1. Normas desarrolladas por el subcomité ISO/IEC SC-27

MEMORIA DE 1998 - ANEXO I - COMPARECENCIA DEL DIRECTOR DE LA AGENCIA EN EL CONGRESO DE LOS DIPUTADOS.

Comparecencia del señor director de la Agencia de Protección de Datos (Fernández López) para informar sobre:
- Actuaciones de la Agencia de Protección de Datos en relación con las denuncias efectuadas contra la Compañía Telefónica de España, S. A., por pretender vender los datos de carácter personal de sus abonados sin contar con su consentimiento expreso. A solicitud del Grupo Parlamentario Mixto (Número de expediente 212/001174)
- Actuaciones que ha previsto llevar a cabo la Agencia de Protección de Datos ante la posible difusión por parte de Telefónica de datos personales de los usuarios de esta compañía con fines comerciales.
A solicitud del Grupo Parlamentario Mixto (Número de expediente 212/001180) .....
Sesión núm. 18 celebrada el miércoles, 27 de mayo de 1998
El señor PRESIDENTE: Como punto segundo del orden del día figura la comparecencia ante esta Comisión del magistrado don Juan Manuel Fernández López, director de la Agencia de Protección de Datos, a petición propia, para informar sobre la situación y orientación de la actuación futura como director del citado órgano, pero sobre ella se acumulan tres peticiones de comparecencia, todas ellas emanadas del Grupo Mixto. Concretamente se trata de una solicitud para informar de las actuaciones de la Agencia de Protección de Datos en relación con las denuncias efectuadas contra la Compañía Telefónica Nacional de España, S. A., por pretender vender los datos de carácter personal de sus abonados sin contar con su consentimiento expreso, suscrita por los portavoces del Grupo Mixto los señores Saura y Alcaraz. Otra versa sobre el mismo objeto, suscrita por los portavoces del Grupo Mixto el señor diputado don Francisco Rodríguez y la señora diputada doña Begoña Lasagabaster; y una tercera sobre objeto distinto, solicitud de comparecencia para informar de las líneas generales, es decir, en este sentido redundante con la petición a solicitud del director, pero con mención específica de las actuaciones que piensa llevar en relación con la cesión por el Ministerio de Defensa a la empresa que resulte adjudicataria del concurso para la campaña publicitaria de tropa profesional de un listado con los nombres y direcciones de dos millones de jóvenes españoles en soporte informático, suscrita por los portavoces del Grupo Mixto el señor Alcaraz Ramos y la señora Rivadulla Gràcia.
En primer término parece de cortesía obligada, tras reproducir las disculpas por las circunstancias determinantes de la demora, que en nombre de la Comisión demos la bienvenida a don Juan Manuel Fernández López, quien desde el pasado 3 de abril titulariza la dirección de la Agencia de Protección de Datos. Pongo en conocimiento de SS. SS. que el señor Fernández López pertenece a la carrera judicial con la categoría de magistrado; fue vocal del Tribunal de Defensa de la Competencia, primero, y después vicepresidente; es profesor de Derecho mercantil de la Universidad Complutense de Madrid; por encargo del Consejo General del Poder Judicial ha desempeñado y dirigido distintos cursos de especialización en materia de propiedad industrial y competencia desleal y Derecho comunitario europeo; tiene numerosas publicaciones en el ámbito específico del Derecho mercantil, numerosas monografías y artículos en revistas especializadas; es miembro de la Asociación Internacional para la Protección de la Propiedad Industrial, vicepresidente del Instituto de Derecho y Ética Industrial y académico de la Real Academia de Jurisprudencia y Legislación. Éste es el holgado currículum académico y profesional con el que el señor Fernández López accede a la dirección de la Agencia de Protección de Datos.
Me parece obligado en este punto también, aunque ya lo hiciéramos con ocasión de su última comparecencia, reiterar nuestro reconocimiento y gratitud hacia su predecesor, el señor Martín Casallo, que tan fluidas y cordiales relaciones mantuvo con la Cámara a través del vehículo de esta Comisión ante la que figuraba como compareciente habitual, como estamos seguros de que lo será en lo sucesivo el señor Fernández López. Quiero reiterarle mi bienvenida a esta Comisión y advertirle que el formato tradicional de este tipo de comparecencias por uso o costumbre parlamentario, con independencia de que se produzca, como en este caso, la acumulación de distintas iniciativas, suele comenzar por una exposición inicial del señor compareciente y después los grupos, empezando por aquellos que tienen específicamente solicitada la comparecencia, piden la palabra e intervienen sobre la misma. Naturalmente esto queda al arbitrio del propio señor director. Si prefiere prescindir de esa exposición inicial y pasar directamente a que se explayen los portavoces de los grupos en sus peticiones de comparecencia está en su ámbito de disposición, pero, insisto, el formato tradicional es que la sesión comience por una exposición inicial. (Asentimiento.)
En tal sentido, y a la vista de los signos de asentimiento, don Juan Manuel Fernández López, director de la Agencia de Protección de Datos, tiene la palabra.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor presidente. Señorías, es para mí un gran honor, al mismo tiempo que una gran satisfacción, poder comparecer hoy ante la Comisión Constitucional del Congreso de los Diputados. De ahí que mis primeras palabras sean de agradecimiento hacia SS. SS. que han posibilitado que hoy me encuentre aquí, porque ello supone, señorías, que la Agencia de Protección de Datos sea reconocida como un órgano protector de derechos constitucionales. Una de mis primeras intenciones al tomar posesión del cargo de director de la Agencia ha sido comparecer ante la Cámara para informar sobre la situación de la misma y la orientación actual y futura, que haré a continuación después de responder a las preguntas concretas que me formula el Grupo Mixto, siguiendo el orden del día.
Respondiendo a las solicitudes del Grupo Mixto relativas a la utilización comercial por Telefónica de datos personales sin contar con el consentimiento expreso de los afectados y las actuaciones previstas por la Agencia de Protección de Datos, he de significar lo siguiente. Ya en el año 1996, ante varias denuncias en las que se pone de manifiesto haber recibido propaganda en sus nuevos domicilios por los afectados, propaganda procedente de diversas entidades conteniendo sus datos personales que habían sido cedidos por la filial de Telefónica Telefónica Publicidad e Información, a través del producto Coditel, se abre un procedimiento en la Agencia de Protección de Datos contra Telefónica de España por cesión de datos a su filial TPI, por tratamiento de datos sin consentimiento por parte de TPI y por cesión de datos por TPI a terceros. Se declaran probados la cesión de datos de Telefónica a TPI como también el tratamiento y posterior cesión de estos datos a terceros, a empresas para realizar campañas de marketing. Por resolución de 6 de junio de 1997 se sanciona a Telefónica de España con 50.000.001 pesetas por cesión de los datos a TPI. Se sanciona también a TPI con 10.000.001 pesetas por tratamiento de datos sin consentimiento de los afectados y se sanciona con

50.000.001 pesetas a TPI por cesión de datos a terceros. Posteriormente, en 1997 varias denuncias de ciudadanos manifiestan no estar de acuerdo en la forma en que Telefónica de España estaba procediendo a recabar el consentimiento de los abonados para proceder a la cesión de sus datos a otras empresas del grupo; esto se refiere a la primera circular de Telefónica.
Se acuerda la apertura del procedimiento por cesión de datos de Telefónica a terceros y por falta de información en la recogida de esos datos. Se declaran probados tanto la cesión como la falta de información en la recogida de datos.
Por resolución de 3 de abril de 1998 -ya firmada por mí- se sanciona a Telefónica con 30 millones de pesetas por falta de información en la recogida de datos y no se le sanciona por la cesión de datos al habérsele impuesto ya sanción por este motivo en el anterior expediente al que he hecho referencia. Por una sola denuncia en que el afectado dice que se han utilizado sus datos personales para publicidad, después de haber solicitado expresamente que no fueran utilizados para esta finalidad, se abre un nuevo procedimiento sancionador contra Telefónica por tratamiento de datos sin el consentimiento del afectado. Se declara como hecho probado el tratamiento sin consentimiento y por resolución de 11 de este mes se sanciona a Telefónica en la cuantía de 10.000.001 pesetas. Hay abierto otro procedimiento por dos denuncias por no haber proporcionado TPI -la filial de Telefónica- toda la información sobre el derecho de acceso. Al parecer, informan que tienen determinados datos pero no todos. Se acuerda la apertura del procedimiento y está pendiente aún de ser resuelto. También de oficio se abre otro procedimiento a Telefónica que remitió a sus abonados una circular informativa solicitando su consentimiento para la cesión de datos a empresas del grupo y a terceros. Se ha acordado la apertura del procedimiento por falta de información para la cesión de datos y está todavía pendiente de ser resuelto. Como consecuencia de todas estas actuaciones, además de las sanciones que ya he relatado a SS. SS., Telefónica ha comunicado a sus abonados que no va a ceder los datos a terceros.
(Un señor diputado: Los ha cedido.) Por su parte, TPI comunica a la Agencia de Protección de Datos la destrucción de sus ficheros y los ha dado de baja. Finalmente, se han abierto unas diligencias informativas de oficio a Telefónica ante la noticia aparecida en la prensa de la posible fuga de datos de abonados que aparecieron publicados en el diario *Egin*. Estamos investigando este asunto y aún no tenemos ninguna solución al respecto. Ésta es, señorías, la actuación de la Agencia de Protección de Datos en el asunto que han sometido a mi información. Posteriormente, con mucho gusto aclararé o concretaré cualquier dato que deseen sus señorías.
En cuanto a la petición del Grupo Parlamentario Mixto para que informe sobre la cesión por el Ministerio de Defensa a la empresa que resulte adjudicataria del concurso para la campaña publicitaria de tropa profesional de un listado con los nombres y direcciones de dos millones de jóvenes en soporte informático, he de informar lo siguiente.
Habiendo sido nombrado director de la Agencia de Protección de Datos y antes de tomar posesión del cargo, apareció en la prensa una noticia referida al objeto de la pregunta que hoy se me formula. Toda vez que el anterior director ya había cesado y pese a no haber tomado yo posesión, entendí que debía, no obstante, intervenir de inmediato para comprobar el alcance de dicha información, lo que hice el mismo día poniéndome al habla con el señor subsecretario del Ministerio de Defensa. Recibí información de que se pensaba llevar adelante una campaña publicitaria para informar del acceso a la categoría de tropa profesional, una amplia campaña que comprendía no sólo la confección y distribución del *mailing* sino también anuncios en prensa y en televisión, manifestándome el señor subsecretario de Defensa la disposición de aquel departamento para cumplir en todo con la legalidad, por lo que tenían decidido realizar una consulta por escrito a la Agencia de Protección de Datos. En dos ocasiones se ha dirigido el Ministerio de Defensa a la Agencia, que ha respondido a sus consultas en fechas 3 y 22 del pasado mes de abril. En definitiva, señorías, el mayor problema no resulta tanto de la entrega del fichero a un tercero para la prestación de un servicio, ya que ello es posible sin consentimiento del afectado siempre que no se cedan los datos a terceros ajenos al contrato, que se destruyan los datos una vez prestado el servicio y que no se apliquen a fin distinto del que figura en el contrato de servicios. Estas exigencias podían cumplirse en el contrato administrativo a suscribir con la agencia de publicidad. Pero el problema principal, señorías, está en si los datos que se recaban para una concreta finalidad, en este caso el reclutamiento, pueden ser utilizados por el responsable del fichero directa o indirectamente para una finalidad distinta de la que permitió recabar los datos y tratarlos informatizadamente,
lo cual, señorías, está prohibido por el artículo 4.2 de la Ley Orgánica de Protecciónde Datos. Estas consultas administrativas y de entidades privadas que se reciben habitualmente en la Agencia y que pueden resultar ser objeto de un procedimiento sancionador venían siendo, hasta ahora, respondidas directamente por el director. Entiendo que en situaciones como ésta se podía estar prejuzgando y la potestad sancionadora pudiera quedar implicada al evacuar estas consultas. Por ello, sin desatender a las mismas, he decidido que en la etapa en que me corresponde dirigir la Agencia las mismas sean evacuadas por los servicios jurídicos de la Agencia, dejando a salvo las potestades que la ley atribuye al director, entre las que no figura el evacuar este tipo de consultas. Se han recibido también en la Agencia escritos relacionados con el asunto: por un lado, del Partido Democrático de Nueva Izquierda, instando las actuaciones oportunas para evitar la operación de cesión y, por otro, de la Plataforma de opinión reivindicativa, una asociación de consumidores, en los que se denuncian posibles infracciones de la Ley Orgánica de Protección de Datos. Una tercera comunicación se ha recibido del Defensor del Pueblo, en la que, dentro de sus facultades institucionales, solicita informes sobre las actuaciones realizadas por la Agencia de Protección de Datos en este asunto. Se recibió el día 6 de este mes y el día 7 se ha dado respuesta al Defensor del Pueblo dándole traslado de los escritos que se han dirigido al Ministerio de Defensa.
Pasando a informar sobre la situación de la Agencia de Protección de Datos y las líneas de actuación futuras que como director de la misma pienso seguir, he de decirles, señorías, que la Ley Orgánica 5/1992, de Regulación del tratamiento automatizado de los datos de carácter personal, en desarrollo del artículo 18.4 de la Constitución, tiene por objeto limitar el uso de la informática y otros medios de tratamiento automatizado de datos de carácter personal para garantizar la privacidad de las personas físicas, como de sobra conocen SS. SS. Por ello se crea la Agencia de Protección de Datos. En el corto tiempo de funcionamiento de la Agencia, puesto que fue creada por Real Decreto 428 de 1993 y empezó a funcionar en el año 1994, la labor desarrollada ha sido, a mi juicio, muy importante. El primer objetivo de la Agencia fue la inscripción de ficheros automatizados tanto de titularidad pública como privada. A este respecto, al día de hoy hay 230.990 ficheros inscritos, de los cuales 28.359 son de titularidad pública y 202.631 de titularidad privada. Debo rectificar porque los datos los he referido a hoy y son al día de ayer, porque hoy, en este momento, posiblemente estos datos ya hayan cambiado por nuevas inscripciones. Además de la inscripción, estos ficheros se modifican, se dan de

baja y se sustituyen por otros; de aquí que la Agencia de Protección de datos tramite anualmente entre 4.000 y 5.000 altas, de 3.000 a 4.000 modificaciones y unas mil bajas. Ante el desconocimiento de la ley, se han hecho campañas sectoriales para informar de la obligatoriedad de la inscripción, prestando apoyo y resolviendo consultas y dudas tanto a entidades públicas como privadas, siendo éstas más significativas en la Administración local.
Como unidad especialmente relevante dentro de la Agencia está el área de atención al ciudadano, que se viene ocupando tanto de evacuar las consultas que aquellos formulan como de divulgar el conocimiento de la ley y los derechos que la misma ampara. Se reciben consultas telefónicas, presenciales de los ciudadanos y por escrito: unas 8.000 consultas telefónicas, que pueden convertirse en 12.000 este año; presenciales, 1.200 referidas a 1996 y 1.400 como perspectiva para este año; y por escrito, donde el aumento es mayor, 600 fueron recibidas en 1996, 1.009 en el año 1997 y se espera alcanzar las 1.800 en este año. Para dar cumplimiento a la ley, un órgano indispensable para la Agencia es la unidad de inspección.
Se ocupa de comprobar en la práctica, mediante las oportunas revisiones *in situ,* que los tratamientos que realizan los responsables de los ficheros automatizados se ajustan a la legalidad. Dada la especialidad de la materia y las dificultades que comporta la labor inspectora, los encargados de este cometido son en su mayoría especialistas altamente cualificados en las tecnologías informáticas.
Los dos grandes bloques de inspección son: actuaciones de oficio, atendiendo en su mayoría a planificación sectorial, o por denuncias concretas de los ciudadanos.
Los expedientes tramitados por la inspección han ido en lógico crecimiento, desde 87 en el año 1994 a 682 en 1997 y 246 en lo que va transcurrido de este año. A este respecto, es de significar que mientras en países de desarrollo tecnológico alto y de gran protección a los derechos fundamentales se han realizado tres inspecciones en un período de tiempo, la Agencia de Protección de Datos ha llegado a 375 en el mismo período. Así lo pude comprobar y poner de manifiesto en la reunión de las autoridades de protección de datos europeas, celebrada en Dublín el pasado mes de abril. Como consecuencia de la labor inspectora se han abierto procedimientos sancionadores a aquellos en los que se comprueba, en principio, indicios de infracción. Las cifras han ido creciendo desde los cuatro procedimientos que se abrieron en 1994 hasta los 202 en 1997. En el presente año y al día de la fecha hay abiertos 53 procedimientos sancionadores. Las sanciones impuestas sobrepasan los 2.000 millones de pesetas.
Asimismo se han tramitado, en cifra también creciente, 113 procedimientos de tutelas de derechos en 1997 y en lo que va de año 75.

La Agencia ha dado cumplimiento a la obligación de informar los proyectos de disposiciones generales que desarrollan o inciden en la Ley Orgánica de Protección de Datos y que han sido sometidos a su consideración, evacuando el año pasado 20 informes al respecto. Por obligaciones derivadas de nuestra pertenencia a la Unión Europea principalmente y por otras señaladas en la propia ley, la Agencia de Protección de Datos mantiene su presencia activa en la autoridad de control común de Schengen, en el grupo de trabajo del artículo 29 de la Directiva 46 de 1995, en el Consejo de Europa en el convenio 108 y en el grupo Europol, derivado del convenio Europol firmado y ratificado por España, como conocen sus señorías. La Agencia participa también en los grupos de trabajo creados por las propias autoridades de control de la Unión Europea. Así, en el grupo Berlín o grupo IWG, según sus siglas inglesas, que se ocupa del sector de las telecomunicaciones, en el grupo de protección de datos en materia de crédito al consumo y en el recientemente formado para el estudio de la protección de datos en los sistemas de reservas aéreas. En el marco de la cooperación internacional, que el artículo 36.1 de la ley orgánica atribuye a la Agencia, ésta está presente en la conferencia anual de protección de datos de la Unión Europea y en la conferencia anual de autoridades de protección de datos mundiales.
Éstas son, señorías, las principales actividades de la Agencia de Protección de Datos y su situación actual.
De cara al futuro son prioridades de este director de la Agencia de Protección de Datos las siguientes. Una. En cuanto a temas legislativos, la trasposición de la Directiva 46, del año 1995, del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en el tratamiento de datos personales y la libre circulación de éstos. La Agencia de Protección de Datos ya informó en el mes de febrero pasado sobre un primer borrador de anteproyecto; uno nuevo se ha sometido a informe de la Agencia a petición mía y en él se trabaja actualmente. Entiendo, señorías, que toda vez que la trasposición ha de suponer la modificación de la ley orgánica debería aprovecharse la ocasión para introducir algunas reformas puntuales que la práctica durante estos años aconseja. Así, por ejemplo, ampliar las definiciones del artículo 3 a los conceptos de cesión y encargado de tratamiento, regular el derecho de oposición y el de subrogación en la titularidad del fichero, flexibilizar la determinación de la cuantía de las multas, pudiendo conllevar éstas la publicación de la resolución como sanción adicional, lo que sirve para ejemplarizar y además para dar a conocer a los ciudadanos las posibilidades que les ofrece la ley.
Dos. Para un efectivo cumplimiento de la ley es preciso que los responsables de los ficheros adopten medidas de seguridad apropiadas. Hasta ahora no se ha desarrollado el artículo 9 de la ley, en el que se prevé un reglamento de medidas de seguridad. La Agencia ha participado muy activamente en la elaboración del anteproyecto de reglamento que desarrolla estas medidas y que está a punto de ser sometido para su aprobación al Consejo de Ministros.
Prioridad de la Agencia ha de ser informar de las exigencias que este reglamento comporte a los responsables del fichero para que al finalizar la fecha de adaptación todos hayan adoptado las medidas de seguridad acordes con la naturaleza de los datos. Los períodos de adaptación que prevé la ley van de seis meses a un año, dependiendo del tipo de medidas de seguridad, que a su vez está en relación con el tipo de datos más sensibles o no que se guarde en el fichero. Se distinguen así tres niveles de seguridad: básico, medio y alto. El básico ha de ser cumplido por todos; el medio se refiere a aquellos ficheros de solvencia patrimonial y de crédito que contengan también datos de infracciones administrativas, Hacienda pública, servicios financieros; y el nivel alto es para todos aquellos que contengan datos especialmente protegidos, es decir, aquellos referidos a la ideología, religión y creencias, origen racial, salud o vida sexual y los recabados con fines policiales sin consentimiento del afectado. Las medidas de seguridad que prevé el reglamento son diversas, tanto técnicas como organizativas, y su rigor es mayor según el grado de protección mayor que requieren los datos.
Tres. Entiendo que, aunque puede pensarse que el artículo 36.h) de la Ley Orgánica de Protección de Datos no exige el informe preceptivo de la Agencia más que en las disposiciones generales que desarrolle la misma, el espíritu de la

norma y las exigencias de racionalidad legislativa determinan que la Agencia pueda y deba informar normativas sectoriales que afectan a la protección de datos. Sirvan de ejemplo, señorías, las recientes leyes de condiciones generales de la contratación y la Ley de Telecomunicaciones.
Por ello he realizado las gestiones pertinentes en el Ministerio de Justicia para poder tener información y manifestar el criterio de la Agencia sobre cualquier disposición de carácter general que afecte directa o indirectamente a la protección de datos. A este respecto es de destacar que habrá que trasponer a nuestro derecho interno la Directiva 66, de 1997, relativa al tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.
Destaca en esta directiva el derecho que reconoce su artículo 7 a los abonados a recibir facturas no desglosadas y establece que cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante el que origine la llamada deberá poder suprimir, mediante un procedimiento sencillo y gratuito, la identificación de la citada línea llamante. La directiva exige también que los datos personales que se contengan en las guías telefónicas se limiten a lo estrictamente necesario para identificar a un abonado, quien tendrá derecho de forma gratuita a que se le excluya de una guía impresa o electrónica. Asimismo se le reconoce el derecho a indicar que sus datos personales no se utilicen para fines de venta directa, a que se omita parcialmente su dirección y a que no exista referencia que revele su sexo. También cabe destacar que las llamadas automáticas o de fax con fines de venta directa sólo se podrán hacer respecto de aquellos abonados que hayan dado su consentimiento previo.
Cuatro. A pesar de la labor desarrollada hasta ahora por la Agencia, entiendo que, dado lo relativamente reciente de la ley, no es suficientemente conocida por los ciudadanos a los que ampara ni por las entidades públicas y privadas que deben cumplirla. Hay las siguientes líneas de actuación: Cuatro, uno. Potenciar el servicio de atención al ciudadano. Para saber el grado de conocimiento de la ley por parte de los ciudadanos, estamos estudiando la posibilidad de que realice una encuesta el Centro de Investigaciones Sociológicas. Cuatro, dos. Llevar a cabo una campaña de publicidad, dentro de los límites presupuestarios de la Agencia, insertando anuncios en periódicos y prensa sectorial. También, la presentación pública de nuestra memoria anual. Cuatro, tres. Participación y organización de seminarios, jornadas y cursillos para los sectores empresariales y administraciones públicas, en particular para las corporaciones locales. Cuatro, cuatro. Publicaciones específicas de la Agencia, divulgativas de las exigencias de la AEI, en particular en el ámbito de las nuevas tecnologías y de los derechos de los ciudadanos en este campo.
Cinco. Otra de mis prioridades es estimular la adopción de códigos tipo de carácter sectorial que, de un lado, potencien la protección del ciudadano y, de otro, fijen para los gestores de datos de un mismo sector empresarial un marco jurídico conforme con la ley, facilitando así su mejor cumplimiento. En este momento se trabaja con la Asociación Española de Marketing Directo en la confección de un código deontológico para actividades de venta y promoción por medio de Internet.
Seis. Coordinación con otras instituciones, en especial con el Defensor del Pueblo, que también recibe quejas sobre incumplimiento de la ley, cuyo artículo 45.4 obliga al director de la Agencia a comunicar las infracciones que puedan cometer las administraciones públicas.
Siete. Planes de inspección. Habiéndose realizado la inspección sectorial de los ficheros y hospitales públicos, Fuerzas y Cuerpos de Seguridad, tanto del Estado como autonómicos y locales, y las estadísticas de las comunidades autónomas, se lleva a cabo en la actualidad o está programada para un futuro inmediato la revisión del sistema Schengen en España, de las salas de juego, del sector de las telecomunicaciones, el de la solvencia patrimonial, también del sector del seguro y los grandes ficheros públicos, en especial el de la Agencia Tributaria y el de la Seguridad Social.
Ocho. Otra de mis líneas de actuación es la aplicación estricta de la ley a los infractores, en especial a los reincidentes. Si bien lo deseable en un futuro es que el grado de cumplimiento de la ley haga disminuir el número de estos procedimientos hoy por hoy crecientes, la realidad es que van en aumento. La sanción, señorías, es, en cierto modo, el fracaso del Derecho, pero la sanción también es un medio de defensa del Estado de Derecho.
Nueve. Para el desarrollo de las funciones del director de la Agencia de Protección de Datos, la ley ha previsto un comité consultivo como órgano de asesoramiento, en el que están representados los principales estamentos de la sociedad: Congreso, Senado, universidades, administraciones central, autonómica y local, Real Academia de la Historia, Consejo de Consumidores y Consejo Superior de Cámaras. La primera sesión, desde mi toma de posesión, tuvo lugar el pasado día 20 de los corrientes, con un apretado orden del día. Pienso estimular en la medida de lo posible el funcionamiento del consejo consultivo, que en la primera reunión se ha mostrado seriamente interesado con los temas sometidos a consideración y del que he recibido un apoyo importante, que agradezco.
Diez. Asimismo, la Agencia de Protección de Datos ha de continuar presente en los foros internacionales antes referidos, en los que viene obligada a participar. A este respecto, es de destacar que la Agencia española ha sido encargada de organizar la XX Conferencia internacional de autoridades de protección de datos, que tendrá lugar en Santiago de Compostela del 16 al 18 de septiembre próximo.
En la misma participan las autoridades de control de datos de todo el mundo y unos ochenta observadores. Tenemos elaborado el programa provisional y SS. SS. quedan invitados a asistir a este evento, al que sin duda prestigiarán con su presencia. A través del señor presidente, haré llegar a SS. SS. el programa definitivo.
Lo que he enunciado son, inicialmente, las líneas generales de las tareas que he identificado como prioritarias en el corto espacio transcurrido al frente de la Agencia de Protección de Datos.
Estoy abierto a las sugerencias que SS. SS. puedan formularme al respecto y quedo a su disposición para contestar o cumplimentar cualquier extremo relacionado con las mismas.
El señor PRESIDENTE: Muchas gracias, señor Fernández López, tanto por su cumplida información como por ese ofrecimiento final general de mantener abiertos los cauces para la más fluida colaboración con el Parlamento por medio de esta comisión.
En un turno general de portavoces y dando la palabra en primer término a los solicitantes específicos de la comparecencia, el señor Alcaraz Ramos tiene la palabra.
El señor ALCARAZ RAMOS: Lógicamente, las primeras palabras como portavoz de Nueva IzquierdaIniciativa per Catalunya deben ser para felicitar al señor Fernández López por su reciente nombramiento, como creo que también es de justicia hacer un recordatorio aquí a la labor desarrollada por el señor Martín Casallo en la época anterior.
Quiero decir al señor Fernández López que creemos que ha empezado con buen pie. Valoramos muy positivamente que, con independencia de que se encontrara algunas solicitudes de comparecencia, se haya adelantado pidiendo

usted mismo comparecer. Creo que esto es algo que siempre es de agradecer. Además, también he de decirle que cuenta con nuestro apoyo en las líneas que ha expuesto al final de su intervención; nos parecen las sensatas, las adecuadas, las razonables y las positivas. Por tanto, creo que, como digo, ha empezado con buen pie y estamos convencidos de que ésta va a ser la dinámica general de lo que quede de legislatura.
Unificando en mi intervención las dos comparecencias que nosotros pedíamos sobre Telefónica y Defensa, más alguna breve alusión a los otros temas que el señor Fernández ha introducido, trataré de ser bastante breve.
En cuanto a la cuestión de Telefónica, después de lo indicado, creo que la relevancia del concepto del consentimiento expresó más todo lo que se dispone en el artículo 11 de la Lortad ha quedado bien reflejado en las actuaciones que se nos han explicado, con independencia de todas aquellas que siguen abiertas, como se ha dicho.
Esto también nos tranquiliza porque en el momento en que surgió el problema hubo alguna discrepancia, al menos aparente, que llegó a los medios de comunicación, entre el Defensor del Pueblo y el anterior presidente de la Agencia de Protección de Datos, que podía ser un elemento de inquietud que entiendo que ahora queda solventado.
Por lo tanto, nos congratulamos por la acción de la Agencia. Cabe una reflexión, que no sé si el señor Fernández compartirá, sobre lo que sucede en casos como el de Telefónica, grandes empresas que han funcionado en régimen de monopolio y que los ciudadanos han tenido inevitablemente que cederles una serie de datos personales, de los que luego se hace un mal uso. Debería ser un tema para reflexionar. Mi primera pregunta es si el señor Fernández entiende, como presidente de la Agencia, que los datos obtenidos por empresas que han funcionado en régimen de monopolio deben tener un tratamiento de especial protección. Aquí cabe una pregunta más concreta y, si se quiere, más en el ámbito de lo subjetivo, que es cómo valora esta reincidencia en las infracciones de Telefónica.
Porque la impresión que da es que a Telefónica no le preocupa demasiado que le sancione la Agencia, lo que nos conduciría a una pregunta sobre si es necesario algún tipo de modificación en relación con las sanciones a empresas de esta magnitud, a las que se les imponen multas objetivamente importantes pero que, sin embargo, parece que no les hacen ni siquiera cosquillas. Es una actitud francamente vergonzosa la de la Telefónica y la de esa filial, la TPI, que -si me lo permiten SS. SS.- parece las iniciales de *Telefónica Piratas Informáticos. En resumen, la pregunta es si considera suficiente la normativa vigente y, en su caso, qué modificaciones propondría. Al hilo de lo anterior, también cabría hacer una reflexión sobre cómo se puede asegurar que el ciudadano titular de los datos protegidos tenga un dominio permanente sobre dichos datos, sin estar expuesto continuamente a la duda sobre el concepto de consentimientos presuntos o mecanismos similares.*
Entrando en la siguiente cuestión, sobre actuaciones realizadas o que piensa llevar a cabo en relación con la cesión por el Ministerio de Defensa de datos relativos a dos millones de ciudadanos españoles de entre 18 y 24 años, potenciales aspirantes a soldado profesional, debo agradecerle ante todo la mención expresa que usted ha hecho del Partido Democrático de la Nueva Izquierda, que -como ha dicho- se preocupó directamente de esta cuestión, que parece extraordinariamente grave. Como una consideración puramente pragmática, a nadie se nos oculta que disponer de datos de esa franja de edad es un bocado muy apetitoso para cualquier empresa. Hay que recordar -relacionándolo con el artículo 27 de la Lortad- que los datos, en este caso, no son obtenidos por el Ministerio de Defensa, sino por los entes reclutadores, fundamentalmente consulados y sobre todo ayuntamientos, que realizan una actividad previa al reclutamiento, para que, luego, el Ministerio de Defensa, con la tropa y la marinería, desarrolle las actividades de encuadramientos, sorteos, etcétera, y que son datos que se obtienen por estas entidades con una finalidad concreta, que es la prestación del servicio militar y no cualquier otra, aunque esté conectada con el Ministerio de Defensa. Nuestra interpretación es que se produce una ilegalidad absoluta cuando se dirigen a una campaña que no tiene que ver en sí misma con el fin para el cual se recaban esos datos.
En esta línea, usted ha indicado -y me gustaría que opinara sobre esta apreciación que yo hago ahora- que ha tenido diversos contactos con el Ministerio de Defensa y quisiéramos que valorara si la colaboración recibida hasta ahora del Ministerio ha sido suficiente. También nos gustaría -si se atreve o si está en condiciones- que nos aclarara cuándo va a finalizar el procedimiento de estudio de este problema.
Sobre los análisis generales que usted hacía en su programa de actuación, unas breves pinceladas. Obviamente, ha hecho alusión a la necesidad de urgente trasposición de la Directiva 46/95 de la Comunidad Económica Europea.
Si no recuerdo mal en este momento -y cito de memoria-, la fecha tope para la trasposición debería ser octubre de 1998, pero ya podemos decir que, en sede parlamentaria, será imposible, que difícilmente podremos tramitarlo para esa fecha. ¿Cómo valora usted ese posible retraso?
Usted ha hablado de dos anteproyectos -según parece- del Gobierno y nos gustaría que -si está en condiciones de hacerlo- nos diera su opinión sobre cuándo podría realmentecomenzar la tramitación parlamentaria y, por tanto, si estaremos en condiciones de llevar a buen puerto la trasposición para octubre de 1998 o, en su caso, en qué fecha aproximada.
Se ha referido usted también a la Directiva 66/97 y, en concreto, a un tema que nos preocupa especialmente: las referencias que se hacen en ella al tratamiento de las llamadas telefónicas en la red digital de servicios integrados, que impide preservar la identidad de quien realiza una llamada.
En el momento actual, las empresas que prestan este servicio en España se están negando, en principio, a cumplir -digamos- el espíritu de una directiva, aunque no haya sido traspuesta, y en este sentido -donde efectivamente hay algo más de plazo- he creído entender que usted también considera urgente la trasposición de dicha directiva.
Aquí la pregunta es si tiene conocimiento (entiéndase oficial, porque le haya sido remitido en función de la necesidad del informe preceptivo de la Agencia, etcétera) de que el Gobierno disponga ya de un anteproyecto en la materia.
Finalmente, dos preguntas. Una -aunque ha hecho alusión de pasada-, relativa al grado de satisfacción del cumplimiento de la ley, en sus diversos aspectos, por parte de los entes locales y de las Fuerzas y Cuerpos de Seguridad del Estado. La última, de rigor -que seguramente no será preciso siquiera contestar si contesta alguna de las que anteriormente le formulaba- es qué propuestas haría el director, incluso de orden legislativo, para el mejor funcionamiento de la Agencia.
Nada más. Le reitero la felicitación y la satisfacción de Nueva IzquierdaIniciativa per Catalunya por la celeridad con que usted ha comparecido y por las ideas que, en términos generales, ha expuesto.
El señor PRESIDENTE: Señor compareciente.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Señor Alcaraz Ramos, ante

todo, quiero agradecer su apoyo y su ofrecimiento. Respondiendo concretamente a sus preguntas, he de decirle que sí entiendo que las empresas que, como Telefónica, están sometidas a un monopolio tendrían que tener un tratamiento especial. Y creo que la ley no se lo da. Es evidente que una empresa que tiene esos datos (y que además dispone de ellos desde hace mucho tiempo, puesto que era la única a la que podíamos dar esos datos si queríamos tener servicio telefónico) ha gozado de una situación de privilegio.

Pienso que la solución es la inspección. Usted ha dicho una cosa que efectivamente comparto y es que es posible que las multas que impongamos a Telefónica no le afecten en gran medida o, dicho en otros términos, que le puede resultar barato el infringir. A este respecto, quiero decir que, en el estudio que está haciendo la Agencia del anteproyecto de trasposición de la directiva, una de las propuestas es que las multas puedan llegar hasta el 10 por ciento de la cifra de facturación de las empresas, en términos similares a lo que ocurre en la Ley de defensa de la competencia, con lo cual es seguro que a este tipo de empresas el infringir ya no les va a salir barato. Ésta es una de las modificaciones que personalmente propongo, una mayor flexibilización de las multas; por ejemplo, creo que en los tramos medios, entre 10 millones y 50 millones de pesetas, son demasiado rigurosas, puesto que se puede considerar infracción sólo porque haya habido un retraso en el cambio de los datos. Otra, una mayor cuantificación, hasta el límite del 10 por ciento de la cifra de facturación. Por otro lado, me parece que un medio adecuado es -como decía antes- obligar, como una sanción más, a dar publicidad a las resoluciones que dicte la Agencia, de forma que sirvan como ejemplo y, también, para que los ciudadanos conozcan las posibilidades que la Ley y la Agencia les facilitan.

Me ha preguntado también cómo pueden los ciudadanos tener dominio de sus datos sin el consentimiento presunto y si debe exigirse un consentimiento explícito. Hay distintas formas de dar el consentimiento, no necesariamente tiene que ser expreso, pero sí, a mi modo de ver, tiene que prestarse de una forma clara, informada. A este respecto, hay un tema preocupante porque podía dejar a las empresas del sector del marketing y de la publicidad en nuestro país en situación peor que sus homólogas en los países de la Unión Europea, donde pueden tener más facilidad de acceso a este tipo de datos que se obtienen de los padrones y que sólo en el momento en que el ciudadano dice que no quiere recibir publicidad se puede negar a ello. La realidad es que en el resto de los países europeos estas empresas están trabajando con datos accesibles al público y tal vez que no puedan hacerlo en nuestro país determinará que lo hagan desde Holanda, con la pérdida de los correspondientes puestos de trabajo en nuestro país.

En cuanto al tema de Defensa, como usted muy bien ha dicho, señor Alcaraz, lo importante es que los datos se obtienen para el reclutamiento. La noticia que salió en prensa hablaba de que el problema era que se cedían a una empresa para su tratamiento informático. Si ese tratamiento informático la empresa lo hace por su cuenta, con los debidos rigores, y luego se destruyen los datos, no hay ningún problema; el problema es que defensa obtiene los datos para el reclutamiento y, como señala nuestro artículo 4.2 de la ley orgánica, no pueden ser utilizados para otra finalidad distinta. Ahí está el problema. La colaboración que he recibido del Ministerio de Defensa tengo que decir que ha sido ejemplar. Desde el primer momento el subsecretario atendió mi petición de información, información que nos ha dado en todo momento. Se han remitido dos informes por parte de la Agencia y parece ser que no se ha llevado a cabo esta campaña, que se han atendido las opiniones que al respecto ha manifestado la Agencia sobre este asunto.

La trasposición de la directiva de 1995, cuyo plazo, como bien ha señalado S. S., finaliza en el mes de octubre, evidentemente es imposible. A mí tampoco me preocupa. ¿Qué directiva y qué país la traspone en el tiempo? La realidad es que prácticamente ninguno. En cualquier caso, lo que hay que hacer es trasponerla pronto y de forma eficaz.

A este respecto, también puedo informar a S. S. que toda vez que nuestra ley orgánica, cuando fue redactada, tuvo en cuenta la entonces propuesta de directiva, las adaptaciones que tenemos que hacer a la propia directiva son pequeñas. Si quiere, a mí lo que más me preocupa en este momento son las reformas puntuales que, aprovechando que se va a trasponer la directiva, se pueden introducir en la ley del tenor de algunas de la que he señalado. Los demás países de la Unión Europea, excepto Italia, no tienen traspuesta la directiva. Italia la tiene traspuesta, pero no tenía hasta hace un año ninguna legislación al respecto, con lo cual creo que estamos a la cabeza de nuestros aliados en la Unión Europea. De la Directiva 66, que yo sepa, hasta ahora no hay ningún anteproyecto para su trasposición, lo cual tampoco es ilógico, toda vez que, como conocen SS. SS., hace sólo unos días ha visto la luz la Ley de Telecomunicaciones, y ésta en definitiva puede ser en cierto modo un reglamento a la ley, porque la directiva contiene, por un lado, cuestiones que afectan a la ley orgánica de protección de datos y otras que afectan a la Ley de Telecomunicaciones. De todas formas, como ya he señalado antes, estamos en contacto con el Ministerio de Justicia para que cualquier proyecto que afecte de una forma general o de una forma sectorial a la protección de datos se nos pase para el preceptivo informe.

A su última pregunta sobre el grado de cumplimiento por las Fuerzas y Cuerpos de Seguridad del Estado y por los ayuntamientos, tengo que decirle que es altamente satisfactorio.

Se han inspeccionado estos ficheros y en cualquier caso han recabado nuestra colaboración. El mayor problema, si quiere usted, está en que hay algunos ayunta mientos que son muy pequeños y que aún no han tenido el suficiente conocimiento de tener que llevar a cabo el registro de sus ficheros. La labor que está haciendo la Agencia de recordárselo, de ayudarles, muchas veces incluso de redactar la norma que tienen que publicar por ser entidades públicas a la previa inscripción es constante, pero en las grandes ciudades, en los grandes municipios, todos los ayuntamientos puede decirse que en la práctica tienen registrados sus ficheros en la Agencia de Protección de Datos.

El señor PRESIDENTE: ¿Algún comentario, señor Alcaraz? (Asentimiento.) Tres minutos, por favor.

El señor ALCARAZ RAMOS: De manera brevísima, voy a centrarme solamente en dos cosas que ha planteado el señor Fernández; no supone estrictamente discrepancia, sino una reflexión.

El consentimiento presunto, y usted me parece que, desde un punto de vista sensato, en principio insiste en que lo importante es ese concepto de información clara e informada, o de consentimiento claro e informado, y no estrictamente expreso plantea un problema. El problema es que la interpretación jurídica del concepto clara e informada es muy ambigua, mientras que el de conocimiento expreso sí que parece que tiene unos perfiles jurídicos mucho más acotados. Por lo tanto, yo creo que o se insiste en el concepto de conocimiento expreso, si fuera necesario, con alguna matización, o difícilmente nos encontraríamos con un concepto, jurídicamente, que evitara problemas futuros.

Sobre la trasposición yo tengo unos argumentos, pero entenderá también que desde la visión de los grupos parlamentarios no pueda ser un consuelo que se vaya convirtiendo en una práctica habitual el retraso en la trasposición de directivas. La reflexión que dejo es si no sería útil hacer el esfuerzo para que las dos directivas se traspusieran a la vez, que se pudiera hacer la reforma de las normas correspondientes de una manera única y no estar parcheando cada año

o cada dos años.
El señor PRESIDENTE: También en su condición de firmante de solicitud de comparecencia, tiene la palabra la señora Lasagabaster.
La señora LASAGABASTER OLAZÁBAL: Seré muy breve, señor presidente. Cómo no, agradezco la presencia del señor Fernández López y por supuesto le doy la enhorabuena por su nombramiento para este cargo de una Agencia que yo creo que debiera ser muy importante, que debe ser muy importante, para los ciudadanos, a pesar de que quizás no se tiene conocimiento de cuáles son los derechos que ampara la Lortad para todos nosotros.
En relación con Telefónica, la verdad es que el relato que usted ha realizado nos demuestra lo que ya sabíamos pero con muchos más detalles, que es que en apenas dos años, desde 1996 hasta ahora, Telefónica ha sido objeto de la apertura, si yo no he tomado mal nota, de al menos cinco o seis expedientes, en algunos casos a instancias de la pro pia Agencia, en otros por denuncia de ciudadanos, con lo que, independientemente de las multas de esos cincuenta millones de las tres sanciones, creo que han sido, en algún caso y en algún otro más, también otra serie de sanciones, realmente parece que no temen mucho las sanciones cuando en apenas dos años, vuelvo a señalar, ha habido tantos expedientes.
Mi pregunta sería, amén de ese efecto disuasorio que dice usted de recopilar o de copiar el modelo de las sanciones de la Ley de defensa de la competencia, que a su vez viene también lógicamente de la parte del modelo europeo, si hay mecanismos de prevención -como usted bien dice, la sanción quizás no sea lo adecuado; quizá se puedan realizar otros- y si realmente Telefónica merece especial atención para la Agencia de Protección de Datos, en su unidad de inspección, dado el cúmulo de expedientes que tenemos en los dos últimos años. Qué otros mecanismos de preven - ción, si es que pueden realizarse, amén de medidas de seguridad del artículo 9, tienen ustedes pensado aplicar.
En segundo lugar, muy brevemente, de las prioridades que usted ha marcado creo que es bueno el acercamiento a los ciudadanos, al menos eso es lo que he entendido de su exposición. En lo que se refiere a las directivas, no voy a exponer otra vez los mismos pensamientos que el señor Alcaraz ha señalado, pero me parece que son muy importan - tes.
La primera, lógicamente, no sólo por la adaptación, sino por las reformas que se pretenden hacer de la ley de 1992, en cuanto a cesiones, subrogaciones y otras cuestiones que usted ha señalado. Y la segunda me parece importante porque, si no me equivoco -y si lo estuviera, rectifico de antemano-, es una directiva que en esta casa se ha mencio - nado para temas delicados. Cuando la Directiva 66/97, si no recuerdo mal, en uno de sus considerandos habla de la posibilidad de los Estados miembros de adoptar medidas para temas de seguridad, orden público, etcétera, hay que tener muy claro que esa directiva no permite determinadas actuaciones particulares -y todos sabemos de qué estamos hablando, del Cesid-, sino que lo que establece es que permite legislar a los Estados miembros. Esa interpretación hay que tenerla muy clara. Es una directiva de tratamiento de datos personales y de protección de la intimidad en el sector de telecomunicaciones que tiene mucha relevancia, especialmente, por lo que hemos visto en el pasado. Como Cámara legislativa, tendríamos que prestar atención a ambas cuestiones, en la medida en que se refieren a temas muy importantes y de relevancia directa para todos nosotros.
Le deseo que tenga en sus prioridades todo el éxito y, tanto si es así como no, le volveremos a ver en esta Cámara.
El señor PRESIDENTE: Señor Fernández López.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias por su felici - tación y por su apoyo, que, indudablemente, como el de todas SS. SS., he de precisar en la labor al frente de la Agencia de Protección de Datos.
En cuanto al tema de Telefónica, si bien cuanto ha dicho S. S. lo comparto, no soy tan pesimista con los resultados, porque no podemos olvidar que, con independencia de las multas, Telefónica ha comunicado a los ciudadanos que no va a ceder los datos para fines publicitarios. También hay otro hecho importante, y es que su filial, TPI, ha destruido los datos que obraban en su poder. Son unos resultados importantes. Por supuesto, sigue siendo objeto de estudio y de inspección, porque no podemos olvidar, según he manifestado, que aún hay tres procedimientos abiertos y que han de seguirse en todos sus trámites.
Por lo que respecta a las directivas, soy el primero que quiere que se cumplan las fechas de trasposición. Sé también las dificultades que existen y sé que, cuando se trata de directivas de mínimos, los países esperan a ver qué hacen los restantes para de esta forma llevar a cabo la trasposición.
Insisto en que, en la mayor parte, la directiva ya está incorporada a nuestra ley. Las reformas son sólo deseos míos. Yo no tengo potestad legislativa y sólo como órgano independiente que se encarga de aplicar la ley y que está para proteger a los ciudadanos puedo sólo sugerir lo que, a mi entender, puede suponer alguna mejora. De la segunda directiva, tenemos que decir que su publicación ha sido reciente, del 12 del pasado mes de enero.
Como S. S. ha destacado, es una directiva importante, que en muchos aspectos trasciende lo referente a la protección de los datos. Creo que es una directiva que habrá de trasponer más de un ministerio; posiblemente Fomento tenga que llevar a cabo un reglamento de acuerdo con su ley de telecomunicaciones y Justicia tenga que incidir en la trasposición de esta directiva. No sé cómo van los trámites pero, como he dicho antes, estoy alerta para que la Agencia pueda opinar al respecto.
El señor PRESIDENTE: Por el Grupo Parlamentario Vasco (EAJPNV) la señora Uría tiene la palabra.
La señora URÍA ECHEVARRÍA: Señor director de la Agencia, quiero darle la bienvenida en nombre del grupo al que represento en esta Comisión y desearle éxito en su cometido en la Agencia, puesto que se trata de un órgano de espe - cial relevancia, ya que tiene encomendada la tutela de lo que establece el artículo 18.4 de la Constitución, en cuanto a velar de que se limite el uso de la informática y de otras técnicas y medios de tratamiento automatizado de datos de carácter personal, para garantizar bienes tan fundamentales como el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos, cometido este de especial relevancia, que el grupo al que repre - sento se ha tomado en serio.
Lo digo en relación con el ámbito en el que tiene especiales responsabilidades y respecto del Gobierno vasco, cuya labor en esta materia fue especialmente alabada por su predecesor al frente de la Agencia en un aspecto tan delicado como fue la regularización de los ficheros policiales, los ficheros de la Ertzaintza. Igualmente, en fechas recientes, se ha procedido a unificar la gestión o a centralizar en un solo órgano toda la protección de datos informáticos y se dice en la exposición de motivos de la orden que lo regula que con el objetivo primordial de mejorar las relaciones con la Agencia

de Protección de Datos.
Quiero decir que es cometido esencial del Gobierno en el que el partido al que represento tiene responsabilidades de gobierno.
En el mismo sentido, desde el comienzo de esta legislatura he tenido ocasión de preguntar en distintas ocasiones por la trasposición de la directiva que ha sido punto recurrente en las intervenciones de quienes me han precedido.
Ya en la primera comparecencia en la Comisión de Justicia de la señora ministra de Justicia, le preguntaba, en junio del año 1996, qué se pensaba hacer con la trasposición de esta directiva, aunque sabía que no vencía hasta este año, y le instaba a si era posible reconducir el asunto haciendo que coincidiese con la finalización de los cuatro recursos de inconstitucionalidad que están pendientes en esta materia, ya que uno de ellos estaba planteado por el Defensor del Pueblo, otro por el propio grupo que hoy sostiene al Gobierno, por 50 diputados del Grupo Popular, y lo otros dos lo eran por cuestiones competenciales, interpuestos por el Consejo ejecutivo de la Generalidad o por el Parlamento catalán. Intentar, en la nueva redacción que se diese a la Lortad, un arreglo que pudiese suponer el desistimiento en estos procedimientos. Y lo planteábamos con el objetivo de que de una vez por todas quedase claro cuál es el ámbito normativo que rige en esta materia, no teniendo la pendencia de cuatro posibles sentencias del Tribunal Constitucional.
En sucesivas ocasiones he reiterado esta misma pregunta a la señora ministra y la última fue en febrero de este año, con ocasión de los sucesos que han motivado las peticiones de comparecencia de quienes me han precedido en el uso de la palabra, es decir, la cuestión de la cesión de datos, por Telefónica, y también una multa -se ha citado sólo a Telefónica, pero también ha sido objeto de amplio tratamiento esta otra en los medios de comunicación- interpuesta a Codorniú por alquilar las bases de datos de sus clientes. Sin embargo, no me satisfizo la respuesta que obtuve del Ejecutivo, puesto que se me indicó que hasta octubre no vence la directiva. Ya ha manifestado ahora el portavoz del Grupo Mixto, en nombre de Nueva Izquierda, que si en octubre se trae el proyecto, difícilmente para ese mes va a estar completado el texto legal. Se me indicó que entre las prioridades del Ministerio no gozaba de especial protección ésta, sino que se le daba la misma relevancia que a la ley de venta a plazos de bienes muebles. Teniendo en cuenta que estamos hablando de un aspecto tan fundamental como es la protección, el respeto o el poder hacer efectivo el derecho que reconoce el punto cuatro del artículo 18, me parece que es una prioridad que debiera haberse respetado.
Ya ha indicado usted, y efectivamente así lo sé, que la iniciativa normativa no le corresponde a la Agencia, sino al Gobierno, pero me es dado suponer que usted, que está recién nombrado por este Gobierno, tendrá una mayor capacidad de persuasión sobre él que la que podrá tener su predecesor, que no hay que olvidar que estaba nombrado por el último Gobierno socialista. Por cierto, quisiera aprovechar en este primer momento para rendir un tributo a la labor realizada por el señor Martín Casallo en la puesta en marcha de la Agencia de Protección de Datos.
En relación con la trasposición de la directiva, hay algunas cuestiones que inquietan especialmente a mi grupo, a las que usted no ha hecho referencia y que me gustaría plantear. Si con ocasión de la trasposición de la directiva se va a aprovechar para dividir, separar o hacer alguna distinción entre los ficheros de titularidad pública y los de titularidad privada. Si se va a abordar de alguna manera el tratamiento de los datos personales y la libertad de expresión, aspecto que creo que es fundamental. Una cuestión distinta y que me resulta particularmente interesante es la de la propia configuración jurídica de la Agencia. En su situación actual, es un ente público de los previstos en la ley presupuestaria, en el artículo 6.5, y, sin embargo, algunos de los preceptos de la directiva que hay que trasponer, por ejemplo el 28, parece que abogarían por una solución más vinculada al órgano legislativo, ya que parece que la Agencia tendrá que tener alguna posibilidad de iniciativa o de sugerir cuestiones a los Parlamentos o a otras instituciones públicas. Quisiera saber si se ha pensado en cambiar esta adscripción, vinculándola como comisionado, o de alguna otra forma especial, al Parlamento, o se la va a mantener con este tipo de personificación jurídica.
Me quería referir también a un supuesto que usted ha citado, respecto del cual le haré una pregunta. Ha mencionado usted el asunto en el que, con ocasión de haberse detectado el espionaje efectuado en la sede de la coalición de Herri Batasuna, el periódico Egin publicó datos procedentes de Telefónica. En una información periodística me pareció entender que usted mismo decía que iba a ser complicada la persecución de esas conductas porque no estaba hecho el reglamento en el que se estableciesen los medios que tienen obligación de cumplir las empresas para proteger estos datos. Le quería preguntar si el retraso que, desde el punto de vista del grupo al que represento, está habiendo en la trasposición de la directiva y en la elaboración de los reglamentos va a facilitar que conductas de este estilo queden sin aclarar o sin posibilidad de investigación.
Nada más que esto. Únicamente quiero reiterarle el mayor éxito en el cometido que emprende, porque creo que el éxito suyo será de todos los ciudadanos, ya que la protección de nuestros datos es lo que tiene encomendado la Agencia.
El señor PRESIDENTE: Señor Fernández López.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Señora Uría, muchas gracias por su felicitación y por sus buenos deseos. Es cierto, como ha manifestado S. S., que la relación que ha mantenido la Agencia con la Ertzaintza ha sido excelente, su grado de colaboración ha sido óptimo. Hace apenas unos días, hemos tenido una reunión más porque han querido someter a nuestra consideración los últimos flecos de un texto legislativo y la realidad es que la colaboración ha sido estrecha y fructífera para ambos. En la trasposición de la directiva, me remito un poco a lo ya dicho. La directiva está en un noventa y tantos por ciento -no sé afinar más los decimales- traspuesta a nuestra legislación; de lo que se trata es de mejorar la ley.
Tal vez, como ha señalado S. S., al estar pendientes los recursos de inconstitucionalidad y no haberse aún resuelto por el Tribunal Constitucional, se ha esperado a su resolución y por eso tiene algún retraso.
Ha hecho referencia a si se va a distinguir entre los ficheros de titularidad pública y titularidad privada. Ya están suficientemente distinguidos, creo, en la actual ley orgánica y van a continuar con esa misma distinción, que, por otro lado, en cambio, no hace la directiva. A mi modo de ver, eso lleva a una mayor seguridad, por cuanto que los de titularidad pública tienen que publicar una norma por la que se rija el fichero que han de registrar.
La posibilidad de sugerir al Parlamento reformas legislativas sería una buena función. Otros órganos la tienen, como es el caso, también mencionado antes, del Tribunal de Defensa de la Competencia, que se puede dirigir tanto al Gobierno como a las Cámaras sugiriendo alguna reforma en materia que les afecte.
En relación con la filtración, la venta, la publicidad de los datos de ciertos ciudadanos, por parte del diario *Egin,* salidos de Telefónica, evidentemente, si existiera el reglamento de medidas de seguridad, que es un complemento al marco legislativo, se podría determinar mejor el tipo de infracción que ha podido existir. De todas formas, y aunque la Agencia

sigue investigando, creo que son otras instancias las que primordialmente deben hacerlo. Sin duda, el reglamento de medidas de seguridad que, como digo, está a punto de ser aprobado, va a facilitar que exista un control y que ni terceros que accedan a un registro puedan apropiarse de datos que no les corresponden, ni empleados o directivos infieles puedan vender o emplear los datos que existen en un fichero para finalidades distintas. Esto será una mejora. Como también he informado, el reglamento tiene un plazo de adaptación y en ese plazo la Agencia tratará de concienciar a todos de la necesidad de establecer las medidas, que no todas son técnicas y caras porque hay muchas organizativas, saber quién y por qué esas personas acceden a un registro y no otras. En esta fase, como digo, la Agencia tratará de informar a todos y de facilitar el cumplimiento del reglamento para ver si ello es posible en el plazo de adaptación.
El señor PRESIDENTE: Por el Grupo Parlamentario Catalán de Convergència i Unió, el señor Silva tiene la palabra.
El señor SILVA SÁNCHEZ: Obligaciones derivadas de la representación que todos ostentamos me han impedido asistir a las primeras intervenciones del director de la Agencia de Protección de Datos y, por tanto -entiendo que otra cosa sería descortesía-, lo que procede es felicitarle por su nombramiento, desearle obviamente lo mejor, la gestión más brillante al frente de la Agencia y manifestarle la solidaridad de mi grupo parlamentario respecto de la protección de datos; de alguna manera, fuimos nosotros los que planteamos la enmienda que supuso esa redacción concreta en el artículo 18 de la Constitución.
Sí que he llegado a tiempo para oír una reflexión del señor director que entiendo que pone de manifiesto una necesidad de homogeneización, dentro del ámbito de la Unión Europea, en el desarrollo concreto de la directiva. Si bien la Directiva 96 contempla la relación que puede haber entre la Unión Europea y los terceros Estados respecto de la protección de los datos, es cierto que poco sentido tendría establecer una legislación que, adaptando la normativa, fuese más restrictiva que en otros países y que permitiese el tratamiento automatizado de los datos en otros países, que afecte exactamente igual a nuestros ciudadanos, sin gozar de los beneficios que pudiera dar el comercio de esos datos precisamente.
Nosotros entendemos que ése ha de ser un principio básico. Hay que dar la mayor protección que pueda ofrecerse a los ciudadanos, pero no establecer una legislación restrictiva respecto de la que pueda existir en otros países del ámbito de la Unión Europea que pueda perjudicar a determinadas empresas, bien sea en el ámbito del desarrollo comercial de estos datos o bien en el de protección respecto de la morosidad o de marketing directo. Lo que estaríamos haciendo, sin ofrecer una mayor protección a los ciudadanos, es engordar a empresas ajenas y no a las propias.
Como sí he llegado a ese punto de su intervención, tengo que ponerle de manifiesto que también ése es nuestro principio.
Como decía anteriormente, enhorabuena. Le apoyaremos en la medida que nos sea posible. Aprovecho esta intervención para hacer constar la brillante gestión que realizó su antecesor y no dudamos que usted también la realizará.
Hasta ahí llegamos.
El señor PRESIDENTE: Señor Fernández López.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor Silva, por su felicitación y sus buenos deseos. Como antes puse de manifiesto, hay un problema serio en que cierto comercio, que es lícito y que se practica en el resto de los países de la Unión Europea, aquí tiene ciertas dificultades, sobre todo en cuanto al acceso a datos que proceden del padrón y que la Ley de ordenación del comercio minorista expresamente permite, pero en cambio la ley orgánica electoral general expresamente prohíbe, con lo cual tenemos una contradicción legislativa lamentable, porque también esto sume en dudas a nuestros ciudadanos. A este respecto, y dentro de procedimientos sancionadores, el anterior director de la Agencia hizo una consulta a la Junta Electoral Central y recibió la contestación de la prevalencia de la Ley orgánica general electoral, por su carácter orgánico, sobre la Ley de ordenación del comercio minorista, por su carácter de simple ley; además y a pesar de su posterioridad, hacía imposible que pudieran utilizarse estos datos por las empresas de marketing. Es una opinión que, permítanme sus señorías, con respecto a la Junta Electoral Central, desde mi independencia intelectual, no comparto, pero que he de acatar. En cualquier caso, hasta que no se pronuncien los tribunales de justicia, el criterio de la Agencia tiene que ser el mismo.
El señor PRESIDENTE: Por el Grupo Parlamentario Federal de Izquierda Unida, tiene la palabra el señor Frutos.
El señor FRUTOS GRAS: Bienvenido, señor Fernández, a esta Comisión. Le deseo mucha suerte y acierto en el desarrollo de todo el programa de trabajo que ha expuesto usted anteriormente. Voy a ser muy breve. Usted ha dicho que la multa es la quiebra del Derecho.
En el momento en que se tiene que multar es que el derecho ha quebrado. Telefónica, por lo que parece ser, ha quebrado el derecho varias veces en los dos últimos años. Por lo tanto, es un elemento a tener en cuenta, empresa pública privatizada en su totalidad y es un elemento a controlar.
Siempre en esto deberá haber, dentro del marco del cumplimiento global de la ley, una actuación selectiva hacia determinadas empresas que pueden vulnerar más que otras, por su capacidad, el derecho a la intimidad de las personas.
Esperamos que el plan de la Agencia de Protección de Datos y la trasposición de la directiva europea que usted ha expuesto sirvan para crear una realidad diferente, desde -he querido entender- un código deontológico y añado que introduzca elementos de control democrático en la selva consumista en la que nos encontramos ahora, donde parece que el comercio, el libre mercado -que tampoco es tan libre- lo puede permitir todo, cualquier vulneración de cualquier derecho individual o colectivo. El control de la arbitrariedad posible es antes que la sanción. El cumplimiento de la ley no quiebra del derecho, y desde el más riguroso respeto a la intimidad de las personas, en una sociedad en la que la violación de la intimidad se produce muchas veces desde las más groseras manifestaciones subculturales, a través de potentes medios de comunicación.
Por tanto, bienvenidas sean todas las propuestas que usted ha señalado y le reitero mucha suerte en el desarrollo del plan de trabajo que ha expuesto.
El señor PRESIDENTE: Señor Fernández López.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor Frutos, por sus buenos deseos y por su felicitación a mi persona. Sus preocupaciones son las mías. Como he puesto de manifiesto antes, en los últimos tiempos se han abierto, incluso de oficio, sin denuncia del ciudadano, varios procedimientos a Telefónica, que están pendientes de resolver. Es decir, estamos, como ve usted, vigilantes.
El señor PRESIDENTE: Antes de conceder la palabra al señor Navarrete quiero que conste en el «Diario de Sesiones»

la felicitación de esta Comisión por la renovación de su mandato como comisionado de esta Cámara acerca de la Agencia de Protección de Datos. Me parece de justicia esta mención.

Por el Grupo Parlamentario Socialista, tiene la palabra el señor Navarrete.

El señor NAVARRETE MERINO: Intentaré, de una manera distinta de lo que puede mostrar mi retraso de esta mañana, merecerme la confianza de la Cámara para presentarla ante el Consejo consultivo de la Agencia de Protección de Datos. Vaya por adelantado que mi retraso no ha sido voluntario, sino debido a una bronquitis que me ha dejado dormir de mala forma.

El señor PRESIDENTE: Hacemos votos por su recuperación, señor Navarrete.

El señor NAVARRETE MERINO: Muchas gracias. Dicho esto, tengo que manifestar -al igual que han hecho los compañeros de la Comisión que se han expresado anteriormente- mi felicitación al nuevo director general de la Agencia, de quien ya me consta, con la escasa relación que hemos tenido, su gran capacidad de trabajo y su gran pasión por el mismo. Una vez más quiero recordar en esta Cámara la excelente labor pionera que realizó el señor Martín Casallo, que ha posibilitado que la Agencia de Protección de Datos y lo que la misma representa en nuestro ordenamiento jurídico pasara, de ser un ente de razón legislativa, a convertirse en una potente realidad, aun cuando todavía, como es lógico, no ha desplegado todas sus capacidades. También tengo que expresar que comparto las opiniones manifestadas por el señor director de la Agencia en cuanto a las líneas generales que van a inspirar la actuación.

Le deseo suerte, porque me parece que es un terreno enormemente complicado, tan complicado como el de la directiva, a la que repetidamente se ha hecho alusión, que hay que trasponer al Derecho interno español, que, en su artículo 1, cuando habla de su objeto, dice, en el párrafo uno: protección de la intimidad, normas de protección de la intimidad o tratamiento de protección de la intimidad. Y en su párrafo dos dice: lo anterior no dará causa a que se impida la libre circulación de los datos personales dentro de los Estados miembros. Es decir, coloquen ustedes todas las barreras que sean precisas para proteger la intimidad, pero al mismo tiempo esas barreras no pueden impedir la libre circulación de los datos. Es una misión muy complicada al tratar de mantenerse en un equilibrio entre tan extremadas y contradictorias limitaciones. Yo creo que esto tiene que ver con la relativa novedad del invento. Las normas de protección de la intimidad derivadas de la aparición de un fenómeno tecnológico llamado ordenadores han comportado, por lo pronto, una especie de reacción espiritual, moral, que ha terminado teniendo unas consecuencias en los ordenamientos legales. Esa reacción se parece mucho -me parece que ya lo he dicho en alguna ocasión en esta Comisión- a lo que sucedió con el descubrimiento de la imprenta, que provocó la aparición de la censura eclesiástica como manifestación del temor social a las consecuencias nefandas que aquel descubrimiento tecnológico iba a tener. Con los ordenadores ha pasado lo mismo. Yo creo que los poetas y los literatos han contribuido extraordinariamente a esta actuación de pusilanimidad que tiene la sociedad: el gran hermano, la estructura de cristal, etcétera. ¿En qué quedará esta modernidad? Imagino que ocurrirá igual que con la imprenta, que desapareció el nihil obstat, la censura eclesiástica, la censura del Estado y quedarán determinadas normas legales de orden penal de contenido muy estricto en manos de los tribunales de justicia,

que reprimirán los excesos que puedan cometer algunas personas en el ejercicio de su libertad de expresión.

No estoy condenando la legislación protectora de la intimidad que ha surgido al socaire de los ordenadores, que me parece puede tener su virtualidad; es decir, a través de estas normas, en mi opinión exageradamente restrictivas, se está creando una conciencia social del adecuado uso de este tipo de tratamiento automatizado, que como la bomba atómica tiene una potencia letal muy superior a la que podrían tener los excesos cometidos a través de la prensa escrita. Con esta conciencia, al menos por mi parte, de lo efímero de nuestra función y de estas barreras que más bien deben ayudar al crecimiento de un árbol que desarrolle adecuadamente la flor de la libertad, que es la última misión de cualquier ordenamiento legal, tenemos que asumir que hoy tiene que haber una legislación mucho más restrictiva de la que probablemente existirá el día de mañana y entre todos debemos contribuir a su perfeccionamiento.

Me da la impresión de que a través de estas normas se ha construido una especie de monumental catedral del fariseísmo; es decir, que por un lado se acota muchísimo lo que es el tratamiento de datos personales, y por otro lado se abren agujeros de tal naturaleza que muchas veces convierten en inane la eficacia de las normas jurídicas protectoras de la intimidad. Un buen ejemplo lo representa la nueva directiva, que comparada con la Lortad supone una disminución de las garantías jurídicas de la protección de la intimidad, pero por otra parte va más allá de lo que era el proyecto de directiva anteriormente existente y de la propia Lortad, porque pretende que en un plazo de doce años sus barreras protectoras de la intimidad alcancen no sólo al tratamiento automatizado de los datos personales, es decir el que tiene lugar a través de los ordenadores, sino a cualquier otro fichero organizado de datos personales, aunque no esté mecanizado, con lo cual el día que a la Agencia de Protección de Datos o la autoridad de control, como llaman otras legislaciones, tenga que controlar los ficheros personales no incluidos en ordenadores, no sé qué tipo de policía, cualitativa y cuantitativamente hablando, va a necesitar para efectuar ese control.

Dicho lo anterior, me parece necesario insistir y que la Comisión sea consciente de ello (debe ser el punto de apoyo imprescindible que la Comisión Constitucional debe prestar a la Agencia de Protección de Datos), en la deseable mejora de las relaciones de la Agencia de Protección de Datos con otros organismos imprescindibles para que la misma pueda cumplir eficazmente su función. Me refiero específicamente al Defensor del Pueblo y a esta propia Comisión, que desde el principio ha acogido con simpatía y con espíritu de colaboración a esta recién nacida Agencia de Protección de Datos, pero me refiero también al Ministerio de Justicia, porque para que un organismo funcione no sólo es necesario que aparezca impreso en las páginas del Boletín Oficial del Estado, sino que si quiere cumplir sus objetivos tiene que estar dotado de medios económicos y de personal y me consta, y quiero que lo sepa la Comisión Constitucional y especialmente el partido del Gobierno, que las funciones que hoy legalmente se atribuyen a la Agencia de Protección de Datos no pueden ser adecuadamente ejercidas con el personal y los medios económicos de que dispone dicha agencia.

Por otra parte, es preciso que ahora que se han iniciado los trabajos para la trasposición de la directiva de la Unión Europea, nos planteemos cómo se va a llamar la norma que recoge la protección de la intimidad, actualmente Lortad, Ley orgánica para el tratamiento automatizado de datos personales. Aunque haya un plazo de doce años para el tratamiento de los ficheros manuales es evidente que no debiera seguir denominándose así. Además, creo que ésta es una buena oportunidad para corregir ciertos defectos sistemáticos, de los que también me acuso personalmente en cuanto que fui ponente en la elaboración de la Lortad, como por ejemplo el problema que se ha suscitado en relación

con el Ministerio de Defensa, que puede tener un principio de solución en el artículo 27 de la Lortad, que habla de las garantías y de las condiciones en que debe realizarse la prestación de servicios de tratamiento automatizado de datos de carácter personal por cuenta de terceros, que es justamente lo que el Ministerio de Defensa quería efectuar: un tratamiento por cuenta de terceros de datos personales imprescindibles para el cumplimiento de sus funciones públicas. El problema es que las garantías para ese tratamiento se establecen, como he dicho, en el artículo 27 de la Lortad, que se ubica en el capítulo segundo, ficheros de titularidad privada, que a su vez está incluido en el Título IV, disposiciones sectoriales, que tiene un capítulo primero que habla de los ficheros de titularidad pública y que concluye en el artículo 22. Por tanto, atendiendo a una interpretación sistemática parece que el artículo que recoge las garantías que debe tener el tratamiento de los datos personales por cuenta de un tercero sólo es aplicable a los ficheros de titularidad privada y, en consecuencia, no permite que el Ministerio de Defensa o cualquier otro organismo público solucione sus problemas desde el momento que conceda a un tercero la posibilidad de tratar esos datos personales por cuenta del organismo público.

Ésa es una cuestión que merece la pena ser resuelta al modificarse la Lortad como consecuencia de la trasposición de la directiva, llevando esta cuestión del tratamiento por cuenta de terceros a alguno de los capítulos anteriores al título IV, con lo cual sería de aplicación general tanto para los ficheros de titularidad pública como para los de titularidad privada.

Luego hay determinadas necesidades de la sociedad española, necesidades que yo diría son muy básicas en el aspecto de combatir la evasión fiscal, evitar el fraude social y hacer aflorar la economía sumergida, tres elementos constitutivos de la sociedad española que nos colocan al mismo nivel que el Real Madrid, esto es que estamos a la cabeza de Europa en economía sumergida, en evasión fiscal y en fraude social. ¿Cómo se combaten esos elementos, que no son precisamente honoríficos, de la sociedad española? Mediante el cruce de datos. ¿Es posible ese cruce de datos según la Lortad? Yo tengo mis dudas, que deberían despejarse, porque entre otras cosas la nueva directiva, con un lenguaje muy poco afín con nuestra terminología jurídica, en su artículo 12 dice que los principios fundamentales de la protección de la intimidad, el derecho de acceso y el derecho de información, entre otros, deben ceder ante la seguridad del Estado, la defensa, la seguridad jurídica, el interés económico o financiero importante de un Estado miembro. Es decir, el espíritu de la nueva directiva no es incompatible con la lucha que es preciso realizar dentro de nuestro país para combatir la evasión fiscal, el fraude social y el fenómeno de la economía sumergida, pero tienen que buscarse en la Lortad unas normas suficientemente claras que permitan sin ningún género de dudas la instrumentación de los ordenadores, dirigida hacia esta finalidad.

Por otro lado, las directivas con mucha frecuencia incurren en vocabularios que nos resultan extraños y que nos plantean problemas muy grandes de interpretación. Ya me he referido en el propio artículo 12 al interés económico y financiero importante de un Estado miembro. Yo creo que esto se puede decir en castellano con una mejor precisión jurídica. Hay una permanente remisión, que está hecha con la buena voluntad de abrir agujeros en el marco protector de la intimidad en la directiva, según mi leal saber y entender, y que necesita una definición. ¿Qué es, por ejemplo, el interés vital al que hace referencia el artículo 13 como excepción al consentimiento? ¿El interés vital quiere decir un interés fundamental o quiere decir protección del derecho a la vida? ¿Interés vital quiere decir protección de la integridad física de las personas? Yo no lo sé, y creo que sería una hipoteca demasiado extraordinaria la que se transmitiría a cualquier persona que queriendo ser respetuosa con el cumplimiento de las leyes tuviera que interpretar qué es el interés vital. Ésta es una labor que nos debe corresponder a los legisladores; facilitar las cosas al buen ciudadano que quiere cumplir con la legalidad.

Se ha tocado un tema que yo creo que a todos nos debe preocupar porque es algo digno de ser incluido dentro de ese museo de los horrores jurídicos, la antinomia que actualmente existe entre la Ley orgánica electoral general, cuando declara la exclusiva finalidad del censo electoral para los objetivos de convocatorias de consultas populares, y por otra parte, la Ley de ordenación del comercio minorista, que ha previsto la utilización del censo para algo que también forma parte de las características de nuestra contemporaneidad, que son las ventas a domicilio. A propósito de esto, se ha expresado la opinión favorable a que la antinomia se resuelva aplicando el censo a esos objetivos. Yo creo que sería uno de los pocos casos en que la materia prima que está en el fondo de la actividad económica de una empresa se suministra por el Estado, esto sería equivalente a si los géneros que un híper fuera a vender al público se le suministraran por el Estado. ¿Pero por qué una empresa que se dedique al marketing tiene que tomar los datos gratuitamente del censo electoral? Que los
busque, que hable con los interesados, que los vaya obteniendo.

Es una medida que propongo. Por otra parte a mi me preocupa -nos debe preocupar a los legisladores- contemplar los derechos no como algo definitivamente acabado y para toda la vida, sino que los derechos también tienen esa dimensión que los escolásticos llaman *in fieri,* es decir, los derechos están permanentemente evolucionando en virtud de una dinámica que les viene impuesta por la propia evolución de la realidad social, y yo creo que debemos empezar a preguntarnos si los que hoy se consideran como datos sensibles, que tienen mucho que ver con la trayectoria de nuestro país -es decir, la religión, las creencias, las opiniones políticas, el tema de las preferencias sexuales-, tienen ya en estos momentos el mismo sentido que tuvieron en el año 1978, cuando los padres de la patria, uno de los cuales nos honra con su presidencia, incluyeron dentro de la Constitución esos sagrados derechos que habían sido maltratados, conculcados permanentemente por el franquismo.

¿Qué es más problemático hoy para un ciudadano que quiere defender su intimidad? ¿Que salgan a la luz pública su o sus domicilios o que se sepa que es católico o protestante, homosexual o heterosexual? Desde luego dentro del franquismo era muchísimo más grave que se supiera que una persona era protestante, atea o agnóstica a que se conociera su domicilio, pero ¿hoy es así? ¿No debería ser considerado el domicilio, que, juntamente con la contabilidad, puede ser un elemento importantísimo de la construcción de la biografía de un sujeto? ¿Debe el domicilio estar en manos de cualquiera? Y no digo solamente en manos de los posibles atracadores o en manos de los posibles terroristas; simplemente el que quiera saber nuestra vida, quién entra en nuestra casa, quién sale de ella, o cómo gastamos nuestro tiempo no laboral. A mí me parece que el domicilio es un tema importantísimo, es un elemento sensible, y desde luego cada vez más (no es que tenga las cosas definitivamente claras, yo me imagino que no es fácil que nadie que piense en profundidad sobre esto las tenga claras) me inclino por la solución de que el marketing es indispensable, pero que debieran ser las agencias de marketing las que en entrevistas individuales fueran obteniendo el necesario número de domicilios -porque tampoco necesitan el domicilio de todos los españoles- para que su actividad comercial

tenga la clientela indispensable. Sobre lo que ha ocurrido con Telefónica o algún otro caso particular que se ha mencionado se me ocurre añadir que quizá una actividad inspectora de la Agencia de Protección de Datos debiera estar especialmente dirigida a las grandes empresas, porque partícipe en la comisión de una infracción lo puede ser cualquier ciudadano, y si éste es un empresario da lo mismo que sea grande o pequeño, pero siempre será el elemento pasivo de la comisión de una antijuridicidad. Las más corrientes antijuridicidades activas que se pueden cometer en el terreno del tráfico ilícito de datos
personales se cometen sin duda por las grandes empresas, que son las que disponen de los grandísimos bancos de datos, que convierten en una fuente generalmente ilícita de beneficios: grandes empresas, hipermercados, grandes superficies, empresas eléctricas, compañías de se guros, bancos, etcétera, sin que el hecho de mencionarlas signifique que globalmente esté condenando a la totalidad de cada uno de los sectores que acabo de mencionar.
Nada más, salvo reiterar mi deseo de representar dignamente a la Cámara en la Agencia de Protección de Datos y de prestar la más absoluta colaboración personal, de mi grupo y creo que la de todos los demás componentes específicos de esta Comisión Constitucional, para que la agencia fortalezca su cometido, tan necesario para la sociedad española, al menos durante los próximos cincuenta años.
El señor PRESIDENTE: Oír a S. S. en esta materia resulta siempre ilustrativo y apasionante, se hace perdonar con creces su latitud.
Señor director de la Agencia de Protección de Datos, tiene la palabra.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor Nava - rrete, por sus buenos deseos y por su colaboración, que además ya sé -he tenido ocasión de constatarlo- que ha empezado a prestar en la primera reunión del Consejo Consultivo. Sería imposible ir contestando a cada una de las reflexiones de S. S., todas importantes y que he escuchado con sumo interés, por lo que sólo haré alguna precisión o manifestaré mi opinión sobre alguno de los temas que ha tratado el señor Navarrete.
En cuanto a la circulación de los datos entre los Estados miembros, y por otro lado, el control que tiene de existir de los mismos, indudablemente estamos ya en la Unión Europea y, como ciudadanos europeos, es lógico que tengamos todos el mismo trato y que nuestros datos puedan circular o no, según queramos, por todos los países o no figurar en fichero alguno. Para mí, señorías, lo más importante aquí es que los datos sólo se utilicen para la finalidad con que fueron recogidos y, segundo, que se obtengan con el consentimiento informado del ciudadano. Si yo doy mi consenti - miento y quiero figurar en 200.000 ficheros no habrá problema alguno; si yo no quiero figurar en ningún fichero sólo tendré que figurar en aquellos que las disposiciones legales o mis relaciones contractuales me obliguen a ello.
Creo que en esto se puede resumir la protección que en definitiva está dando la ley. En cuanto a las buenas relaciones que S. S. ha dicho que son deseables con el Defensor del Pueblo y el Ministerio de Justicia, por supuesto y hasta el momento, las relaciones de la Agencia con el Ministerio de Justicia son óptimas.
Como he manifestado a S. S., a sugerencia mía, han puesto a mi disposición que a través de los órdenes del día de las comisiones de subsecretarios se puedan conocer todos los proyectos y anteproyectos de ley para que así pueda la agencia pedir aquellos que considere pueden tener alguna relación con su cometido. En cuanto al Defensor del Pueblo mi intención es mantener la más cordial y respetuosa relación, dentro de la independencia de cada uno de los órganos.
En cuanto al problema que ha puesto de manifiesto S. S. sobre la imposibilidad que pudiera existir desde el marco legislativo a que los distintos órganos de la Administración puedan cruzarse los datos para perseguir el fraude fiscal, la economía sumergida, etcétera, creo que no hay problema alguno. Fíjese, señoría, que el artículo 18 de la Ley orgánica, en el que se habla de la creación de los ficheros de titularidad pública, dice que la creación, modificación o supresión de ficheros automatizados de las administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial competente. Y el artículo 19 dice que 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 la disposición de creación del fichero o por disposición posterior de igual o superior rango que regule su uso. Con ello, la propia disposición de creación del fichero puede permitir este cruce de datos y, a mi modo de ver, no hay ningún problema.
En cuanto a la necesidad que muestra S. S de que las empresas de marketing no accedan a los datos que se ofrecen al público y que sólo se pueda hacer a través del conocimiento expreso del ciudadano, indudablemente es una posibili - dad, pero sí le puedo decir que en el resto de países miembros de la Unión Europea las cosas no son así y que se les posibilita el acceso, al menos de nombres y direcciones, de aquellos medios que son accesibles al público.
En cuanto a la preocupación, también mostrada por S. S., de la inspección a grandes empresas, en el plan de priori - dades diseñado está precisamente la inspección de grandes grupos donde hay una recogida mayor de datos y donde, como consecuencia de ello, pudiera existir un mayor tipo de infracción. Por supuesto, estamos inspeccionando grandes grupos y grandes sectores.
El señor PRESIDENTE: ¿Algún comentario, señor Navarrete?
El señor NAVARRETE MERINO: Simplemente quiero decir, señor director, que efectivamente lo que dice el artículo 19 es cierto, pero quisiera señalar que cuando se está en el proceso de investigación, de descubrir si alguien está cobrando inadecuadamente las prestaciones por desempleo, o si alguien que tiene una finca agrícola con cierto número de tractores, está indebidamente pagando determinados impuestos, quizá no sea el momento más adecuado para darse cuenta de que en la disposición creadora de los ficheros correspondientes se omitió el cruce del dato de los ordenadores que hay en la Hacienda pública con los de la Seguridad Social, con los del Catastro, etcétera. Por tanto, evidentemente no hay una prohibición en la Lortad para el tratamiento de esos datos tan indispensables para detectar los agujeros negros de la economía y de la sociedad española, pero aprovechando que vamos a revisar la Lortad debemos dejar más claramente explícita, sin necesidad de reajustar otras normas de carácter más sectorial, la facultad de las administraciones públicas para cruzar sus datos con esos objetivos que genéricamente se llaman del bienestar económico de los Estados miembros, en la nueva directiva. Por consiguiente, no hay contradicción alguna con lo que usted ha manifestado, sino que sólo hay que señalar los inconvenientes prácticos que las normas actuales representan para este tipo de investigaciones.
Por lo demás, agradezco muchísimo su respuesta y su entusiasmo en esta materia que le ha sido tan recientemente encargada.

El señor PRESIDENTE: Por el Grupo Parlamentario Popular, el señor Izquierdo tiene la palabra.
El señor IZQUIERDO JUÁREZ: Después de los múltiples y reiterados parabienes que inició el presidente de la Comisión y a los que se han sumado todos los grupos parlamentarios, el Grupo Parlamentario Popular hace suyas todas esas manifestaciones, le damos la bienvenida y le deseamos los mejores éxitos. Lo hacemos de esta manera tan rápida y sencilla puesto que ya no quedan palabras para hacerlo de otra forma.
Nada tiene que decir el Grupo Parlamentario Popular, señor Fernández López, a las relaciones de la Agencia de Protección de Datos, con los problemas que se han suscitado ante la actuación de determinadas empresas privadas, aunque algo tendríamos que decir si esas relaciones hubiesen sido distintas, por lo que felicitamos y saludamos su extensísima y amplísima exposición al respecto, que pone a salvo las responsabilidades de la Agencia de Protección de Datos y, por ende, las de la Administración y las del propio Gobierno, que es lo que tiene que hacer y por lo que tiene que velar.
Saludamos muy especialmente, señor Fernández López, aquellas referencias que usted ha hecho a las relaciones de la Agencia de Protección de Datos con el resto de la Administración. A nuestro grupo le parece que alguna vez y entre todos podremos intentar empezar a superar ese viejo recurso de la oratoria que es siempre el tema de la coordinación y dar un sentido superior que es el de la coherencia y el sentido común. Por tanto, las magníficas relaciones que usted ha expuesto entre el Ministerio de Defensa, la propia Agencia de Protección de Datos y el Defensor del Pueblo, sean bienvenidas, porque es algo en lo que siempre encontrará el apoyo del Grupo Parlamentario Popular.
Saludamos también, señor Fernández López, los importantes datos de incremento que se han producido en el último bienio en cuanto a los procedimientos de inspección, sanción y tutela y finalmente le decimos que compartimos plenamente las prioridades que ha expuesto en su trabajo futuro, para las que siempre encontrará también el apoyo del Grupo Parlamentario Popular.
El señor PRESIDENTE: Señor Fernández López.
El señor DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS (Fernández López): Muchas gracias, señor Izquierdo, por su felicitación, por sus sugerencias y por su ofrecimiento de apoyo, que indudablemente me será de gran utilidad, lo mismo que el que me puedan prestar todas SS. SS.

El señor PRESIDENTE: Concluimos en este momento con los puntos 2, 3, 4 y 5 previstos en el orden del día. Reitero los términos en que hablaba el señor director de la Agencia de Protección de Datos al comienzo de esta sesión. Sin duda la naturaleza de su actividad y la singular competencia que esta Comisión tiene respecto a los trabajos de la agencia que tan dignamente dirige, depararán nuevas y pienso que frecuentes y positivas oportunidades para mantener un intercambio tan rico y tan constructivo como ha sido el de esta mañana. Muchas gracias, señor director.

MEMORIA DE 1998 - ANEXO II - INFORMES PRECEPTIVOS EVACUADOS POR LA AGENCIA DE PROTECCIÓN DE DATOS

-Informe sobre el nuevo texto del 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.
Solicitado por: Secretario General Técnico Ministerio de Justicia
Fecha informe: 08-01-98

-Informe solicitado por el Instituto Nacional de Estadística sobre la posible cesión de datos personales obrantes en los padrones Municipales solicitada por distintas Administraciones Públicas con la finalidad, según manifiestan, de poder cumplir, más satisfactoriamente, las competencias que tienen atribuidas.
Solicitado por: Director General de Estadísticas de Población e Información. I.N.E.
Fecha informe: 09-01-98

-Proyecto de Real Decreto sobre la información a suministrar a los afectados en relación con determinados datos.
Solicitado por: Solicitado por el Secretario General Técnico del Ministerio de Justicia
Fecha informe: 27-01-98

-Proyecto de Real Decreto por el que se aprueba el Reglamento de Archivos Militares
Solicitado por: Solicitado por el Subsecretario del Ministerio de Defensa
Fecha informe: 29-01-98

-Informe sobre el Proyecto de Real Decreto por el que se aprueba el Reglamento del Seguro de Responsabilidad Civil derivada de la circulación de vehículos a motor, de suscripción obligatoria.
Solicitado por: Directora General de Seguros
Fecha informe: 05-02-98

-Informe sobre el borrador del Anteproyecto de Ley Orgánica por el que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que tiene por objeto la adaptación al Derecho español a la Directiva 95/46/CE.
Solicitado por: Secretario General Técnico del Ministerio de Justicia
Fecha informe: 27-02-98

-Resolución del Viceconsejero de Seguridad de 28 de mayo por la que se dictan instrucciones sobre algunos aspectos relativos al tratamiento de datos personales con fines policiales por parte de la Ertzaintza.
Solicitado por: Departamento de Interior del Gobierno Vasco
Fecha informe: 07/05/98

-Informe sobre el proyecto de Reforma del Reglamento Hipotecaria
Solicitado por: Director General de Registros y Notariados
Fecha informe: 20/05/98

-Informe sobre el Proyecto de Real Decreto por el que se crea y regula la especialidad sanitaria de psicología clínica
Solicitado por: Solicitado por la Secretaría General Técnica del Ministerio de Sanidad y Consumo
Fecha informe: 28-05-98

-Informe al Proyecto de Real Decreto por el que se aprueba el Reglameto por el que desarrolla el Título III de la Ley General de telecomunicaciones
Solicitado por: Secretaria General de Telecomunicaciones
Fecha informe: 23/06/98

-Informe sobre la Resolución conjunta de la Presidencia del Instituto Nacional de Estadística y del Director General de Administració Local
Solicitado por: Presidenta del Instituto Nacional de Estadística
Fecha informe: 08/07/98

-Informe al Proyecto de Orden Ministerial por la que se aprueba el modelo de informe psicológico de los militares de empleo de la categoría de tropa y marinería profesionales y de los militares de reemplazo.
Solicitado por: Subsecretaría del Ministerio de Defensa
Fecha informe: 30/07/98

-Informe sobre la Resolución conjunta de la Presidencia del Instituto Nacional de Estadística y del Director General de Administración Local por la que se dictan instrucciones técnicas a los Ayuntamientos sobre uso y cesión de datos del Padrón Municipal.
Solicitado por: Presidenta del Instituto Nacional de Estadística
Fecha informe: 15/09/98

-Informe sobre encuesta de fecundidad 1998

Solicitado por: Director General de Estadística de Población e Información. INE
Fecha informe: 15/09/98

-Informe acerca del Plan para la formación de una Base de Datos Nacional del Catastro en relación a su inclusión en los Anteproyectos de Ley de Presupuestos Generales del Estado y de Medidas Fiscales.
Solicitado por: Subsecretario de Justicia
Fecha informe: 22/09/98

-Informe en relación con el Borrador del Decreto por el que se regula la creación y funcionamiento del Registro de Tumores de Cantabria
Solicitado por: Consejeria de Consumo, Sanidad y Bienestar Social
Gobierno de Cantabria
Fecha informe: 24/09/98

-Informe sobre la nota emitida sobre el informe del borrador del Anteproyecto de Ley Orgánica por el que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que tiene por objeto la adaptación al Derecho español a la Directiva 95/46/CE.
Solicitado por: Secretario de Estado de Justicia
Fecha informe: 30/09/98

-Informe sobre el Anteproyecto de Ley de Medidas Fiscales, Administrativas y de Orden Social del Ministerio de Economía y Hacienda.
Solicitado por: Subsecretario de Justicia
Fecha informe: 02/10/98

-Informe sobre el Proyecto de Real Decreto por el que se aprueba el Reglamento de Ordenación y Supervisión de los Seguros Privados
Solicitado por: Secretario General Técnico de Justicia
Fecha informe: 13/11/98

-Informe sobre el Proyecto de Real Decreto por el que se aprueba el Reglamento del Registro de Organizaciones No Gubernamentales
Solicitado por: Secretario General Técnico de Justicia
Fecha informe: 4/12/98

-Informe sobre el Proyecto de Orden por la que se crea y regula el Índice Nacional de Defunciones
Solicitado por: Director General de Salud Pública
Fecha informe: 16/12/98

-Informe sobre el Proyecto de Resolución del Departamento de Gestión Tributaria por la que se aprueba el modelo de comunicación de la situación personal y familiar del perceptor de rentas de trabajo, o de variación, ante el pagador y se determina la forma en que debe efectuarse dicha comunicación
Solicitado por: Directora del Departamento de Gestión Tributaria
Fecha informe: 23/12/98

MEMORIA DE 1998 - ANEXO III - INSTRUCCIÓN 1/98 DE LA AGENCIA DE PROTECCIÓN DE DATOS RELATIVA AL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN.

(Este documento se encuentra accesible a través de la base de datos "LEGISLACIÓN")

MEMORIA DE 1998 - ANEXO IV - ORDEN DEL MINISTERIO DE JUSTICIA DE 31 DE JULIO DEL 98 POR LA QUE SE AMPLIA LA RELACIÓN DE PAÍSES CON PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EQUIPARABLE A LA ESPAÑOLA, A EFECTOS DE TRANSFERENCIA INTERNACIONAL DE DATOS.

MEMORIA DE 1998 - ANEXO V - PROYECTO DE LEY ORGÁNICA POR LA QUE SE MODIFICA LA LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL

Exposición de motivos

La presente Ley tiene por objeto la adaptación del Derecho español a la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y para ello se procede a introducir en la normativa española reguladora de la materia, contenida en la Ley Orgánica 5/1992, de 29 de octubre, las modificaciones que vienen reclamadas por el contenido de la referida Directiva, a fin de que el conjunto normativo resultante se adapte y acomode a las exigencias de homogeneidad dispositiva establecidas por la Unión Europea.

En el momento de promulgarse la Ley Orgánica 5/1992, de 29 de octubre, que ahora es objeto de modificación, estaba en trámites de discusión y elaboración la Directiva que se transpone, por lo que los contenidos normativos de lo que en aquel tiempo era una mera propuesta se tuvieron en cuenta por el legislador español para dar respuesta a la problemática derivada de la protección de la intimidad en el tratamiento de datos personales. Ello significa que la mencionada Ley Orgánica 5/1992, se ajusta en la gran mayoría de sus previsiones a las disposiciones contenidas en la Directiva 95/46/CE, siendo necesario únicamente introducir en aquélla las precisas reformas que den como resultado la total adecuación entre dicha Ley y la Directiva comunitaria.

Ahora bien, las modificaciones legislativas que para la necesaria adecuación a la Directiva se introducen en la Ley vigente, no por aparentemente exiguas carecen de una singular relevancia, pues en definitiva afectan a aspectos tan importantes como los siguientes: Se amplía el ámbito de aplicación de la Ley, si bien se mantienen determinados supuestos en que no es de aplicación el régimen de protección de datos establecido en la misma; se incrementa la protección de los afectados, tanto en lo que respecta a su necesaria información en la obtención de los datos como en la constante presencia de su consentimiento en el tratamiento y cesión de sus datos personales; se incorpora el derecho del afectado de oponerse al tratamiento de sus datos en determinados supuestos; se prevén nuevos supuestos de excepción en las transferencias internacionales de datos, y se aplican a los ficheros convencionales o no automatizados las disposiciones de la Ley reguladora del tratamiento de datos.

Artículo único. Modificación de la Ley Orgánica 5/1992.

Los artículos que a continuación se relacionan de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, quedan modificados en los términos siguientes:

Uno. En el artículo 1 se sustituye la expresión «tratamiento automatizado de datos de carácter personal» por «tratamiento de datos de carácter personal».

Dos. El apartado 2 del artículo 2 queda redactado de la forma siguiente:

«El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, reguladora del Régimen del Personal Militar Profesional.
d) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.»

Tres. El apartado 3 del artículo 2 queda redactado de la forma siguiente:

«3. Se regirán por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36.»

Cuatro. Se adicionan al artículo 3 las letras g) y h), con el siguiente contenido:

«g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero.
h) Consentimiento del afectado: Toda manifestación de voluntad, libre, específica e informada, mediante la que el afectado consienta el tratamiento de datos personales que le conciernan.»

Cinco. El párrafo primero del apartado 1 del artículo 4 queda redactado de la forma siguiente:

«Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho

tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.»

Seis. El apartado 2 del artículo 4 queda redactado de la forma siguiente:

«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, salvo que el tratamiento posterior de éstos lo sea con fines históricos, estadísticos o científicos.»

Siete. El párrafo tercero del apartado 5 del artículo 4 queda redactado de la forma siguiente:

«Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.»

Ocho. La letra e) del apartado 1 del artículo 5 queda redactada de la forma siguiente:

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

Nueve. El apartado 3 del artículo 5 queda redactado de la forma siguiente:

«No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se precisa reformas que den como resultado la total adecuación entre dicha Ley y la Directiva comunitaria. Ahora bien, las modificaciones legislativas que para la necesaria adecuación a la Directiva se introducen en la Ley vigente, no por aparentemente exiguas carecen de una singular relevancia, pues en definitiva afectan a aspectos tan importantes como los siguientes: Se amplía el ámbito de aplicación de la Ley, si bien se mantienen determinados supuestos en que no es de aplicación el régimen de protección de datos establecido en la misma; se incrementa la protección de los afectados, tanto en lo que respecta a su necesaria información en la obtención de los datos como en la constante presencia de su consentimiento en el tratamiento y cesión de sus datos personales; se incorpora el derecho del afectado de oponerse al tratamiento de sus datos en determinados supuestos; se prevén nuevos supuestos de excepción en las transferencias internacionales de datos, y se aplican a los ficheros convencionales o no automatizados las disposiciones de la Ley reguladora del tratamiento de datos.

Artículo único. Modificación de la Ley Orgánica 5/1992.
Los artículos que a continuación se relacionan de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, quedan modificados en los términos siguientes:

Uno. En el artículo 1 se sustituye la expresión «tratamiento automatizado de datos de carácter personal» por «tratamiento de datos de carácter personal».

Dos. El apartado 2 del artículo 2 queda redactado de la forma siguiente:

«El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, reguladora del Régimen del Personal Militar Profesional.
d) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.»

Tres. El apartado 3 del artículo 2 queda redactado de la forma siguiente:

«3. Se regirán por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36.»

Cuatro. Se adicionan al artículo 3 las letras g) y h), con el siguiente contenido:

«g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero.
h) Consentimiento del afectado: Toda manifestación de voluntad, libre, específica e informada, mediante la que el afectado consienta el tratamiento de datos personales que le conciernan.»

Cinco. E1 párrafo primero del apartado 1 del artículo 4 queda redactado de la forma siguiente:

«Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.»

Seis. El apartado 2 del artículo 4 queda redactado de la forma siguiente:

«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, salvo que el tratamiento posterior de éstos lo sea con fines históricos, estadísticos o científicos.»

Siete. El párrafo tercero del apartado 5 del artículo 4 queda redactado de la forma siguiente:

«Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.»

Ocho. La letra e) del apartado 1 del artículo 5 queda redactada de la forma siguiente:

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

Nueve. El apartado 3 del artículo 5 queda redactado de la forma siguiente:

«No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales
que se solicitan o de las circunstancias en que se recaban.»

Diez. Se adicionan al artículo 5 los siguientes apartados 4 y 5:

«4. Cuando los datos de carácter personal no hayan sido recabados del afectado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido de los datos, de su procedencia, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando el tratamiento de datos esté expresamente previsto en una Ley cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al afectado resulte imposible o exija esfuerzos desproporcionados a criterio de la Agencia de Protección de Datos, en consideración al número de afectados, a la antigüedad de los datos y a las posibles medidas compensatorias.»

Once. El apartado 1 del artículo 6 queda redactado
de la forma siguiente:

«El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.»

Doce. El apartado 2 del artículo 6 queda redactado de la forma siguiente:

«No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del afectado; o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos.»

Trece. Se adiciona un apartado 4 al artículo 6, con el contenido siguiente:

«4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.»

Catorce. El apartado 2 del artículo 7 queda redactado de la forma siguiente:

«Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mante-

nidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.»

Quince. El apartado 4 del artículo 7 queda redactado de la forma siguiente:

«Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o vida sexual.»

Dieciséis. Se adiciona un apartado 6 al artículo 7, con el siguiente contenido:

«No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento automatizado los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un
profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento automatizado los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.»

Diecisiete. En el apartado 1 del artículo 9 se sustituye la expresión «El responsable del fichero deberá adoptar», por la de «El responsable del fichero y, en su caso, el encargado del tratamiento, deberá adoptar».

Dieciocho. La letra d) del apartado 2 del artículo 11 queda redactada de la forma siguiente:

«Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas.»

Diecinueve. Se adiciona un segundo inciso al artículo 12, con el siguiente contenido:

«En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre la lógica utilizada en los tratamientos de datos referidos a aquél.»

Veinte. El apartado l del artículo 14 queda redactado de la forma siguiente:

«El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados, así como sobre el origen de dichos datos.»

Veintiuno. El apartado 2 del artículo 15 queda redactado de la forma siguiente:

«Serán rectificados y cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y en particular cuando tales datos resulten inexactos o incompletos.»

Veintidós. El apartado 1 del artículo 19 queda redactado de la forma siguiente:

«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 hubiere sido prevista por las disposiciones de creación del fichero o por disposición posterior de superior rango que regule su uso, o cuando la cesión tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.»

Veintitrés. El apartado 3 del artículo 20 queda redactado de la forma siguiente:

«La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.»

Veinticuatro. En el apartado 1 del artículo 22 se suprime la expresión «o dificulte gravemente».

Veinticinco. El apartado 1 del artículo 29 queda redactado de la forma siguiente:

«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 hayan sido facilitados por los propios afectados u obtenidos con su consentimiento o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos.»

Veintiséis. Se adiciona un artículo 30 bis con el siguiente contenido:

«Artículo 30 bis. Tratamientos destinados a la prospección. En los supuestos de tratamientos de datos de carácter personal destinados a la prospección, los afectados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, así como a ser informados por el responsable del fichero antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se les ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.»

Veintisiete. La letra c) del artículo 33 queda redactada de la forma siguiente:

«Cuando la transferencia sea necesaria para la salvaguarda del interés vital del afectado.»

Veintiocho. Se adicionan al artículo 33 las letras e), f), g), h), i), j) y k), con el siguiente contenido:

«e) Cuando el afectado haya dado su consentimiento inequívocamente a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público importante. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea.»

Veintinueve. El apartado 1 del artículo 42 queda redactado de la forma siguiente:

«Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.»

Treinta. La disposición final segunda queda redactada de la forma siguiente:

«Las disposiciones de la presente Ley se aplicarán a los tratamientos no automatizados de datos de carácter personal contenidos o destinados a ser contenidos en un fichero. Quedan excluidas a estos efectos las carpetas que no estén estructuradas.»

DISPOSICIÓN ADICIONAL
Única. Ficheros preexistentes
Los ficheros y tratamientos automatizados que, como consecuencia de las modificaciones introducidas en la Ley Orgánica 5/1992, de 29 de octubre, quedan incluidos en el ámbito de aplicación de ésta, deberán ajustarse a la misma dentro del plazo de tres años, a contar desde la entrada en vigor de la presente Ley Orgánica. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la Ley Orgánica 5/1992, de 29 de octubre, y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

DISPOSICIONES FINALES
Primera. Carácter de la Ley
Los apartados veintidós, veinticinco, veintiséis y veintinueve del artículo único y la disposición adicional única tienen carácter de Ley ordinaria.
Segunda. Entrada en vigor

La presente Ley Orgánica entrará en vigor al mes de su publicación en el «Boletín Oficial del Estado».

MEMORIA DE 1998 - ANEXO VI - CÓDIGO ÉTICO DE PROTECCIÓN DE DATOS PERSONALES EN INTERNET

PREÁMBULO

La LORTAD, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Sin embargo, al aparecer Internet como nuevo medio de comunicación, existen ciertos vacíos en la normativa actual que provocan una desprotección en el consumidor.

En consecuencia, la **Asociación Española de Comercio Electrónico (AECE)** reconoce la necesidad de regular mediante unas normas de compromiso voluntario por parte de las empresas que operan en Internet, con el fin de proteger la intimidad de las personas en el tratamiento automatizado de los datos de carácter personal en Internet.
Podrán adherirse al **Código Ético** todas aquellas empresas que comercializan productos o servicios en Internet y tratan datos personales.

Las ventajas de adherirse al código son las siguientes:
1. Aumento de la confianza del consumidor potencial para adentrarse en este nuevo mercado que supone tantas facilidades y comodidades.
2. Posibilidad de utilización del **Sello de Garantía**, que posiciona a la empresa como una entidad seria y preocupada por la protección de la intimidad de las personas.

En el **Código** existe un capítulo que contiene unos principios adicionales aplicables a las actividades on-line dirigidas principalmente a menores, los cuales en comparación con los adultos pueden no entender la naturaleza de la información que se les pide o los usos a los cuales se puede destinar la información. Por razones de diferencias de madurez, los anunciantes que operan On-line o en webs de Internet dirigidos principalmente a menores se comprometen a animar a los padres a participar y supervisar las experiencias on-line de sus hijos.

No se pretende, por tanto, en este **Código**, tratar de sustituir a los padres ni asumir las responsabilidades que les corresponden respecto de su participación en las actividades de sus hijos en orden a encaminar su educación hacia la madurez y conocimiento de la trascendencia de sus actos, ni impedir a los menores su participación en los sistemas de comunicación, ya que, como manifiesta la Ley orgánica 1/1996, de protección del menor, deben ser considerados como sujetos activos, participativos y creativos, con capacidad de modificar su propio medio personal y social; de participar en la búsqueda y satisfacción de sus necesidades y en la satisfacción de las necesidades de los demás, siendo la mejor forma de garantizar social y jurídicamente la protección a la infancia la promoción de su autonomía como sujetos. En atención a estos principios, la citada ley de protección del menor garantiza a estos el derecho a buscar, recibir y utilizar la información adecuada a su desarrollo, responsabilizando a los padres o tutores y los poderes públicos de que la información que reciban sea veraz, plural y respetuosa con los principios constitucionales.

El **Código Ético** facilita a estos colectivos el cumplimiento de tales responsabilidades mediante el compromiso de las empresas que lo suscriben de atender a los principios establecidos en la citada Ley en cuanto a la información que se solicite y dirija a los menores, y garantiza a los padres la posible intervención en las relaciones de los menores con las empresas de comercio electrónico.

Las obligaciones de este **código** recaerán sobre las empresas que operan en Internet y que se adhieran voluntariamente al mismo:

• Tanto en las relaciones de la empresa con el consumidor, cuando se traten datos personales,
• Como en las relaciones de la empresa con otra empresa, cuando se traten datos personales.
Todas las empresas que voluntariamente se adhieran al código podrán utilizar el "sello de garantía de protección de datos"

Aunque los principios de **Protección de Datos de la AECE** son aplicables en cualquier tipo de medio, los siguientes principios y ejemplos enfocan temas específicos del Marketing On-line y en Internet.

Principalmente se tratan las obligaciones del anunciante en Internet de informar a los usuarios que entren en su Web, sobre sus derechos con el fin de proteger sus datos personales. Asimismo se determinarán las obligaciones del anunciante de no vulnerar la privacidad de quienes entren en su web, garantizando así los derechos de los ciudadanos.

CÓDIGO ÉTICO

CAPÍTULO PRIMERO

PRINCIPIOS GENERALES.

ARTÍCULO 1: *Definiciones*

A los efectos del presente Código, se entenderá por:

a) *Consumidor:* Persona física titular de los datos que sean objeto de tratamiento.
b) *Anunciante*: Persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento.
c) *Menor*: Persona que no haya alcanzado los dieciocho años de edad.

ARTÍCULO 2: *Seguridad en las Conexiones*

Las Empresas adheridas a este Código deberán contratar la provisión del servicio de Internet únicamente con empresas que estén a su vez adheridas al mismo o que garanticen el cumplimiento de las obligaciones que de él se derivan.

ARTÍCULO 3: *Seguridad en la Red.*

Las empresas anunciantes que no cuenten con un sistema de conexión segura que restrinja la posibilidad de captación por terceros de los datos personales que estén obteniendo On-line, deberán advertirlo a los consumidores, especialmente en el caso de recabación de datos relativos a tarjetas de crédito y cuentas bancarias.

CAPÍTULO SEGUNDO

DERECHOS DE LOS CONSUMIDORES

ARTÍCULO 4: *Deber de Información*

Las empresas que se anuncian en Internet y recaben, capturen y traten datos personales, deberán informar a los consumidores, mediante un aviso en su Web, de dicho tratamiento.

De esta forma, el consumidor podrá, si lo desea, ejercer su derecho de oposición, tanto en lo que se refiere a la captación como al tratamiento y transferencia de los datos.

El anunciante deberá incluir el sello de garantía en su página de inicio (home page) cuya selección proporcionará al consumidor un acceso a pantallas donde se detallará el aviso.

El aviso deberá ser fácilmente localizable y de fácil comprensión y siempre deberá contener, como mínimo, la siguiente información:

Identificación indubitada de la empresa.

Una dirección de E-mail así como una dirección postal u otro sistema de comunicación, a través de los cuales se puedan ejercer los derechos de acceso, rectificación, cancelación y de especificación de las finalidades para las que autoriza el uso de sus datos.

En su caso, el hecho de la captación de información almacenada en el equipo informático y el tipo de información que se capta.

En su caso, del hecho de colocación de cookies.

De la finalidad ó finalidades a que se destina la información obtenida.

En su caso, de la intención de ceder los datos, especificando la información a ceder así como la finalidad a que se destinarán los datos cedidos

ARTÍCULO 5: *Derecho de oposición*

La empresa que opera en internet tendrá la obligación de garantizar al consumidor el ejercicio de su derecho de oposición.

1. El consumidor podrá oponerse siempre:

Al tratamiento de sus datos, salvo que el tratamiento sea necesario para la ejecución de los contratos celebrados.

A que sus datos sean utilizados para alguna o algunas de las finalidades determinadas en la información sobre el tratamiento.

A la cesión de la información a terceros.

2. Para la efectividad de estos derechos se informará sobre su posible ejercicio y de los modos de ejercitarlos.

3.En el caso de que se esté captando información almacenada en el equipo informático, el derecho de oposición deberá poder ejercerse mediante un sistema On-line.

En el caso de que la información se recabe del consumidor, esto es, cuando se le solicite que rellene un cuestionario o se almacene información facilitada por él para el establecimiento de relaciones comerciales, el ejercicio del derecho de oposición deberá ser muy sencillo, mediante una dirección de E-mail.

4.- En la recabación del consentimiento deberán distinguirse los diferentes aspectos para los que se solicita éste, con la posibilidad de oponerse diferenciadamente a cada uno de los puntos anteriores.

5.- En todo caso, deberá facilitarse siempre una dirección postal u otro sistema de comunicación, que no suponga gastos ni incomodidades superiores a ésta, para el posible ejercicio de estos derechos.

ARTÍCULO 6: *Finalidad*

El consumidor podrá, en cualquier momento, determinar la finalidad o finalidades a que consiente que sean destinados sus datos, o excluir alguna finalidad inicialmente consentida.

En ningún caso, las empresas podrán utilizar la información para finalidades distintas de las que haya consentido el consumidor, salvo que, previamente, le hayan advertido de la intención de hacerlo otorgándole un plazo y un procedimiento razonables para oponerse.

ARTÍCULO 7: *Cesiones y Finalidad de la Cesión*

La información relativa a la posible cesión de los datos deberá siempre identificar a los cesionarios o, en todo caso hacer referencia a las características de las empresas o personas a quienes se vayan a ceder los datos, así como a las finalidades perseguidas con la cesión.

En ningún caso podrán cederse datos relativos a la facturación procedente de las relaciones comerciales que se mantengan o se hayan mantenido con el consumidor, salvo que lo disponga la Ley.

MARKETING POR E-MAIL

ARTICULO 8: *Emisión de Publicidad*

Las ofertas de publicidad por E-mail se podrán enviar a clientes de la propia empresa si no se hubieran opuesto previamente a ella. También se podrán enviar a grupos de noticias (newsgroups), tablón de anuncios (bulletin boards) y foros de charlas (chats) cuando sean coherentes con las políticas declaradas en el tema del foro en cuestión.

Para facilitar el cumplimiento de este principio, los operadores de los foros adheridos al código deberán publicar las políticas aplicables a las posibles ofertas en su foro.

Los anunciantes deberán consultar las políticas del foro antes de dirigir ofertas por E-mail al foro, respetando, en su caso la oposición colectiva manifestada por el moderador.

ARTÍCULO 9: *Información al Consumidor*

Los anunciantes que operen en foros de charla, grupos de noticias y otros foros públicos, deberán informar expresa y previamente a los individuos que visitan estos espacios, de que la información proporcionada por ellos en estas zonas no protegidas puede ser captada y utilizada por empresas no adheridas al Código y puede dar lugar a la recepción de mensajes no solicitados.

Los anunciantes también deberán apoyar iniciativas para ayudar a educar al consumidor sobre cómo proteger su intimidad en la Red.

ARTICULO 10: *Uso de la Técnica del Spam* .

Las fuentes de publicidad por E-mail deberán identificarse claramente como tales en el subject del E-mail, revelando asimismo la identidad del anunciante.

Aquellos anunciantes que utilizan E-mail deberán informar sobre la posibilidad de notificar al anunciante su deseo de no recibir ofertas posteriores y proporcionar un mecanismo a través del cual el consumidor pueda ejercitar este derecho.

Las ofertas deberán identificarse de modo que el que las recibe pueda reconocerlas inmediatamente como ofertas.

Los consumidores deberán poder oponerse por E-mail o por cualquier otro medio de comunicación a la recepción de este tipo de ofertas. El anunciante deberá indicar claramente dónde puede dirigirse el consumidor para ejercer su Derecho de Oposición, especialmente si la dirección electrónica es distinta de la que envía las ofertas.

La información que se almacene en las denominadas "listas de no abonados" será la mínima e imprescindible para

evitar el envío de publicidad no deseada.

ARTÍCULO 11: *Explotación de las Listas de Datos.*

Todas aquellas empresas involucradas en la utilización, alquiler, venta o intercambio de listas de datos a fin de realizar ofertas por E-mail, deberán tomar medidas para garantizar que esa explotación de los datos cumple con los principios de este Código Ético.

Los anunciantes deberán incorporar estos principios en sus contratos de alquiler de listados, exigiendo el compromiso de su cumplimiento por parte de quien contrate con ellos, y proporcionar una copia del Código Ético de Protección de Datos Personales en Internet editado por la AECE, a terceros.

ARTÍCULO 12: *Uso de Listas elaboradas a partir de fuentes accesibles al público* .

Al utilizar listados de direcciones electrónicas elaborados a partir de fuentes accesibles al público, los anunciantes deberán asegurarse de que los consumidores incorporados a dichas listas hayan tenido la opción de ver eliminadas sus direcciones electrónicas.

En el caso de que estas listas hayan sido elaboradas por otros, los anunciantes deberán exigir contractualmente que los titulares de las listas incluyan únicamente las direcciones electrónicas de personas que no se hayan opuesto al uso a que pretenden destinar los datos así obtenidos.

CAPITULO TERCERO

TRATAMIENTO DE DATOS SOBRE LOS MENORES

ARTICULO 13: *Objeto de la Comunicación con los Menores de edad* .

Para recoger datos o de comunicarse On-line con menores, las empresas anunciantes deberán tener en cuenta la edad, el conocimiento y la madurez de su público objetivo.

En ningún caso podrán recabarse del menor de edad datos relativos o relacionados con la situación económica o la intimidad de los otros miembros de la familia.

ARTÍCULO 14: *Ámbito de aplicación de los principios referidos a menores.*

Las previsiones establecidas en este Código que se refieren a la obtención y tratamiento de datos de menores, se entienden referidos a los datos obtenidos a través de las consultas y visitas a las páginas Web que ofrezcan productos, servicios e información destinadas, principalmente, a niños menores de dieciocho años.

ARTÍCULO 15: *Intervención de los Padres en el Tratamiento de los Datos de sus Hijos menores* .

Los anunciantes deberán atender las preocupaciones de los padres sobre la recopilación de los nombres, direcciones y cualquier otra información sobre sus hijos menores.

Los anunciantes deberán facilitar la posibilidad de que los padres puedan ejercer los derechos de acceso, cancelación y determinación de la finalidad sobre los datos de sus hijos. La cancelación y determinación de la finalidad podrán ejercerse por medio de un aviso que será conservado por el anunciante y deberá ser respetado siempre.

En el caso de que el menor conecte con la página del anunciante y solicite que se le remita información o publicidad, en contra del aviso de sus padres, no podrá atenderse dicha solicitud.

La contradicción de dicho aviso sólo podrá hacerse por los padres mediante correo no electrónico, de modo que pueda comprobarse la autoría de la nueva comunicación.

Los anunciantes deberán animar a los menores para que consulten con sus padres antes de proporcionar datos.

Los anunciantes también deberán apoyar cualquier esfuerzo que se realice, por parte de otros Organismos para ayudar a informar a los padres sobre cómo proteger On-line la intimidad de sus hijos, incluyendo información sobre herramientas de software y control de acceso para los padres, que impidan que los niños proporcionen su nombre, dirección y otros datos personales.

ARTICULO 16: *Uso de los Datos de Menores.*

Además del respeto a la opción de los padres de limitar la recopilación de estos datos On-line, las empresas anunciantes deberán limitar la utilización de datos proporcionados por los menores a la única finalidad de la promoción, venta y suministro de sus productos y servicios dirigidos a menores.

En ningún caso podrán cederse los datos relativos a menores, ni utilizarse para campañas que sean inadecuadas para

la edad correspondiente al menor.

ARTÍCULO 17: *Información del uso de los datos relativos a menores.*

Las empresas anunciantes también deberán clarificar que la información relativa a menores se solicita exclusivamente para fines comerciales de promoción de los productos y servicios de la empresa anunciante.

ARTICULO 18: *Medidas de Seguridad*

Los anunciantes deberán establecer unas medidas de seguridad estrictas para asegurarse contra el acceso, alteración o cesión de datos de menores obtenidos On-line.

CAPITULO CUARTO

MODALIDADES DE UTILIZACIÓN DEL SELLO DE GARANTÍA

ARTÍCULO 19: *Objeto.*

El Sello de Garantía creado por la Asociación tiene por objeto el reconocimiento de las empresas que han aceptado cumplir las normas éticas incluidas en el mismo.

ARTÍCULO 20: *Obtención*

Únicamente las empresas adheridas al Código Ético pueden utilizar el Sello de Garantía y se comprometerán por escrito dirigido a la AECE a aplicarlo en cualquier circunstancia. La utilización del Sello es facultativa. Es obvio, sin embargo, que cada cual se aprovechará de la publicidad hecha por los otros miembros, por lo que afecta al interés de todos el promover la difusión de este Sello.

ARTÍCULO 21: *Modalidades de Utilización.*

Dado su objeto esencial, que es el de constituir una marca distintiva colectiva, el Sello no podrá ser dispuesto ni, en todo caso, utilizado en los documentos de venta o en la publicidad, de tal forma que pueda ser considerado:

1. ya sea como una marca propia de la empresa usuaria,
2. ya sea como una garantía (en especial, de origen o de calidad) de los productos o de servicios ofrecidos a la venta.

La AECE se reserva el derecho, en todo momento, de apreciar y controlar las condiciones de utilización del Sello y de tomar todas las disposiciones útiles en caso de utilización anómala.

A este efecto, las empresas usuarias de la marca colectiva se comprometen a aplicar sin demora y sin reserva las instrucciones de utilización que les sean comunicadas por la Asociación.

Queda prohibida, salvo autorización expresa y escrita de la Asociación, cualquier reproducción del Sello que se utilice fuera de las páginas Web de la empresa anunciante adherida al código.

CAPÍTULO QUINTO

CONTROL DEL CUMPLIMIENTO DE LAS NORMAS DEL CÓDIGO Y RESOLUCIÓN DE LOS LITIGIOS.

ARTÍCULO 22: *Control de cumplimiento*

El control del cumplimiento de las normas del código ético se realizará por el comité de Protección de Datos de la AECE (a partir de ahora el Comité).

El Comité estará compuesto por 10 personas, de las cuales, 5 de ellas serán miembros de la Junta Directiva de la Asociación, habrá 4 representantes de Asociaciones de Consumidores y un representante de la Asociación de Auto-control de la Publicidad.

El Comité será convocado por su presidente o por un tercio de sus miembros en el caso de que se tenga noticia de la violación de alguna de las normas del código.

El Comité realizará un programa anual de auditorías sistemáticas y al azar, entre las empresas que se adhieran voluntariamente al código ético y utilicen el Sello de Garantía, con el fin de comprobar el cumplimento de las normas.

El Comité tomará sus decisiones en materia de litigios, por mayoría de 3/4 partes de los votos de los miembros presentes.

La empresa afectada por el procedimiento podrá hacerse oír por el Comité, y podrá hacerse asistir también por un

experto.

ARTÍCULO 23: *Presentación de Reclamaciones.*

Cuando un consumidor considere que una empresa que utiliza el Sello de Garantía de Protección de Datos de la AECE ha actuado contra este código, podrá remitir una queja por E-mail o por carta a la empresa anunciante responsable del fichero, o a la dirección de la Junta Directiva de la Asociación de Comercio Electrónico.

En el caso de que el responsable del fichero no justifique suficientemente la inexistencia de incumplimiento o no satisfaga al consumidor en el plazo de cinco días, el consumidor tiene derecho a presentarla ante el Comité de Protección de Datos de la AECE, tanto por E-mail como por carta, aportando todas las pruebas que se estimen útiles.

ARTÍCULO 24: *Sanciones.*

El Comité apreciará, en función de la gravedad del caso y de los daños causados, las sanciones aplicar. Estas podrán ser de:

Advertencia

Amonestación

Retirada temporal del Sello de Garantía

Retirada definitiva del Sello de Garantía

Propuesta de expulsión de la AECE (aplicable sólo a los miembros de la AECE y de acuerdo con el procedimiento establecido en los Estatutos de la AECE).

ARTÍCULO 25: *Notificación, Publicidad y Acciones Legales.*

El aviso o la sanción del Comité serán notificados a la empresa y a la persona interesada, por medio del Secretario del citado Comité. El Comité se reserva el derecho de dar publicidad externa a la sanción.

En el caso de existencia de violaciones a los principios de la Ley Orgánica de Protección de los Datos de carácter Personal, el Comité podrá presentar denuncia ante la Agencia de Protección de Datos.

DISPOSICIÓN FINAL

ARTÍCULO 26: *Revisión y Actualización de este Código.*

Cada dos años se planteará la oportunidad de revisar el contenido de este Código Deontológico a fin de actualizarlo a las innovaciones técnicas y de comportamiento del sector. La revisión que se proponga deberá presentarse para su inscripción en el Registro General de la Agencia de Protección de Datos.

LA POLÍTICA DE LA INTIMIDAD EN EL WEB DE LA AECE

Como consecuencia de lo dicho anteriormente, la AECE desarrollará marcos y programas para cubrir las expectativas de intimidad del consumidor, informando a éstos sobre la utilización de sus datos y ofreciéndoles la opción de eliminar sus nombres de las listas de E-mail (Sistema similar al Servicio de Listas Robinson, para la publicidad por correo).

La AECE tendrá el Servicio de Asesoría de Protección de Datos Personales para todos sus miembros. Las personas que se comuniquen con la AECE, y por tanto proporcionen una dirección de E-mail, recibirán comunicaciones posteriores de la Asociación por E-mail. Aquellos que no deseen recibir mensajes de E-mail de la AECE lo podrán notificar vía E-mail al departamento de socios. Las direcciones de E-mail NO serán cedidas ni vendidas a terceros.

Aquellas personas que soliciten información sobre la AECE, sus servicios o programas educativos y que proporcionen a la Asociación su nombre y dirección de correos, se añadirán a nuestra base de datos a fin de poder recibir envíos de la Asociación relacionados con programas y eventos organizados por la Asociación. En el tratamiento automatizado de estos datos la AECE cumplirá con todas las garantías establecidas en este Código. Asimismo la AECE informará a estas personas que soliciten información, la naturaleza de las entidades a las que la AECE podría ceder sus datos si le son facilitados.

Puntualmente la AECE ofrecerá la posibilidad de acceso a las direcciones postales recogidas en su Web a otras asociaciones o a las empresas miembros de dichas asociaciones para ofertar productos o servicios cuidadosamente seleccionados que pudieran ser de su interés. Asimismo, ofrecerá la posibilidad, a quien no desee recibir estas ofertas de notificarlo de forma expresa.

La AECE ayuda a sus empresas miembros a crear sus propias Declaraciones de Política de Intimidad. Estas declaraciones serán afines con los Principios de Intimidad me Marketing On-line de la Asociación. La AECE está creando una sección especial en su Web. El emplazamiento permitirá que los creadores de Webs y administradores confeccionen y

coloquen On-line una declaración de política de intimidad ajustada a las prácticas especificas de la empresas. Cuando la empresa responda a varias preguntas basada en la política de información de su emplazamiento, esta herramienta de recursos recogerá las respuestas automáticamente, creando un documento privado de principios de intimidad que podrá ser editado y colocado directamente en una Web. La dirección de la herramienta de políticas de intimidad de la AECE será: (http://www.aece.org).

LA AECE LE AYUDA A CREAR LA POLÍTICA DE PRIVACIDAD ON-LINE DE SU EMPRESA.

Rellene el siguiente cuestionario y le enviaremos una página Web para incluir en el Web de su empresa.

La AECE considera que cualquier empresa que haga marketing Directo on-line, debe poner a disposición del consumidor una guía de Privacidad en un lugar visible de su Web.

Para ayudar a las empresas a crear su propia Guía de Privacidad, la AECE ha creado una sección en su Web dedicada a ello, en la que la empresa deberá rellenar un cuestionario. Esta herramienta ha sido desarrollada para ayudar a las empresas a crear su propia Guía de Privacidad (o Declaración de Política de Intimidad) acorde con el Código Ético de la AECE para Marketing On-line.

FIN

MEMORIA DE 1998 - ANEXO VII - CONVENIO EUROPOL

CONVENIO BASADO EN EL ARTICULO K.3 DEL TRATADO DE LA UNION EUROPEA POR EL QUE SE CREA UNA OFICINA EUROPEA DE POLICIA (CONVENIO EUROPOL)

Las altas partes contratantes del presente Convenio, Estados miembros de la Unión Europea,
Considerando el acto del Consejo de fecha...
Conscientes de los problemas urgentes que plantean el terrorismo, el tráfico ilícito de drogas y otras formas graves de delincuencia internacional;
Considerando que es necesario realizar avances en la solidaridad y la cooperación entre los Estados miembros de la Unión Europea, en particular mejorando la cooperación policial entre ellos;
Considerando que el propósito de dichos avances es poder mejorar más aún la protección del orden y la seguridad públicos;
Considerando que en el Tratado de la Unión Europea, de 7 de febrero de 1992, se convino la creación de una Oficina Europea de Policía (Europol);
Considerando la Decisión del Consejo Europeo de 29 de octubre de 1993, que dispone que Europol se establezca en los Países Bajos y tenga su sede en La Haya;
Recordando el objetivo común consistente en lograr una mejora de la cooperación policial en el ámbito del terrorismo, del tráfico ilícito de drogas y de otras formas graves de delincuencia internacional mediante un intercambio de información permanente, seguro e intensivo entre Europol y las unidades nacionales de los Estados miembros;
Teniendo en cuenta que las formas de cooperación establecidas en el presente Convenio no deben afectar a otras formas de cooperación bilateral o multilateral;
Convencidas de que la cooperación policial es uno de los ámbitos en que ha de concederse particular atención a la protección de los derechos del individuo, en particular a la protección de sus datos personales;
Considerando que las actividades de Europol con arreglo al presente Convenio no afectan a las competencias de las Comunidades Europeas; que Europol y las Comunidades Europeas comparten dentro de la Unión Europea un mismo interés en que se establezcan unas formas de cooperación que permitan a ambas ejercer con la máxima eficacia sus respectivas funciones,
Han convenido en lo siguiente:

INDICE

Título I. Creación y descripción de funciones.
Artículo 1. Creación.
Artículo 2. Objetivos.
Artículo 3. Funciones.
Artículo 4. Unidades nacionales.
Artículo 5. Funcionarios de enlace.
Artículo 6. Sistema informatizado de recogida de datos.
Título II. Sistema de información.
Artículo 7. Creación del sistema de información.
Artículo 8. Contenido del sistema de información.
Artículo 9. Derecho de acceso al sistema de información.
Título III. Ficheros de trabajo con fines de análisis.
Artículo 10. Recogida, tratamiento y utilización de datos personales.
Artículo 11. Sistema de índice.
Artículo 12. Disposición de creación de ficheros.
Título IV. Disposiciones comunes relativas al tratamiento de la información.
Artículo 13. Obligación de informar.
Artículo 14. Nivel de protección de los datos.
Artículo 15. Responsabilidad en materia de protección de datos.
Artículo 16. Normas sobre constancia documental.
Artículo 17. Normas de utilización.
Artículo 18. Transmisión de datos a Estados e instancias terceros.
Artículo 19. Derecho de acceso.
Artículo 20. Rectificación y supresión de datos.
Artículo 21. Plazos de conservación y supresión de los ficheros.
Artículo 22. Conservación y rectificación de datos que figuren en expedientes.
Artículo 23. Autoridad nacional de control.
Artículo 24. Autoridad común de control.
Artículo 25. Seguridad de los datos.
Título V. Estatuto jurídico, organización y disposiciones financieras.
Artículo 26. Capacidad jurídica.
Artículo 27. Organos de Europol.
Artículo 28. Consejo de Administración.
Artículo 29. Director.
Artículo 30. Personal.
Artículo 31. Confidencialidad.
Artículo 32. Obligación de reserva y confidencialidad.

Artículo 33. Lenguas.
Artículo 34. Información al Parlamento Europeo.
Artículo 35. Presupuesto.
Artículo 36. Censura de cuentas.
Artículo 37. Acuerdo de sede.
Título VI. Responsabilidad y protección jurídica.
Artículo 38. Responsabilidad en caso de tratamiento ilícito o incorrecto de datos.
Artículo 39. Otros tipos de responsabilidad.
Artículo 40. Resolución de controversias y de litigios.
Artículo 41. Privilegios e inmunidades.
Título VII. Disposiciones finales.
Artículo 42. Relaciones con Estados e instancias terceros.
Artículo 43. Modificación del Convenio.
Artículo 44. Reservas.
Artículo 45. Entrada en vigor.
Artículo 46. Adhesión de nuevos Estados miembros.
Artículo 47. Depositario.
Anexo mencionado en el artículo 2.
Declaraciones.

TITULO I

Creación y descripción de funciones

Artículo 1. Creación.

1. Los Estados miembros de la Unión Europea, denominados en lo sucesivo los Estados miembros, crean por el presente Convenio una Oficina Europea de Policía, denominada en lo sucesivo Europol.

2. Europol estará vinculada en cada Estado miembro a una única unidad nacional que se creará o designará de conformidad con lo dispuesto en el artículo 4.

Artículo 2. Objetivos.

1. El objetivo de Europol consiste en mejorar, en el marco de la cooperación entre los Estados miembros de conformidad con el punto 9 del artículo K.1 del Tratado de la Unión Europea, por medio de las actividades que se enumeran en el presente Convenio, la eficacia de los servicios competentes de los Estados miembros y la cooperación entre los mismos con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional, en la medida en que existan indicios concretos de una estructura delictiva organizada y que dos o más Estados miembros se vean afectados por las formas de delincuencia antes mencionadas, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros.

2. Para alcanzar progresivamente los objetivos mencionados en el apartado 1, Europol actuará en primer lugar en materia de prevención y lucha contra el tráfico ilícito de estupefacientes, de material nuclear y radiactivo, las redes de inmigración clandestina, la trata de seres humanos y el tráfico de vehículos robados.

Europol se ocupará también, en un plazo máximo de dos años a partir de la entrada en vigor del presente Convenio, de los delitos cometidos o que puedan cometerse en el marco de actividades de terrorismo que atenten contra la vida, la integridad física y la libertad de las personas, así como contra sus bienes. El Consejo podrá decidir por unanimidad, de acuerdo con el procedimiento establecido en el Título VI del Tratado de la Unión Europea, encargar a Europol que se ocupe de estas actividades terroristas antes de la expiración del plazo.

El Consejo podrá decidir por unanimidad, de acuerdo con el procedimiento establecido en el Título VI del Tratado de la Unión Europea, encomendar a Europol que se ocupe de otras formas de delincuencia de las mencionadas en el anexo del presente Convenio o de aspectos específicos de las mismas. Antes de decidir, el Consejo encargará al Consejo de Administración de Europol que elabore la resolución pertinente y en particular que exponga las consecuencias que tendrá para Europol en términos presupuestarios y de personal.

3. La competencia de Europol sobre una forma de delincuencia o sobre aspectos específicos de la misma abarcará igualmente:

1) El blanqueo de dinero ligado a esas formas de delincuencias o a sus aspectos específicos.

2) Los delitos conexos.

Se considerarán conexos y se tendrán en consideración con arreglo a las modalidades establecidas en los artículos 8 y 10:

Los delitos cometidos con objeto de procurarse los medios para perpetrar los actos que sean competencia de Europol.

Los delitos cometidos para facilitar o consumar la ejecución de los actos que sean competencia de Europol.

Los delitos cometidos para conseguir la impunidad de los actos que sean competencia de Europol.

4. A los efectos del presente Convenio, se entenderá por servicios competentes todos los organismos públicos existentes en los Estados miembros, siempre que en virtud del Derecho nacional sean competentes para prevenir y combatir la delincuencia.

5. A los efectos de los apartados 1 y 2, se entenderá por tráfico ilícito de estupefacientes los actos delictivos mencionados en el apartado 1 del artículo 3 de la Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias psicotrópicas, de 20 de diciembre de 1988 (RCL 1990\2309), y en las disposiciones que la modifican o sustituyen.

Artículo 3. Funciones.

1. Para alcanzar los objetivos definidos en el apartado 1 del artículo 2, Europol desempeñará prioritariamente las

siguientes funciones:
1) Facilitar el intercambio de información entre los Estados miembros.
2) Recoger, compilar y analizar informaciones y datos.
3) Comunicar sin demora a los servicios competentes de los Estados miembros, por medio de las unidades nacionales que se definen en el artículo 4, los datos que les afecten y la relación entre los actos delictivos de los que hayan tenido conocimiento.
4) Facilitar las investigaciones en los Estados miembros transmitiendo a las unidades nacionales toda la información pertinente al respecto.
5) Gestionar sistemas informatizados de recogida de datos que contengan los datos previstos en los artículos 8, 10 y 11.
2. Con el fin de mejorar a través de las unidades nacionales la cooperación y la eficacia de los servicios competentes de los Estados miembros en el marco de los objetivos definidos en el apartado 1 del artículo 2, Europol desempeñará, además, las funciones siguientes:
1) Profundizar en los conocimientos especializados utilizados por los servicios competentes de los Estados miembros en el marco de sus investigaciones y ofrecer asesoramiento para las mismas.
2) Proporcionar datos estratégicos para facilitar y promover la utilización eficaz y racional de los recursos disponibles a nivel nacional para las actividades operativas.
3) Elaborar informes generales sobre el estado de los trabajos.
3. Además, en el marco de los objetivos que establece el apartado 1 del artículo 2, Europol podrá, en la medida en que lo permitan su dotación de personal y sus recursos presupuestarios y dentro de los límites fijados por el Consejo de Administración, asistir a los Estados miembros, mediante asesoramiento e investigaciones en los ámbitos siguientes:
1) Formación de los miembros de los servicios competentes.
2) Organización y equipamiento de dichos servicios.
3) Métodos de prevención de la delincuencia.
4) Métodos de policía técnicos y científicos, y métodos de investigación.

Artículo 4. Unidades nacionales.

1. Cada Estado miembro creará o designará una unidad nacional encargada de ejecutar las funciones enumeradas en el presente artículo.
2. La unidad nacional será el único órgano de enlace entre Europol y los servicios competentes de los Estados miembros. Las relaciones entre la unidad nacional y los servicios competentes se regirán por el Derecho nacional respectivo, en particular por sus normas constitucionales.
3. Los Estados miembros adoptarán todas las medidas necesarias para asegurar la ejecución de las funciones de la unidad nacional y, en particular, el acceso de la unidad nacional a los datos nacionales pertinentes.
4. La función de las unidades nacionales será:
1) Suministrar por iniciativa propia a Europol las informaciones y datos necesarios para el desempeño de las funciones de este organismo.
2) Responder a las solicitudes de información, de suministro de datos y de asesoramiento formuladas por Europol.
3) Mantener al día sus informaciones y datos.
4) Con arreglo a las disposiciones del Derecho nacional, aprovechar las informaciones y los datos de interés para los servicios competentes y transmitirlos a los mismos.
5) Remitir a Europol las solicitudes de asesoramiento, información, datos y análisis.
6) Transmitir a Europol informaciones para su almacenamiento en los sistemas informatizados de recogida de datos.
7) Velar por la legalidad de cada operación de intercambio de información con Europol.
5. Sin perjuicio del ejercicio de las responsabilidades de los Estados miembros, enunciadas en el apartado 2 del artículo K.2 del Tratado de la Unión Europea, las unidades nacionales no tendrán la obligación de transmitir, en un caso concreto, los datos e informaciones, a que se refieren los puntos 1, 2 y 6 del apartado 4 y los artículos 8 y 10, si la transmisión:
1) Afecta a intereses nacionales esenciales en materia de seguridad.
2) Compromete investigaciones en curso o la seguridad de una persona.
3) Se refiere a datos de servicios o actividades específicas de información en materia de seguridad del Estado.
6. Los gastos de comunicación de las unidades nacionales con Europol correrán a cargo de los Estados miembros y, con excepción de los gastos de conexión, no serán imputados a Europol.
7. Los jefes de las unidades nacionales se reunirán para prestar asesoramiento a Europol siempre que ésta necesite su ayuda.

Artículo 5. Funcionarios de enlace.

1. Cada unidad nacional enviará a Europol por lo menos a un funcionario de enlace. El número de funcionarios de enlace que podrán enviar los Estados miembros a Europol se fijará mediante acuerdo unánime del Consejo de Administración; este último podrá modificar dicho acuerdo en todo momento mediante decisión unánime. Sin perjuicio de las disposiciones específicas del presente Convenio, los funcionarios de enlace estarán sujetos al Derecho nacional del Estado miembro acreditante.
2. Las unidades nacionales encargarán a sus funcionarios de enlace la defensa de los intereses de las mismas en Europol de acuerdo con el Derecho nacional del Estado miembro acreditante y ajustándose a las disposiciones relativas al funcionamiento de Europol.
3. A reserva de lo dispuesto en los apartados 4 y 5 del artículo 4, los funcionarios de enlace apoyarán, en el marco de los objetivos establecidos en el apartado 1 del artículo 2, el intercambio de información entre las unidades nacionales acreditantes y Europol, en particular mediante:
1) La transmisión de información de las unidades nacionales acreditantes a Europol.
2) La transmisión de datos de Europol a las unidades nacionales acreditantes.
3) La cooperación con el personal de Europol mediante la transmisión de información y el asesoramiento en el análisis de la información que afecte a los Estados miembros acreditantes.
4. Al mismo tiempo, los funcionarios de enlace contribuirán, con arreglo a su Derecho nacional y en el marco de los objetivos establecidos en el apartado 1 del artículo 2, al intercambio de información procedente de las unidades

nacionales y a la coordinación de las medidas que se deriven.
5. En la medida en que sea necesario para cumplir lo dispuesto en el apartado 3, los funcionarios de enlace tendrán derecho a consultar los distintos ficheros, de acuerdo con las disposiciones oportunas precisadas en los artículos pertinentes.
6. Por analogía se aplicará a las actividades de los funcionarios de enlace el artículo 25.
7. Sin perjuicio de las demás disposiciones del presente Convenio, los derechos y obligaciones de los funcionarios de enlace respecto a Europol serán establecidos, por unanimidad, por el Consejo de Administración.
8. Los funcionarios de enlace gozarán de los privilegios e inmunidades necesarios para el cumplimiento de sus cometidos de conformidad con lo dispuesto en el apartado 2 del artículo 41.
9. Europol pondrá gratuitamente, a disposición de los Estados miembros, los locales necesarios para las actividades de sus respectivos funcionarios de enlace en el edificio de Europol. Todos los demás gastos derivados del envío de los funcionarios de enlace serán sufragados por los Estados miembros acreditantes; esto se aplicará, asimismo, a los gastos derivados de dotar con equipo a los funcionarios de enlace siempre que, al establecer el presupuesto de Europol, el Consejo de Administración no recomiende por unanimidad hacer excepciones en determinados casos.
Artículo 6. Sistema informatizado de recogida de datos.
1. Europol gestionará un sistema informatizado de recogida de datos que constará de los siguientes elementos:
1) El sistema de información contemplado en el artículo 7, de contenido limitado y definido con precisión, que permitirá una rápida consulta de la información existente en los Estados miembros y en Europol.
2) Los ficheros de trabajo contemplados en el artículo 10, que se crearán, por un plazo variable, a efectos de análisis y contendrán información pormenorizada.
3) Un sistema de índice que contendrá entradas de los ficheros de análisis a que se refiere el punto 2, según lo dispuesto en el artículo 11.
2. El sistema informatizado de recogida de datos empleados por Europol no deberán en ningún caso conectarse a otros sistemas de tratamiento automatizado, exceptuado el sistema de tratamiento automatizado de las unidades nacionales.

TITULO II

Sistema de información

Artículo 7. Creación del sistema de información.
1. Para cumplir sus funciones, Europol creará y gestionará un sistema de información informatizado. Los Estados miembros, representados por las unidades nacionales y los funcionarios de enlace, suministrarán datos directamente a dicho sistema observando su legislación nacional, y Europol suministrará los datos facilitados por Estados e instancias terceros y los datos resultantes del análisis; el sistema de información será accesible para consulta directa por parte de las unidades nacionales, los funcionarios de enlace, el director, los directores adjuntos, y los agentes de Europol debidamente habilitados.
Por lo que respecta a las personas mencionadas en el punto 2 del apartado 1 del artículo 8, las unidades nacionales sólo tendrán acceso directo al sistema de información para consultar los datos de identidad enumerados en el apartado 2 del artículo 8. Podrán acceder a la totalidad de los datos, previa petición y por mediación de los funcionarios de enlace, cuando lo necesiten para una investigación determinada.
2. Europol:
1) Tendrá por competencia velar por que se respeten las disposiciones en materia de cooperación y de gestión del sistema de información.
2) Será responsable del buen funcionamiento del sistema de información desde los puntos de vista técnico y operativo. Europol tomará en particular todas las medidas necesarias para garantizar la correcta aplicación de las medidas a que se refieren los artículos 21 y 25 por lo que respecta al sistema de información.
3. En los Estados miembros, será responsable de la comunicación con el sistema de información la unidad nacional. Dicha unidad será responsable, en particular, de las medidas de seguridad a que se refiere el artículo 25 en relación con las instalaciones de tratamiento de datos situadas en el territorio del Estado miembro de que se trate, del control mencionado en el artículo 21 y, en la medida en que lo impongan las disposiciones legales, reglamentarias y administrativas y los procedimientos aplicables en dicho Estado miembro, de la correcta ejecución del presente Convenio en cualesquiera otras materias.
Artículo 8. Contenido del sistema de información.
1. En el sistema de información sólo se podrán almacenar, modificar y utilizar los datos necesarios para el cumplimiento de las funciones de Europol, con excepción, de los datos sobre delitos conexos de conformidad con el párrafo segundo del apartado 3 del artículo 2. Estos datos se referirán a:
1) Las personas que sean sospechosas, de acuerdo con el Derecho nacional del Estado miembro de que se trate, de haber cometido o de haber participado en un delito que sea competencia de Europol con arreglo al artículo 2, o que hayan sido condenadas por tal delito.
2) Las personas respecto de las cuales existan hechos graves que justifiquen, de acuerdo con el Derecho nacional, la presunción de que cometerán delitos que son competencia de Europol con arreglo al artículo 2.
2. Los datos relativos a las personas mencionadas en el apartado 1 sólo podrán incluir los elementos siguientes:
1) Apellido, apellido de soltera, nombre y, en su caso, alias o nombres utilizados.
2) Fecha y lugar de nacimiento.
3) Nacionalidad.
4) Sexo.
5) En la medida en que sea necesario, otras características útiles para su identificación, en particular rasgos físicos específicos, objetivos y permanentes.
3. Además de los datos indicados en el apartado 2 y la mención de Europol o de la unidad nacional que los haya

suministrado, podrán almacenarse, modificarse y utilizar en el sistema de información las siguientes indicaciones adicionales con respecto a las personas a que se refiere el apartado 1:
1) Delitos, hechos imputados, fecha y lugar de comisión.
2) Medios utilizados o que puedan serlo.
3) Servicios responsables del expediente y número de referencia de éste.
4) Sospecha de pertenencia a una organización delictiva.
5) Condenas, siempre que se refieran a delitos que sean competencia de Europol con arreglo al artículo 2.
Estos datos también podrán ser introducidos cuando aun no se refieran a ninguna persona. Cuando sea Europol quien introduzca los datos, añadirá al número de referencia del expediente una indicación que señale si los datos fueron transmitidos por terceros o si son el resultado de análisis realizados por Europol.
4. La información complementaria relativa a las categorías de personas a que hace referencia el apartado 1 que obre en poder de Europol y de las unidades nacionales podrá ser comunicada a cualquier unidad nacional y a Europol a instancia de éstas. En el caso de las unidades nacionales, tal comunicación se hará dentro del respeto del Derecho nacional.
Cuando dicha información complementaria se refiere a uno o varios delitos conexos, según se definen en el párrafo segundo del apartado 3 del artículo 2, el dato almacenado en el sistema de información se acompañará de una indicación destinada a señalar la existencia de delitos conexos, con el fin de que las unidades nacionales y Europol puedan intercambiar la información relativa a dichos delitos.
5. En caso de que la causa contra el interesado se archive definitivamente o se pronuncie una resolución absolutoria de dicho interesado, deberán suprimirse los datos a los que se refiera dicha resolución.
Artículo 9. Derecho de acceso al sistema de información.
1. El derecho a introducir directamente datos en el sistema de información y acceder al mismo quedará reservado a las unidades nacionales, a los funcionarios de enlace, al director, a los directores adjuntos y a los agentes de Europol debidamente habilitados. La consulta de los datos se autorizará en la medida en que sea necesaria para el cumplimiento de un cometido concreto y se regirá por las disposiciones legales, reglamentarias y administrativas, así como por los procedimientos de la unidad que efectúe la consulta, a no ser que el presente Convenio contenga otras disposiciones al respecto.
2. La unidad introductora será la única autorizada para modificar, rectificar o suprimir los datos que haya introducido. Si una unidad dispone de indicios que permitan presumir que un dato de los mencionados en el apartado 2 del artículo 8 contiene errores, o si desea completar tales datos, informará de ello inmediatamente a la unidad introductora, la cual deberá comprobar la comunicación sin demora y, en caso necesario, modificar, completar, rectificar o suprimir el dato inmediatamente. De haberse almacenado con respecto a una persona datos de los mencionados en el apartado 3 del artículo 8, cualquier unidad podrá completarlos introduciendo otros datos de los mencionados en el apartado 3 del artículo 8. Si hay contradicciones manifiestas entre estos datos, las unidades de que se trate deberán ponerse de acuerdo. Si una unidad tiene intención de suprimir la totalidad de los datos mencionados en el apartado 2 del artículo 8 introducidos por ella con respecto a una persona y si existen datos de los mencionados en el apartado 3 del artículo 8 referidos a la misma persona introducidos por otras unidades, la responsabilidad en materia de protección de los datos con arreglo al apartado 1 del artículo 15 y el derecho a modificarlos, completarlos, rectificarlos y suprimirlos con arreglo al apartado 2 del artículo 8 se transferirá a la unidad siguiente que haya introducido datos de los mencionados en el apartado 3 del artículo 8 en relación con la misma persona. La unidad que tenga intención de suprimir los datos informará de ello a la unidad a la que corresponda la responsabilidad en materia de protección de datos.
3. La responsabilidad de la licitud de la consulta, la introducción o la modificación de datos del sistema de información recaerá en la unidad que realice dicha consulta, introducción o modificación; dicha unidad deberá ser identificable. La transmisión de información entre las unidades nacionales y las autoridades competentes de los Estados miembros se regirá por el Derecho nacional.

TITULO III

Ficheros de trabajo con fines de análisis

Artículo 10. Recogida, tratamiento y utilización de datos personales.
1. En la medida en que sea necesario para el cumplimiento de los objetivos establecidos en el apartado 1 del artículo 2, Europol podrá almacenar, modificar y utilizar, en otros ficheros, además de los datos no personales, datos relativos a los delitos que sean competencia de Europol con arreglo a lo dispuesto en el apartado 2 del artículo 2, incluidos los delitos conexos previstos en el párrafo segundo del apartado 3 del artículo 2, destinados a trabajos específicos de análisis, referidos a:
1) Las personas mencionadas en el apartado 1 del artículo 8.
2) Personas que sean consideradas posibles testigos en investigaciones sobre los delitos considerados o en una futura causa penal.
3) Personas que hayan sido perjudicadas por uno de los delitos considerados o respecto de las cuales existan motivos para presumir que puedan ser perjudicadas por tal delito.
4) Personas intermediarias y acompañantes.
5) Personas que puedan facilitar información sobre los delitos considerados.
La recogida, el almacenamiento y el tratamiento de los datos que se enumeran en la primera frase del artículo 6 del Convenio del Consejo de Europa, de 28 de enero de 1981 (RCL 1985\2704 y ApNDL 3638), para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal sólo se autorizarán cuando sean estrictamente necesarios para la finalidad del fichero de que se trate y cuando tales datos completen otros datos personales introducidos en ese mismo fichero. Queda prohibido seleccionar una categoría particular de personas a partir únicamente de los datos de la primera frase del artículo 6 del Convenio del Consejo de Europa de 28 de enero de 1981, en vulneración de las normas de finalidad citadas.

El Consejo aprobará por unanimidad, de acuerdo con el procedimiento establecido en el Título VI del Tratado de la Unión Europea, las normas de desarrollo aplicables a los ficheros, preparadas por el Consejo de Administración, en las que se precisarán, en particular, las indicaciones relativas a las categorías de datos personales previstos en el presente artículo y las disposiciones relativas a la seguridad de dichos datos y al control interno de su utilización.

2. Estos ficheros se crearán con fines de análisis, entendiendo por análisis el ordenamiento, tratamiento o utilización de datos para facilitar la investigación criminal. Para cada proyecto de análisis se creará un grupo de análisis en el que se asociarán estrechamente los siguientes participantes, con arreglo a los cometidos definidos en los apartados 1 y 2 del artículo 3 y en el apartado 3 del artículo 5:

1) Los analistas y otros agentes de Europol designados por la dirección de Europol; sólo los analistas estarán facultados para introducir y consultar los datos en el fichero de que se trate.

2) Los funcionarios de enlace o los expertos de los Estados miembros de donde proceda la información o afectados por el análisis en el sentido del apartado 6.

3. A reserva de lo dispuesto en el apartado 5 del artículo 4, a solicitud de Europol o por propia iniciativa, las unidades nacionales comunicarán a Europol toda la información que ésta necesite para el cumplimiento de sus tareas con arreglo al punto 2 del apartado 1 del artículo 3. Los Estados miembros sólo transmitirán los datos en la medida en que su Derecho nacional permita el tratamiento de los mismos a efectos de la prevención, análisis o lucha contra actos delictivos.

Los datos procedentes de unidades nacionales podrán llegar directamente y por todos los medios adecuados a los grupos de análisis, en función de su confidencialidad, a través o no de los funcionarios de enlace afectados.

4. Si además de la información a que se refiere el apartado 3, Europol necesita por razones justificadas datos adicionales para cumplir las funciones que figuran en el punto 2 del apartado 1 del artículo 3 podrá solicitar:

1) De las Comunidades Europeas y de organismos de Derecho público creados en virtud de los Tratados constitutivos de las Comunidades.

2) De otros organismos de Derecho público constituidos en el marco de la Unión Europea.

3) De organismos creados en virtud de un acuerdo firmado entre dos o más Estados miembros de la Unión Europea.

4) De terceros Estados.

5) De organizaciones internacionales y de los organismos de Derecho público dependientes de las mismas.

6) De otros organismos de Derecho público creados en virtud de un acuerdo entre dos o más Estados, y

7) De la Organización Internacional de Policía Criminal.

La transmisión de la información correspondiente por todos los medios pertinentes. Podrá asimismo, en las mismas condiciones y por las mismas vías, aceptarla cuando proceda de estas distintas organizaciones a iniciativa de las mismas. El Consejo fijará por unanimidad, según el procedimiento previsto en el Título VI del Tratado de la Unión Europea, previa consulta del Consejo de Administración, las normas que deberá observar Europol en la materia.

5. Si Europol, mediante otros Convenios, hubiese obtenido el derecho de consultar por vía informática otros sistemas de información, podrá buscar de esta forma datos personales siempre que sea necesario para el ejercicio de sus funciones según el punto 2 del apartado 1 del artículo 3.

6. Si el análisis es de tipo general y estratégico, se mantendrá plenamente asociados a todos los Estados miembros, por mediación de sus funcionarios de enlace o de expertos, a los resultados de los trabajos, sobre todo comunicándoles los informes elaborados por Europol.

Si el análisis se refiere a casos particulares que no afecten a todos los Estados miembros y tiene una orientación operativa directa, participarán en él los representantes de los siguientes Estados miembros:

1) Aquellos de donde proceda la información que haya dado lugar a la decisión de creación del fichero de análisis o a los que dicha información afecta de manera inmediata, y aquellos a los que el grupo de análisis invite posteriormente a asociarse porque se hayan convertido en partes afectadas.

2) Aquellos a los que la consulta del sistema del índice indique que necesitan conocerlo y que lo soliciten en las condiciones definidas en la apartado 7.

7. Los funcionarios de enlace habilitados alegarán esa necesidad. Cada Estado miembro designará y habilitará, a tal efecto, un número limitado de funcionarios de enlace. Transmitirá la lista de los mismos al Consejo de Administración.

Para alegar la necesidad de tener conocimiento de los ficheros en el sentido del apartado 6, el funcionario de enlace la justificará en un escrito que deberá ser aprobado por la autoridad jerárquica de la que dependa en su Estado y que se comunicará a todos los participantes en el análisis. A continuación participará de pleno derecho en el análisis en curso.

En caso de objeción en el grupo de análisis, se aplazará esta asociación de pleno derecho mientras se realiza un procedimiento de conciliación que podrá constar de tres fases sucesivas:

1) Los participantes en el análisis tratarán de ponerse de acuerdo con el funcionario de enlace que haya alegado su necesidad de tener conocimiento del fichero; para ello dispondrá de un plazo máximo de ocho días.

2) Si persiste el desacuerdo, los jefes de las unidades nacionales afectadas y la dirección de Europol se reunirán en un plazo de tres días.

3) Si todavía persiste el desacuerdo, los representantes de las partes afectadas en el Consejo de Administración de Europol se reunirán en un plazo de ocho días. Si el Estado miembro de que se trate no renuncia a alegar su necesidad de tener conocimiento de los ficheros, su participación de pleno derecho se hará efectiva por decisión consensuada.

8. El Estado miembro que transmita un dato a Europol será el único Juez de su grado de confidencialidad y de la variación del mismo. Toda difusión o explotación operativa de un dato de análisis se someterá a la concertación de los participantes en el análisis. Un Estado miembro que acceda a un análisis en curso no podrá, en particular, difundir ni explotar los datos sin el consentimiento previo de los Estados miembros afectados en primer lugar.

Artículo 11. Sistema de índice.

1. Europol elaborará un sistema de índice de los datos almacenado en los ficheros a que se refiere el apartado 1 del artículo 10.

2. El Director, los Directores adjuntos, los Agentes de Europol debidamente habilitados y los funcionarios de enlace tendrán derecho a consultar el sistema de índice. El sistema de índice deberá estar constituido de manera que indique claramente al funcionario de enlace que lo consulte, a partir de los datos consultados, que los ficheros mencionados en el punto 2 del apartado 1 del artículo 6 y en el apartado 1 del artículo 10 contienen información que afecta al Estado

miembro acreditante.
El acceso por parte de los funcionarios de enlace se regulará de forma que permita determinar si una información está almacenada o no, sin que sea posible realizar ningún cotejo ni deducir el contenido de los ficheros.
3. El Consejo de Administración decidirá, por unanimidad, la forma de organización del sistema de índice.
Artículo 12. Disposición de creación de ficheros.
1. Para cada uno de los ficheros automatizados de datos personales que gestione con arreglo al artículo 10 en el marco del cumplimiento de sus funciones, Europol deberá indicar, en una disposición de creación que requerirá el acuerdo del Consejo de Administración, los elementos siguientes:
1) Denominación del fichero.
2) Objetivo del fichero.
3) Categorías de personas acerca de las cuales se vayan a almacenar datos.
4) Naturaleza de los datos que se vayan a almacenar y, si ha lugar, los datos estrictamente necesarios entre los enumerados en la primera fase del artículo 6 del Convenio de Consejo de Europa de 28 de enero de 1981.
5) Tipos de datos personales que permitirán acceder a la totalidad del fichero.
6) Transferencia o introducción de los datos que deban almacenarse.
7) Condiciones en que podrán transmitirse datos personales almacenados en el fichero, a qué destinatarios y según qué procedimiento.
8) Plazos de verificación y duración del almacenamiento de datos.
9) Constancia documental.
El Director de Europol informará inmediatamente a la autoridad común de control prevista en el artículo 24 acerca del proyecto de creación de un fichero de estas características y le comunicará el expediente para que pueda formular, a la atención del Consejo de Administración, todas las observaciones que considere necesarias.
2. Si, debido a la urgencia, no fuera posible obtener la aprobación del Consejo de Administración contemplada en el apartado 1, el Director, por propia iniciativa o a petición de los Estados miembros interesados, podrá decidir, mediante decisión motivada, la creación de un fichero. Informará simultáneamente de ello a los miembros del Consejo de Administración. A continuación se iniciará sin demora el procedimiento del apartado 1, que deberá concluirse con la mayor brevedad.

TITULO IV

Disposiciones comunes relativas al tratamiento de la información

Artículo 13. Obligación de informar.
Europol comunicará sin demora a las unidades nacionales y, a solicitud de las mismas, a sus funcionarios de enlace, la información que afecte a su Estado miembro y las relaciones establecidas entre delitos que sean competencias de Europol a tenor del artículo 2. Podrá, asimismo, transmitir información y datos sobre otros delitos graves, obtenidos por Europol en el ejercicio de sus funciones.
Artículo 14. Nivel de protección de los datos.
1. Por lo que se refiere al tratamiento de datos personales en ficheros en el marco de la aplicación del presente Convenio, cada Estado miembro 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 que sea como mínimo igual al resultante de los principios del Convenio del Consejo de Europa de 28 de enero de 1981, teniendo en cuenta la Recomendación R(87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa encaminada a regular la utilización de datos de carácter personal en el sector de la policía.
2. La transmisión de datos de carácter personal prevista en el presente Convenio no podrá iniciarse hasta que las disposiciones de protección de datos previstas en el apartado 1 hayan entrado en vigor en el territorio de todos los Estados miembros que participen en la transmisión.
3. En la recogida, el tratamiento y la utilización de datos personales, Europol respetará los principios del Convenio del Consejo de Europa de 28 de enero de 1981 y la Recomendación R(87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa.
Europol respetará también dichos principios para los datos no automatizados que obren en su poder en forma de ficheros, es decir, para cualquier conjunto estructurado de datos personales accesible según criterios determinados.
Artículo 15. Responsabilidad en materia de protección de datos.
1. De los datos que conserve Europol, en particular de la licitud de su recogida y de su transmisión a Europol, así como de su introducción, de carácter exacto y actualizado de dichos datos y del control de los plazos de conservación responderá, a reserva de las demás disposiciones del presente Convenio:
1) El Estado miembro que los introdujo o transmitió.
2) Europol, cuando se trate de datos que le fueron transmitidos por terceros o que son resultado de análisis hechos por Europol.
2. Además, a reserva de las demás disposiciones del presente Convenio, Europol responderá de todos los datos que le lleguen y que sean tratados por sus servicios, independientemente de que se hallen incluidos en el sistema de información a que se refiere el artículo 8, en los ficheros creados para los fines de análisis a que se refiere el artículo 10, en el sistema de índice a que se refiere el artículo 11 o en los ficheros mencionados en el apartado 3 del artículo 14.
3. Europol almacenará los datos de manera que pueda determinarse por qué Estado miembro o Estado u organismo tercero fueron transmitidos o si son el resultado de análisis realizados por Europol.
Artículo 16. Normas sobre constancia documental.
Por término medio Europol levantará acta de al menos una de cada diez consultas de datos personales y, en el marco del sistema de información a que se refiere el artículo 7, de todas las consultas, para controlar su licitud. Las actas así levantadas sólo podrán ser utilizadas por Europol y las autoridades de control a que se refieren los artículos 23 y 24 para el fin designado y se suprimirán al cabo de seis meses, excepto cuando se necesiten para un control que se halle

pendiente. El Consejo de Administración establecerá los pormenores previa audiencia de la autoridad común de control.

Artículo 17. Normas de utilización.

1. Unicamente los servicios de los Estados miembros competentes para prevenir y combatir los delitos que son competencia de Europol y las demás formas graves de delincuencia podrán transmitir o utilizar los datos personales extraídos del sistema de información, del sistema de índice o de los ficheros creados para análisis y los datos comunicados por cualquier otro medio apropiado.

La utilización de los datos a que se refiere el párrafo primero se hará respetando la legislación del Estado miembro del que dependan los servicios usuarios.

Europol sólo podrá utilizar los datos a que se refiere el apartado 1 en el desempeño de las funciones contempladas en el artículo 3.

2. Cuando, con respecto a determinados datos, el Estado miembro suministrador o el Estado u organismo tercero contemplado en el apartado 4 del artículo 10, comunique que en ese Estado miembro o Estado u organismo tercero, la utilización de dichos datos está sujeta a limitaciones especiales, el usuario también deberá respetarlas, salvo en aquellos casos en que el Derecho nacional obligue a hacer excepciones a esas limitaciones en beneficio de las autoridades judiciales, de las instituciones legislativas o de cualquier otra entidad independiente creada por Ley y encargada del control de los servicios nacionales competentes definidos en el apartado 4 del artículo 2 del presente Convenio. En dichos casos, sólo se podrá utilizar los datos previa consulta al Estado que los haya suministrado, cuyos intereses y opiniones se tendrán en cuenta en la medida de lo posible.

3. Los datos sólo podrán ser utilizados para fines distintos de los mencionados en el artículo 2 del presente Convenio, o por autoridades distintas de las contempladas en dicho artículo con la autorización previa del Estado miembro que los haya transmitido y siempre que lo permita el Derecho nacional de éste.

Artículo 18. Transmisión de datos a Estados e instancias terceros.

1. En las condiciones expresadas en el apartado 4 del presente artículo, Europol podrá transmitir datos personales almacenados por sus servicios a los terceros Estados y organismos contemplados en el apartado 4 del artículo 10 cuando:

1) En casos concretos, tal medida sea necesaria para prevenir o combatir actos delictivos que sean competencia de Europol con arreglo al artículo 2.

2) En el Estado u organismo de que se trate esté garantizado un nivel adecuado de protección de los datos.

3) Tal medida sea admisible de acuerdo con las normas generales previstas en el apartado 2.

2. El Consejo, de conformidad con el procedimiento previsto en el Título VI del Tratado de la Unión Europea y habida cuenta de las circunstancias contempladas en el apartado 3, fijará por unanimidad las normas generales para la transmisión por Europol de datos personales a terceros Estados y organismos a tenor del apartado 4 del artículo 10. El Consejo de Administración preparará la decisión del Consejo y consultará a la autoridad común de control contemplada en el artículo 24.

3. El carácter adecuado del nivel de protección de los datos que ofrezcan los terceros Estados y organismos a que se refiere el apartado 4 del artículo 10 se evaluará teniendo en cuenta todas las circunstancias que concurran en la transmisión de datos personales; en particular se tendrá en cuenta:

1) La naturaleza de los datos.

2) Su finalidad.

3) La duración del tratamiento previsto, y

4) Las disposiciones generales o específicas aplicables a los terceros Estados y organismos contemplados en el apartado 4 del artículo 10.

4. Si los datos mencionados han sido transmitidos a Europol por un Estado miembro, Europol sólo podrá transmitirlos a terceros Estados u organismos con el acuerdo del Estado miembro. A tal fin, el Estado miembro podrá manifestar su acuerdo previo, general o no, revocable en todo momento.

Si los datos no han sido transmitidos por un Estado miembro, Europol se cerciorará de que el hecho de transmitirlos:

1) No puede poner en peligro el correcto cumplimiento de las funciones que son competencia de un Estado miembro.

2) No amenaza el orden y la seguridad públicos de un Estado miembro ni puede perjudicar de alguna forma los intereses de este último.

5. La responsabilidad de la licitud de la transmisión recaerá en Europol. Europol deberá dejar constancia de dicha transmisión y del motivo de la misma. La transmisión sólo estará autorizada si el destinatario se compromete a utilizar los datos únicamente para el fin que ha motivado la transmisión. Esto no se aplicará a la transmisión de los datos personales necesarios en el marco de una consulta de Europol.

6. Cuando la transmisión con arreglo al apartado 1 se refiera a informaciones confidenciales, sólo estará autorizada si existe un acuerdo sobre la protección del secreto entre Europol y el destinatario.

Artículo 19. Derecho de acceso.

1. Cualquier persona que desee ejercer su derecho de acceso a la información, que le afecte, almacenada en Europol o hacer que se verifique esa información podrá dirigir gratuitamente una solicitud en ese sentido, en el Estado miembro de su elección, a la autoridad nacional competente, que deberá comunicarlo sin dilación a Europol y avisar al solicitante de que Europol le responderá directamente.

2. Europol deberá tramitar completamente la solicitud en los tres meses siguientes a su recepción por la autoridad nacional competente del Estado miembro.

3. El derecho de cualquier persona a acceder a los datos que le afecten o a hacer que se verifiquen esos datos se ejercerá conforme a la legislación del Estado miembro ante el cual se presente la solicitud correspondiente y teniendo en cuenta las disposiciones siguientes:

En caso de que el Derecho del Estado miembro ante el cual se haya presentado la solicitud contemple la comunicación referente a los datos, se denegará la comunicación cuando resulte necesario:

1) Para que Europol pueda cumplir adecuadamente sus funciones.

2) Para proteger la seguridad de los Estados miembros y el orden público o para combatir los delitos.

3) Para proteger los derechos y libertades de terceros.

En cuyo caso no prevalecerá el interés de la persona afectada por la comunicación de la información.

4. El derecho a la comunicación se ejercerá, respetando lo dispuesto en el apartado 3, con arreglo al procedimiento siguiente:

1) Si se trata de datos integrados en el sistema de información definido en el artículo 8, sólo podrá aprobarse su comunicación una vez que el Estado miembro que los haya introducido y los Estados miembros directamente afectados por dicha comunicación hayan tenido ocasión de dar a conocer su postura al respecto, que podrá consistir en la denegación de la comunicación. El Estado miembro que haya introducido los datos indicará los datos que puedan ser comunicados y la forma de comunicación.

2) Si se trata de datos integrados por Europol en el sistema de información, los Estados miembros directamente afectados por su comunicación deberán haber tenido previamente ocasión de dar a conocer su postura al respecto, que podrá consistir en la denegación de la comunicación.

3) Si se trata de datos integrados en los ficheros de trabajo con fines de análisis definidos en el artículo 10, su comunicación estará supeditada al consenso de Europol y de los Estados miembros participantes en el análisis, a tenor del apartado 2 del artículo 10, y del Estado o Estados miembros directamente afectados por dicha comunicación.

Si uno o varios Estados miembros o Europol han manifestado su oposición a la comunicación referente a los datos, Europol notificará al solicitante que ha efectuado las verificaciones necesarias, sin darle indicaciones que puedan revelarle si Europol almacena o no información sobre su persona.

5. El derecho a la verificación se ejercerá con arreglo al procedimiento siguiente:

En caso de que el Derecho nacional aplicable no contemple la comunicación referente a los datos, o cuando se trate de una simple solicitud de verificación, Europol, en estrecha coordinación con las autoridades nacionales afectadas, efectuará las verificaciones y notificará al solicitante que las ha efectuado, sin darle indicaciones que puedan revelarle si Europol almacena o no información sobre su persona.

6. Al responder a una solicitud de verificación o de acceso a los datos, Europol informará al solicitante de que puede interponer un recurso ante la autoridad común de control si no está satisfecho con la decisión adoptada. El solicitante podrá recurrir también a la autoridad común de control si no se ha respondido a su solicitud dentro del plazo fijado en el presente artículo.

7. Si el solicitante interpone un recurso ante la autoridad común de control a que se refiere el artículo 24, la instrucción del recurso corresponderá a dicha autoridad.

Si el recurso atañe a la comunicación referente a los datos introducidos por un Estado miembro en el sistema de información, la autoridad común de control tomará su decisión de conformidad con el Derecho nacional del Estado miembro ante el cual se haya presentado la solicitud. La autoridad común de control consultará previamente a la autoridad nacional de control o al órgano jurisdiccional competente del Estado miembro del que proceda el dato. La autoridad nacional de control o el órgano jurisdiccional competente efectuarán las verificaciones necesarias para determinar, en particular, si la decisión de denegación se ha tomado de conformidad con las disposiciones del apartado 3 y del párrafo primero del apartado 4 del presente artículo. En tal caso, la decisión, que podrá consistir en la denegación de comunicación, será tomada por la autoridad común de control en estrecha coordinación con la autoridad nacional de control o el órgano jurisdiccional competente.

Si el recurso atañe a la comunicación referente a los datos introducidos por Europol en el sistema de información o a los datos almacenados en los ficheros de trabajo con fines de análisis, y persiste la oposición de Europol o de un Estado miembro, la autoridad común de control, tras haber escuchado los argumentos de Europol o del Estado miembro, sólo podrá desoír esa oposición cuando así lo acuerden sus miembros por mayoría de dos tercios. De no reunirse esa mayoría, la autoridad común de control notificará al solicitante que se han efectuado las verificaciones, sin darle indicaciones que puedan revelarle si Europol almacena o no información sobre su persona.

Si el recurso atañe a la verificación de los datos introducidos por un Estado miembro en el sistema de información, la autoridad común de control se cerciorará de que las verificaciones necesarias se han efectuado correctamente, en estrecha coordinación con la autoridad nacional de control del Estado miembro que haya introducido los datos. La autoridad común de control notificará al solicitante que se han efectuado las verificaciones, sin darle indicaciones, que puedan revelarle si Europol almacena o no datos sobre su persona.

Si el recurso atañe a la verificación de datos introducidos por Europol en el sistema de información o de datos almacenados en los ficheros de trabajo con fines de análisis, la autoridad común de control se cerciorará de que Europol ha efectuado correctamente las verificaciones necesarias. La autoridad común de control notificará al solicitante que se han efectuado las verificaciones, sin darle indicaciones que puedan revelarle si Europol almacena o no datos sobre su persona.

8. Las disposiciones que anteceden se aplicarán por analogía a los datos no automatizados que obren en poder de Europol en forma de ficheros, es decir, a cualquier conjunto estructurado de datos personales accesible según criterios determinados.

Artículo 20. Rectificación y supresión de datos.

1. Si se advirtiese que datos almacenados por Europol, tanto si han sido transmitidos por Estados u organismos terceros como si resultan de su actividad de análisis, contienen errores o que su introducción o almacenamiento son contrarios al presente Convenio, Europol deberá rectificarlos o suprimirlos.

2. Si los datos que contienen errores o son contrarios a las disposiciones del presente Convenio han sido introducidos directamente en Europol por un Estado miembro; este último deberá rectificarlos o suprimirlos de acuerdo con Europol. Si los datos que contienen errores han sido transmitidos por cualquier otro medio apropiado, o si los errores que afectan a los datos suministrados por los Estados miembros se deben a una transmisión indebida o contraria a las disposiciones del presente Convenio, o bien a que Europol los ha introducido, procesado o almacenado de manera indebida o contraria a las disposiciones del presente Convenio, Europol deberá rectificarlos o suprimirlos de acuerdo con los Estados miembros afectados.

3. En los casos contemplados en los apartados 1 y 2, se informará sin demora a todos los destinatarios de estos datos, que deberán proceder, asimismo, a rectificarlos o suprimirlos.

4. Cualquier persona tendrá derecho a pedir a Europol que los datos erróneos que le afecten sean rectificados o suprimidos.

Europol deberá notificar al solicitante que se han rectificado o suprimido los datos que le afecten. Si el solicitante no está satisfecho con la respuesta de Europol, o si no ha obtenido respuesta en un plazo de tres meses, podrá recurrir a la autoridad común de control.

Artículo 21. Plazos de conservación y supresión de los ficheros.

1. Los datos contenidos en los ficheros sólo se conservarán en Europol durante el tiempo necesario para que ésta pueda cumplir sus funciones. A más tardar tres años después de su introducción deberá verificarse la necesidad de prolongar su almacenamiento. La verificación de los datos almacenados en el sistema de información y de su supresión serán llevadas a cabo por la unidad que los introdujo. La verificación de los datos almacenados en los demás ficheros de los servicios de Europol y de la supresión de los mismos serán realizadas por Europol. Europol notificará a los Estados miembros con tres meses de antelación y de forma automática el vencimiento de los plazos de verificación en lo que respecta a la conservación de los datos que hayan introducido.

2. Cuando realicen esa verificación, las unidades, a que se refieren las frases tercera y cuarta del apartado 1, podrán optar por conservar los datos hasta la siguiente verificación, si así lo requiere el cumplimiento de las funciones de Europol. De no tomarse tal decisión de prolongación, los datos se suprimirán automáticamente.

3. No se conservarán los datos personales de las personas, contempladas en el punto 1 del párrafo primero del apartado 1 del artículo 10, más de un total de tres años. Este plazo empezará a correr de nuevo automáticamente en la fecha en que se produzca un hecho que motive el almacenamiento de datos sobre dicha persona. Deberá verificarse anualmente la necesidad de conservación de esos datos y se dejará constancia de la verificación.

4. Cuando un Estado miembro suprima en sus ficheros nacionales datos transmitidos a Europol que ésta conserve en los demás ficheros, deberá informar de ello a Europol. En tal caso, Europol suprimirá los datos, a no ser que éstos sigan revistiendo interés para Europol debido a información que obre en su poder y no que posea el Estado miembro transmisor. Europol comunicará al Estado miembro en cuestión la prolongación del almacenamiento de dichos datos.

5. No se procederá a la supresión cuando ésta pueda perjudicar a intereses dignos de protección de la persona de que se trate. En tal caso, los datos ya sólo podrán utilizarse con el consentimiento de ésta.

Artículo 22. Conservación y rectificación de datos que figuren en expediente.

1. Si se advirtiese que un expediente entero de Europol o que algunos de los datos que figuran en expedientes de Europol ya no son necesarios para el cumplimiento de su cometido, o que tal información es, en conjunto, contraria a lo dispuesto en el presente Convenio, se destruirá dicho expediente o bien los datos que corresponda. Mientras el expediente o los datos correspondientes no hayan sido realmente destruidos, se hará figurar una nota que prohíba toda utilización de los mismos.

No se procederá a la destrucción de un expediente cuando existan motivos para presumir que ello perjudicaría a intereses legítimos de la persona a la que se refieran los datos. En tales casos, se incluirá la misma nota que prohíba toda utilización del mismo.

2. Si se advirtiese la presencia de errores en datos que figuran en expedientes de Europol, Europol tendrá la obligación de rectificarlos.

3. Toda persona a la que afecte un expediente de Europol podrá ejercer con respecto a Europol el derecho a la rectificación, a la destrucción del expediente o la consignación de una nota. Se aplicarán el apartado 4 del artículo 20 y los apartados 2 y 7 del artículo 24.

Artículo 23. Autoridad nacional de control.

1. Cada Estado miembro designará una autoridad nacional de control cuya tarea consistirá en vigilar, de manera independiente y con arreglo a la legislación nacional, la licitud de la introducción y la consulta de datos y de la transmisión en cualquier forma de datos personales a Europol por parte del Estado miembro de que se trate, y en garantizar que no se vulneren los derechos de las personas. A tal efecto, la autoridad nacional de control tendrá acceso, a través de las unidades nacionales o los funcionarios de enlace y según los procedimientos nacionales aplicables, a los datos introducidos por el Estado miembro contenidos en el sistema de información y en el sistema de índice.

Para ejercer este control, las autoridades nacionales de control tendrán acceso a las oficinas y a los expedientes de los funcionarios de enlace respectivos dentro de Europol.

Las autoridades nacionales de control vigilarán, asimismo, según los procedimientos nacionales aplicables, las actividades que realicen las unidades nacionales, de conformidad con el apartado 4 del artículo 4, y las que realicen los funcionarios de enlace de conformidad con los puntos 1, 2 y 3 del apartado 3 y los apartados 4 y 5 del artículo 5, en la medida en que dichas actividades guarden relación con la protección de datos personales.

2. Cualquier persona tendrá derecho a solicitar a la autoridad nacional de control que se cerciore de la licitud de la introducción y la transmisión de sus datos personales a Europol, en cualquiera de sus formas, y de la consulta de los datos por parte del Estado miembro de que se trate.

Este derecho se ejercerá con arreglo a la legislación nacional del Estado miembro a cuya autoridad nacional de control se dirija la solicitud.

Artículo 24. Autoridad común de control.

1. Se establecerá una autoridad común de control independiente cuyo cometido será vigilar la actividad de Europol, con arreglo a lo dispuesto en el presente Convenio, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas. La autoridad común de control controlará, además, la licitud de la transmisión de datos que procedan de Europol. Integrarán la autoridad común de control como máximo dos miembros o representantes, en su caso, asistidos por suplentes, de cada una de las autoridades nacionales de control, que deberán ofrecer, por tanto, las máximas garantías de independencia y poseer las capacidades exigidas, y que serán nombrados por cada Estado miembro por períodos de cinco años. Cada Delegación dispondrá de un voto.

La autoridad común de control designará Presidente a uno de sus miembros.

En el ejercicio de sus atribuciones, los miembros de la autoridad común de control no recibirán instrucciones de ninguna autoridad.

2. Europol tendrá la obligación de asistir a la autoridad común de control en el cumplimiento de sus tareas. En particular deberá:

1) Facilitarle información en respuesta a sus solicitudes, acceso a todos los expedientes y documentos, y accesos a los

datos almacenados.
2) Permitirle que acceda en todo momento a todos sus locales.
3) Dar cumplimiento a las decisiones que tome la autoridad común de control en relación con los recursos, de conformidad con las disposiciones del apartado 7 del artículo 19 y del apartado 4 del artículo 20.
3. La autoridad común de control también será competente para analizar las dificultades de aplicación e interpretación que pudiera plantear la actividad de Europol en relación con el tratamiento y la utilización de datos personales, para estudiar los posibles problemas en relación con el control independiente efectuado por las autoridades nacionales de control de los Estados miembros o con el ejercicio del derecho de información, así como para elaborar propuestas armonizadas con miras a hallar soluciones comunes a los problemas existentes.
4. Cualquier persona tendrá derecho a solicitar a la autoridad común de control que se cerciore de que el almacenamiento, la recogida, tratamiento y uso de los datos relativos a su persona que haya efectuado Europol se han realizado de manera lícita y correcta.
5. Si la autoridad común de control comprobase que no se han respetado las disposiciones del presente Convenio en el almacenamiento, tratamiento o utilización de datos personales, dirigirá todas las observaciones que considere oportunas al Director de Europol y solicitará una respuesta en un plazo que ella fije. El Director mantendrá al corriente al Consejo de Administración de todo el procedimiento. En caso de dificultades, la autoridad común de control se dirigirá al Consejo de Administración.
6. La autoridad común de control elaborará informes de actividad a intervalos regulares. Estos se remitirán al Consejo, con arreglo al procedimiento a que se refiere el Título VI del Tratado de la Unión Europea; previamente el Consejo de Administración podrá emitir un dictamen que se adjuntará al informe.
La autoridad común de control decidirá si procede o no publicar su informe de actividad y, en caso afirmativo, decidirá las condiciones de dicha publicación.
7. La autoridad común de control establecerá su reglamento interno por decisión adoptada por unanimidad. El reglamento interno deberá ser aprobado por el Consejo por unanimidad. La autoridad común de control creará en su seno un Comité, integrado por un miembro de cada delegación, cada uno de los cuales tendrá derecho a un voto. Este Comité se encargará de examinar los recursos contemplados en el apartado 7 del artículo 19 y en el apartado 4 del artículo 20, para lo cual podrá utilizar todos los medios pertinentes. Si las partes lo solicitan, comparecerán ante el Comité, asistidas por sus asesores si lo desean. Las decisiones adoptadas en este marco serán definitivas para todas las partes afectadas.
8. La autoridad común de control podrá crear, además, una o varias comisiones.
9. Será consultada sobre la parte del proyecto de presupuesto que le afecta, y su dictamen se adjuntará al proyecto de presupuesto en cuestión.
10. Estará asistida por una Secretaría, cuyas tareas se definirán en el reglamento interno.
Artículo 25. Seguridad de los datos.
1. Europol deberá tomar las medidas técnicas y organizativas necesarias para la ejecución del presente convenio. Una medida sólo se considerará necesaria, cuando el coste que suponga guarde relación con el objetivo de protección que se persiga.
2. Cada uno de los Estados miembros y Europol adoptarán, con miras al tratamiento automatizado de datos en Europol, las medidas adecuadas:
1) Para impedir que cualquier persona no autorizada acceda a las instalaciones utilizadas para el tratamiento de datos personales (control de entrada a las instalaciones).
2) Para impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados por personas no autorizadas (control de los soportes de datos).
3) Para impedir que se introduzcan sin autorización en los ficheros, o que puedan conocerse, modificarse o suprimirse sin autorización datos personales almacenados (control de almacenamiento).
4) 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 (control de la utilización).
5) Para garantizar que las personas autorizadas para el uso de un sistema de tratamiento automatizado de datos sólo puedan tener acceso a los datos que sean de su competencia (control del acceso).
6) Para garantizar que pueda verificarse y constatarse a qué órganos pueden transmitirse datos personales a través de las instalaciones de transmisión de datos (control de la transmisión).
7) Para garantizar que pueda comprobarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos, en qué momento y por quién (control de la introducción).
8) Para impedir que, en el momento de la transmisión de datos personales y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte).
9) Para garantizar que los sistemas utilizados puedan repararse rápidamente en caso de avería (restablecimiento).
10) Para garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados inmediatamente (fiabilidad), y que los datos almacenados no sean falseados por defectos de funcionamiento del sistema (autenticidad).

TITULO V

Estatuto Jurídico, Organización y Disposiciones Financieras

Artículo 26. Capacidad jurídica.
1. Europol estará dotada de personalidad jurídica.
2. Europol tendrá, en cada Estado miembro, la más amplia capacidad jurídica reconocida a las personas jurídicas por la legislación nacional. Europol podrá en particular adquirir o enajenar bienes muebles o inmuebles y tendrá capacidad procesal.
3. Europol estará facultada para celebrar un acuerdo de sede con el Reino de los Países Bajos y para celebrar con los

Estados y organismos terceros, previstos en el apartado 4 del artículo 10, los acuerdos necesarios sobre protección del secreto a tenor del apartado 6 del artículo 18, así como otros acuerdos, en el marco de las normas establecidas por unanimidad por el Consejo sobre la base del presente Convenio y del Título VI del Tratado de la Unión Europea.

Artículo 27. Organos de Europol.

Los órganos de Europol serán:

1) El Consejo de Administración.

2) El Director.

3) El Interventor Financiero.

4) El Comité Presupuestario.

Artículo 28. Consejo de Administración.

1. Europol estará dotada de un Consejo de Administración. El Consejo de Administración:

1) Participará en la ampliación de los objetivos de Europol (apartado 2 del artículo 2).

2) Establecerá por unanimidad los derechos y obligaciones de los funcionarios de enlace para con Europol (artículo 5).

3) Determinará por unanimidad el número de funcionarios de enlace que los Estados miembros pueden enviar a Europol (artículo 5).

4) Preparará las normas de desarrollo aplicables a los ficheros (artículo 10).

5) Participará en la adopción de las normas relativas a las relaciones de Europol con los Estados y organismos terceros, según el apartado 4 del artículo 10 (artículos 10, 18 y 42).

6) Definirá por unanimidad el método de ordenación del sistema de índice (artículo 11).

7) Aprobará por mayoría de dos tercios las disposiciones de creación de ficheros (artículo 12).

8) Podrá tomar posición en relación con las observaciones y los informes de la autoridad común de control (artículo 24).

9) Examinará los problemas que la autoridad común de control señale a su atención (apartado 5 del artículo 24).

10) Definirá los pormenores del procedimiento de control de la licitud de las solicitudes en el marco del sistema de información (artículo 16).

11) Participará en el nombramiento y destitución del Director y de los Directores adjuntos (artículo 29).

12) Supervisará el correcto desempeño de las funciones del Director (artículos 7 y 29).

13) Participará en la adopción del estatuto del personal (artículo 30).

14) Participará en la redacción de acuerdos sobre protección del secreto y en la adopción de normas sobre protección del secreto (artículos 18 y 31).

15) Participará en la confección del presupuesto, incluida la plantilla, en la censura de cuentas y en la aprobación de la gestión del Director (artículos 35 y 36).

16) Adoptará por unanimidad el plan financiero quinquenal (artículo 35).

17) Nombrará por unanimidad al Interventor Financiero y le controlará en el ejercicio de sus funciones (artículo 35).

18) Participará en la adopción del reglamento financiero (artículo 35).

19) Aprobará por unanimidad la celebración del acuerdo de sede (artículo 37).

20) Adoptará por unanimidad las normas de habilitación de los agentes de Europol.

21) Se pronunciará por mayoría de dos tercios sobre los litigios que enfrenten a un Estado miembro con Europol o a Estados miembros entre sí, en relación con las indemnizaciones por responsabilidades derivadas de un tratamiento ilícito o incorrecto (artículo 38).

22) Participará en la modificación del Convenio (artículo 43).

23) Será responsable de otras tareas que le encargue el Consejo, en particular en el marco de las disposiciones de aplicación del presente Convenio.

2. El Consejo de Administración estará compuesto de un representante por Estado miembro. Cada miembro del Consejo de Administración dispondrá de un voto.

3. Cada uno de los miembros del Consejo de Administración podrá hacerse sustituir por un miembro suplente; en caso de ausencia del titular, el miembro suplente podrá ejercer el derecho de voto de éste.

4. La Comisión de las Comunidades Europeas será invitada a participar en las reuniones del Consejo de Administración, sin derecho a voto. Sin embargo, el Consejo de Administración podrá acordar que sus deliberaciones tengan lugar en ausencia del representante de la Comisión.

5. Los miembros titulares o suplentes podrán ser acompañados y asesorados por expertos de sus Estados miembros durante las deliberaciones del Consejo de Administración.

6. La presidencia del Consejo de Administración corresponderá al representante del Estado miembro que ejerza la presidencia del Consejo.

7. El Consejo de Administración se dotará de un reglamento interno adoptado por unanimidad.

8. Las abstenciones no serán óbice para la adopción de acuerdos del Consejo de Administración que requieran unanimidad.

9. El Consejo de Administración se reunirá al menos dos veces al año.

10. El Consejo de Administración adoptará cada año por unanimidad:

1) Un informe general sobre las actividades de Europol durante el año transcurrido.

2) Un informe de previsión de las actividades de Europol en el que se tendrán en cuenta las necesidades operativas de los Estados miembros y las incidencias en el presupuesto y la plantilla de Europol.

Estos informes se presentarán al Consejo de acuerdo con el procedimiento del Título VI del Tratado de la Unión Europea.

Artículo 29. Director.

1. La dirección de Europol estará a cargo de un Director, que será nombrado por unanimidad por el Consejo, oído el Consejo de Administración, y de acuerdo con el procedimiento establecido en el Título VI del Tratado de la Unión Europea, para un período de cuatro años renovable una sola vez.

2. El Director estará asistido por Directores adjuntos. El Consejo determinará el número de Directores adjuntos, que serán nombrados por el procedimiento que se contempla en el apartado 1 para un período de cuatro años, renovable una sola vez. Sus funciones serán precisadas por el Director.

3. El Director será responsable:

1) De la ejecución de las tareas que competen a Europol.
2) De la administración ordinaria.
3) De la gestión del personal.
4) De la preparación y ejecución adecuadas de los acuerdos del Consejo de Administración.
5) De la elaboración de los proyectos de presupuesto, de plantilla y del plan financiero quinquenal, así como de la ejecución del presupuesto de Europol.
6) De todas las demás tareas que le encomiende el presente Convenio o el Consejo de Administración.

4. El Director rendirá cuentas de su gestión al Consejo de Administración y participará en las sesiones del Consejo de Administración.

5. El Director será el representante legal de Europol.

6. Oído el Consejo de Administración, el Director y los Directores adjuntos podrán ser destituidos por decisión del Consejo, que deberá adoptarse por mayoría de dos tercios de los votos de los Estados miembros, según el procedimiento establecido en el Título VI del Tratado de la Unión Europea.

7. No obstante lo dispuesto en los apartados 1 y 2, el primer mandato del Director será de cinco años a partir de la entrada en vigor del Convenio, de cuatro años para el primer Director adjunto y de tres años para el segundo Director adjunto.

Artículo 30. Personal.

1. El Director, los Directores adjuntos y los agentes de Europol se guiarán en su actividad por los objetivos y las funciones de Europol y, salvo disposición contraría del presente Convenio, y sin perjuicio del Título VI del Tratado de la Unión Europea, no podrán solicitar ni recibir orientación alguna de ningún Gobierno, autoridad, organización o persona ajena a Europol.

2. El Director es el superior jerárquico de los Directores adjuntos y de los agentes de Europol. El nombra y destituye a los agentes. En la selección de personal deberá tener en cuenta, además de la idoneidad personal y de la capacidad profesional, el que exista un adecuado reparto entre nacionales de todos los Estados miembros y entre las lenguas oficiales de la Unión Europea.

3. Los aspectos concretos quedarán regulados por un estatuto del personal que adoptará el Consejo por unanimidad, oído el Consejo de Administración, de acuerdo con el procedimiento establecido en el Título VI del Tratado de la Unión Europea.

Artículo 31. Confidencialidad.

1. Europol y los Estados miembros garantizarán mediante medidas adecuadas, la protección de las informaciones confidenciales que se recopilen o intercambien con Europol en virtud del presente Convenio. Para ello, el Consejo adoptará por unanimidad una normativa pertinente sobre protección del secreto, previamente preparada por el Consejo de Administración y presentada al Consejo con arreglo al procedimiento del Título VI del Tratado de la Unión Europea.

2. Cuando Europol deba encomendar a una o varias personas una actividad delicada desde el punto de vista de la seguridad, los Estados miembros se comprometerán a llevar a cabo, a solicitud del Director de Europol, las pesquisas de seguridad respecto de las personas de su nacionalidad con arreglo a sus normas nacionales y a prestarse asistencia mutuamente a este respecto. La autoridad que con arreglo a la normativa nacional sea competente para la investigación de seguridad sólo comunicará a Europol el resultado de dicha investigación, que tendrá efecto vinculante para Europol.

3. Los Estados miembros y Europol sólo podrán confiar el tratamiento de datos en los servicios de Europol a personas especialmente preparadas para ello, y que hayan sido sometidas a un control de seguridad.

Artículo 32. Obligación de reserva y confidencialidad.

1. Los órganos de Europol y sus miembros, los Directores adjuntos y los agentes de Europol y los funcionarios de enlace se abstendrán de toda actividad y, en particular, de toda manifestación de opinión que pueda atentar contra la dignidad de Europol o perjudicar a sus actividades.

2. Los órganos de Europol y sus miembros, los Directores adjuntos y los agentes de Europol y los funcionarios de enlace, así como todas las demás personas expresamente obligadas a mantener reserva o guardar el secreto, estarán obligadas a observar la mayor discreción en todo lo que se refiere a los hechos y asuntos de los que hayan tenido conocimiento en el desempeño de sus funciones o en el marco de su actividad, tanto frente a personas no facultades como frente al público en general. Esta obligación no se aplicará a hechos y asuntos que no requieran el secreto. La obligación de reserva y de confidencialidad persiste, asimismo, tras el cese en sus funciones, la expiración de su contrato de trabajo o el fin de su actividad. La obligación mencionada en la primera fase será notificada por Europol y se señalarán las consecuencias penales de su incumplimiento; la notificación constará por escrito.

3. Los órganos de Europol y sus miembros, los Directores adjuntos, los agentes de Europol y los funcionarios de enlace, así como las personas sujetas a la obligación prevista en el apartado 2 no podrán, si no han sometido la cuestión al Director o, en el caso del Director, al Consejo de Administración, testimoniar ni hacer declaraciones en procedimientos judiciales ni extrajudiciales acerca de hechos de los que hayan tenido conocimiento en el desempeño de sus funciones o de su actividad.

El Director o el Consejo de Administración, según el caso, se pondrán en contacto con la autoridad judicial o con cualquier otro órgano competente a fin de tomar las medidas necesarias, en función del Derecho nacional que se aplique al órgano de que se trate, bien para que se definan las condiciones en que se prestará testimonio, con objeto de garantizar la confidencialidad de la información, o bien, si el Derecho nacional lo permite, para denegar la comunicación referente a la información de que se trate cuando así lo exija la protección de intereses primordiales de Europol o de un Estado miembro.

Si la legislación del Estado miembro reconoce el derecho a negarse a testificar, las personas cuyo testimonio se solicite, deberán recibir la debida autorización para testificar. Corresponderá al Director o, si es él quien debe prestar testimonio, al Consejo de Administración, dar esa autorización. Cuando un funcionario de enlace tenga que testificar acerca de información que haya obtenido de Europol, esta autorización se concederá previo acuerdo del Estado miembro al que pertenezca dicho funcionario de enlace.

Además, cuando el testimonio pueda incluir información datos transmitidos por un Estado miembro o que parezcan afectar a un Estado miembro, se deberá recabar el dictamen de dicho Estado miembro antes de dar la autorización.

Sólo se podrá denegar la autorización para testificar cuando así lo requieran intereses superiores dignos de la protección de Europol o de la del Estado o Estados miembros afectados.

Esta obligación subsistirá, asimismo, después del cese en sus funciones, de la expiración de su contrato de trabajo o al término de su actividad.

4. Cada Estado miembro considerará que el incumplimiento de la obligación de reserva o de guardar secreto, a que se refieren los apartados 2 y 3, constituye una violación de sus disposiciones legales sobre el respeto del secreto profesional o de sus disposiciones relativas a la protección de documentos confidenciales.

Si ha lugar, cada Estado miembro promulgará, a más tardar en la fecha de entrada en vigor del presente Convenio, las normas de Derecho interno o las disposiciones que sean necesarias para castigar las violaciones de la obligación de reserva o de guardar secreto contemplada en los apartados 2 y 3. Tomará las medidas necesarias para que dichas normas y disposiciones se apliquen, asimismo, a aquellos de sus propios agentes que, en el desempeño de su actividad, estén relacionados con Europol.

Artículo 33. Lenguas.

1. Los informes y toda la documentación que se dé a conocer al Consejo de Administración deberán presentársele en todas las lenguas oficiales de la Unión Europea; las lenguas de trabajo del Consejo de Administración serán las lenguas oficiales de la Unión Europea.

2. De las traducciones necesarias para los trabajos de Europol se hará cargo el Centro de Traducción de los órganos de la Unión.

Artículo 34. Información al Parlamento Europeo.

1. La Presidencia del Consejo dirigirá anualmente al Parlamento Europeo un informe especial sobre los trabajos realizados por Europol. Para la modificación del presente Convenio se consultará al Parlamento Europeo.

2. Respecto del Parlamento Europeo, la Presidencia del Consejo o el representante designado por ella tendrá en cuenta las obligaciones de reserva y de protección del secreto.

3. Las obligaciones contempladas en el presente artículo no afectan a los derechos de los Parlamentos nacionales, a las disposiciones del artículo K.6 del Tratado de la Unión Europea ni a los principios generales aplicables a las relaciones con el Parlamento Europeo en virtud del Título VI del Tratado de la Unión Europea.

Artículo 35. Presupuesto.

1. Todos los ingresos y gastos de Europol, incluidos los gastos de la Autoridad Común de Control y de la Secretaría instaurada por dicha autoridad con arreglo al artículo 24, deberán ser objeto de previsiones para cada ejercicio presupuestario y consignarse en el presupuesto. Se adjuntará al presupuesto un cuadro de personal. El ejercicio presupuestario comenzara el 1 de enero y finalizará el 31 de diciembre.

El presupuesto deberá estar equilibrado en ingresos y gastos.

Junto con el presupuesto se establecerá un plan financiero quinquenal.

2. El presupuesto se financiará mediante las contribuciones de los Estados miembros y mediante otros ingresos ocasionales. La contribución de cada Estado miembro se determinará en función de la fracción que represente su producto nacional bruto en la suma total de los productos nacionales brutos de los Estados miembros correspondientes al año anterior a aquel en que se establezca el presupuesto. A efectos del presente artículo se entenderá por «producto nacional bruto» el producto nacional bruto determinado con arreglo a la Directiva 89/130/CEE, Euratom del Consejo, de 13 de febrero de 1989, sobre armonización del cálculo del producto nacional bruto a precios de mercado.

3. El Director elaborará el proyecto de presupuesto y el cuadro del personal para el ejercicio siguiente a más tardar el 31 de marzo de cada año y lo presentará, una vez examinado por el Comité Presupuestario de Europol, al Consejo de Administración, junto con el proyecto de plan financiero quinquenal.

4. El Consejo de Administración decidirá sobre el plan financiero quinquenal. El acuerdo en tal sentido del Consejo de Administración se tomará por unanimidad.

5. El Consejo, oído el Consejo de Administración, establecerá el presupuesto de Europol a más tardar el 30 de junio del año anterior al ejercicio presupuestario con arreglo al procedimiento del Título VI del Tratado de la Unión Europea. El acuerdo del Consejo se tomará por unanimidad. Se seguirá el mismo procedimiento para los presupuestos rectificativos y suplementarios. La aprobación del presupuesto por parte del Consejo supone la obligación por parte de cada Estado miembro de abonar a tiempo la contribución financiera que le corresponda.

6. El Director ejecutará el presupuesto conforme a las disposiciones del reglamento financiero previsto en el apartado 9.

7. Los controles sobre el compromiso y el pago de los gastos, así como los controles sobre la determinación y el cobro de los ingresos, los realizará un Interventor Financiero nombrado por unanimidad por el Consejo de Administración y que será responsable ante éste. El reglamento financiero podrá contemplar que, para determinados ingresos o gastos, el control por el Interventor Financiero se efectúe a posteriori.

8. El Comité Presupuestario estará constituido por un representante de cada Estado miembro experto en cuestiones de presupuesto. Su cometido será preparar las deliberaciones sobre cuestiones presupuestarias y financieras.

9. El Consejo aprobará, mediante el procedimiento a que se refiere el Título VI del Tratado de la Unión Europea y por unanimidad, el Reglamento Financiero; especificando, en particular, el procedimiento de elaboración, modificación y ejecución del presupuesto y de control de su ejecución, así como las formas de pago de las contribuciones financieras de los Estados miembros.

Artículo 36. Censura de cuentas.

1. Las cuentas relativas a todos los ingresos y gastos consignados en el presupuesto, así como el Balance de Activos y Pasivos de Europol, se someterán una vez al año a un control conforme a lo dispuesto en el Reglamento Financiero. Para ello, el Director presentará un informe sobre el cierre de cada ejercicio antes del 31 de mayo del año siguiente.

2. Realizará la censura de cuentas un Comité conjunto de Auditoría formado por tres Auditores, que serán designados por el Tribunal de Cuentas de las Comunidades Europeas a propuesta de su Presidente. El mandato de los Auditores será de tres años, se sucederán de manera que cada año sea sustituido el Auditor que haya sido miembro del Comité Conjunto de Auditoría durante tres años. No obstante, lo dispuesto en la segunda frase, al constituirse el primer Comité conjunto de Auditoría una vez haya empezado a funcionar Europol, el mandato del miembro que, por sorteo.

Ocupe el primer lugar, será de dos años.

Ocupe el segundo lugar, será de tres años.

Ocupe el tercer lugar, será de cuatro años.
Los gastos de la censura de cuentas, si los hay, se consignarán en el presupuesto a que se refiere el artículo 35.
3. El Comité conjunto de Auditoría presentará al Consejo, según el procedimiento previsto en el Título VI del Tratado de la Unión Europea, un informe anual sobre la censura de las cuentas del ejercicio transcurrido, antes de la presentación de ese informe, el Director y el Interventor Financiero podrán emitir su dictamen sobre el informe, que será sometido a debate en el Consejo de Administración.
4. El Director de Europol facilitará a los miembros del Comité Conjunto de Auditoría toda la información y les prestará toda la asistencia que necesiten para el cumplimiento de su cometido.
5. El Consejo decidirá sobre la aprobación de la ejecución del presupuesto por parte del Director previo examen del informe de cierre del ejercicio.
6. En el Reglamento Financiero se precisará el procedimiento de la censura de cuentas.
Artículo 37. Acuerdo de sede.
Las disposiciones necesarias sobre la instalación de Europol en el Estado de la sede y sobre los servicios que dicho Estado deberá prestar, así como las normas especiales aplicables en el Estado de la sede de Europol a los miembros de sus órganos, a sus Directores adjuntos, a sus Agentes y a los miembros de sus familias, se establecerá en un acuerdo de sede entre Europol y el Reino de los Países Bajos, que se celebrará tras aprobación por unanimidad del Consejo de Administración.

TITULO VI

Responsabilidad y protección jurídica

Artículo 38. Responsabilidad en caso de tratamiento ilícito o incorrecto de datos.
1. De conformidad con su Derecho nacional de cada Estado miembro, responderá de cualquier perjuicio causado a las personas en el que intervengan datos que adolezcan de errores de derecho o de hecho almacenados o tratados por Europol. La víctima sólo podrá reclamar indemnización al Estado miembro en que se haya producido el hecho que originó el perjuicio y deberá acudir a los Tribunales que sean competentes en virtud del Derecho nacional de ese Estado. Ningún Estado miembro podrá invocar el hecho de que otro Estado miembro o Europol ha transmitido datos incorrectos para eludir la responsabilidad que le corresponda con arreglo a su Derecho nacional con respecto a una persona perjudicada.
2. Si los datos que adolecen de errores de derecho o de hecho resultan de una transmisión indebida o del incumplimiento de las obligaciones que establece el presente Convenio por uno o varios Estados miembros o de un almacenamiento o tratamiento ilícito o incorrecto por Europol, ésta o el Estado o Estados miembros deberán reintegrar, a instancia de parte, las cantidades abonadas a modo de indemnización, a no ser que el Estado miembro en cuyo territorio se haya cometido el hecho que causó el perjuicio haya utilizado los datos incumpliendo el presente Convenio.
3. Cualquier desacuerdo entre Estado miembro y Europol u otro Estado miembro relativo al principio o la cuantía del reintegro deberá someterse al Consejo de Administración, que se pronunciará por mayoría de dos tercios.
Artículo 39. Otros tipos de responsabilidad.
1. La responsabilidad contractual de Europol se regirá por el Derecho aplicable al contrato de que se trate.
2. En el ámbito de la responsabilidad extracontractual, Europol, independientemente de la responsabilidad prevista en el artículo 38, estará obligada a indemnizar los daños causados por sus órganos, Directores adjuntos o Agentes en el ejercicio de sus funciones, siempre que estos daños les sean imputables. Esto no excluye la posibilidad de que se presenten otras solicitudes de indemnización según la legislación de los Estados miembros.
3. El perjudicado podrá exigir que Europol se abstenga de realizar una acción o que la anule.
4. La jurisdicción nacional de los Estados miembros competente para entender de litigios referentes a la responsabilidad de Europol, contemplada en el presente artículo se determinará por referencia a las disposiciones pertinentes del Convenio de Bruselas de 27 de septiembre de 1968 (RCL 1991\217 y 1151) relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, con las adaptaciones introducidas posteriormente en virtud de Convenios de adhesión.
Artículo 40. Resolución de controversias y de litigios.
1. Las controversias entre los Estados miembros acerca de la interpretación o aplicación del presente Convenio deberán, en una primera etapa, estudiarse en el Consejo según el procedimiento del Título VI del Tratado de la Unión Europea, con miras a su resolución.
2. Si transcurrido un plazo de seis meses no ha podido llegarse a una solución, los Estados miembros entre los que exista la controversia se concertarán sobre el procedimiento por el que se solucionará la controversia.
3. Las disposiciones sobre las vías de recurso, a que se refiere la reglamentación relativa al régimen aplicable a los Agentes temporales y Auxiliares de las Comunidades Europeas, serán aplicables, por analogía, al personal de Europol.
Artículo 41. Privilegios e inmunidades.
1. Europol, los miembros de sus órganos, sus Directores adjuntos y sus Agentes gozarán de los privilegios e inmunidades necesarios para el ejercicio de sus funciones conforme a un Protocolo que contendrá la normativa que deberá aplicarse en todos los Estados miembros.
2. El Reino de los Países Bajos y los demás Estados miembros acordarán, en los mismos términos para los funcionarios de enlace enviados por los demás Estados miembros y para los miembros de sus familias, los privilegios e inmunidades necesarios para el cumplimiento correcto de las funciones de los funcionarios de enlace en Europol.
3. El Protocolo, de que habla el apartado 1, lo adoptará el Consejo por unanimidad, de acuerdo con el procedimiento previsto en el Título VI del Tratado de la Unión Europea y lo aprobarán los Estados miembros según sus respectivas normas constitucionales.

TITULO VII

DISPOSICIONES FINALES

Artículo 42. Relaciones con Estados e instancias terceros.

1. En la medida en que sea útil para el ejercicio de las funciones definidas en el artículo 3, Europol establecerá y mantendrá relaciones de cooperación con instancias terceras a tenor de los puntos 1 a 3 del apartado 4 del artículo 10. El Consejo de Administración establecerá por unanimidad las normas para dichas relaciones. La presente disposición se entiende sin perjuicio de los apartados 4 y 5 del artículo 10 y el apartado 2 del artículo 18. Los intercambios de datos de carácter personal se realizarán exclusivamente con arreglo a lo dispuesto en los Títulos II, III y IV del presente Convenio.

2. En la medida en que sea necesario para el ejercicio de las funciones definidas en el artículo 3, Europol podrá, además, establecer y mantener relaciones con los Estados y otras instancias terceros a tenor de los puntos 4 a 7 del apartado 4 del artículo 10. El Consejo, por unanimidad, establecerá las normas para las relaciones mencionadas en la primera frase, previo dictamen del Consejo de Administración, con arreglo al procedimiento a que se refiere el Título VI del Tratado de la Unión Europea. Será de aplicación por analogía la tercera frase del apartado 1.

Artículo 43. Modificación del Convenio.

1. El Consejo, por unanimidad, oído el Consejo de Administración, decidirá, conforme a lo dispuesto en el apartado 9 del artículo K.1 del Tratado de la Unión Europea y con arreglo al procedimiento a que se refiere el Título VI del Tratado de la Unión Europea, las modificaciones del presente Convenio, recomendará a los Estados miembros que adopten dichas modificaciones según sus respectivas normas constitucionales.

2. Las modificaciones entrarán en vigor de conformidad con el apartado 2 del artículo 45 del presente Convenio.

3. No obstante, a instancia de un Estado miembro y previo examen por el Consejo de Administración, el Consejo, según el procedimiento a que se refiere el Título VI del Tratado de la Unión Europea, podrá decidir, por unanimidad, que se enriquezcan, se modifiquen o se completen las definiciones de las formas de delincuencia contempladas en el anexo. Podrá decidir, asimismo, que se añadan nuevas definiciones relacionadas con dichas formas de delincuencia.

4. El Secretario general del Consejo de la Unión Europea notificará a todos los Estados miembros la fecha de entrada en vigor de las modificaciones.

Artículo 44. Reservas.

No se admitirán reservas con respecto al presente Convenio.

Artículo 45. Entrada en vigor.

1. El presente Convenio se someterá a la adopción, por parte de los Estados miembros, según sus respectivas normas constitucionales.

2. Los Estados miembros notificarán al depositario la conclusión de los procedimientos exigidos por sus respectivas normas constitucionales para la adopción del presente Convenio.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la conclusión de un período de tres meses después de que sea efectuada la notificación, a que se refiere el apartado 2, por el Estado miembro de la Unión Europea en la fecha de adopción por el Consejo del acto por que se establece el presente Convenio, que efectúe este trámite en último lugar.

4. Sin perjuicio de lo dispuesto en el apartado 2, Europol sólo iniciará sus actividades con arreglo al presente Convenio cuando entre en vigor el último de los actos jurídicos previstos en el apartado 7 del artículo 5, el apartado 1 del artículo 10, el apartado 7 del artículo 24, el apartado 3 del artículo 30, el apartado 1 del artículo 31, el apartado 9 del artículo 35, el artículo 37 y los apartados 1 y 2 del artículo 41.

5. Con el comienzo de las actividades de Europol cesará la actividad de la Unidad de Drogas de Europol con arreglo a la acción común del Consejo, de 10 de marzo de 1995, relativa a la Unidad de Drogas de Europol. En ese momento, Europol pasará a ser propietaria de todo el equipamiento financiado con cargo al presupuesto común de la Unidad de Drogas de Europol, desarrollado o creado por la Unidad de Drogas de Europol o puesto a su disposición por el Estado de la sede para utilización gratuita y permanente, así como de la totalidad de los archivos y bancos de datos administrados de modo autónomo por dicha Unidad.

6. A partir de la adopción por el Consejo del acto por el que se establece el presente Convenio, los Estados miembros tomarán, de forma individual o conjunta y en el marco de sus normativas nacionales, todas las medidas preparatorias necesarias para que Europol pueda emprender sus actividades.

Artículo 46. Adhesión de nuevos Estados miembros.

1. El presente Convenio estará abierto a la adhesión de cualquier Estado que se convierta en miembro de la Unión Europea.

2. El texto del Convenio en la lengua del Estado que se adhiera a él, establecido por el Consejo de la Unión Europea, será texto auténtico.

3. Los instrumentos de adhesión se depositarán ante el depositario.

4. El presente Convenio entrará en vigor, respecto del Estado miembro que se adhiera a él, el primer día del mes siguiente a la conclusión de un período de tres meses tras el depósito de su instrumento de adhesión o en la fecha de entrada en vigor del Convenio si éste no hubiera entrado en vigor al concluir el mencionado período.

Artículo 47. Depositario.

1. El Secretario general del Consejo de la Unión Europea será el depositario del presente Convenio.

2. El depositario publicará en el «Diario Oficial de las Comunidades Europeas» las notificaciones, instrumentos o comunicaciones referentes al presente Convenio.

ANEXO

MENCIONADO EN EL ARTICULO 2

Lista de otras formas graves de delincuencia internacional de las que Europol podría ocuparse además de las ya

enunciadas en el apartado 2 del artículo 2 y en cumplimiento de los objetivos de Europol según se enuncian en el apartado 1 del artículo 2

Delitos contra la vida, la integridad física y la libertad:
Homicidio voluntario, agresión con lesiones graves.
Tráfico ilícito de órganos y tejidos humanos.
Secuestro, retención ilegal y toma de rehenes.
Racismo y xenofobia.
Delitos contra la propiedad, los bienes públicos y delitos de fraude:
Robos organizados.
Tráfico ilícito de bienes culturales, incluidas las antigüedades y obras de arte.
Fraude y estafa.
Chantaje y extorsión de fondos.
Violación de derechos de propiedad industrial y falsificación de mercancías.
Falsificación de documentos administrativos y tráfico de documentos falsos.
Falsificación de moneda, falsificación de medios de pago.
Delito informático.
Corrupción.
Comercio ilegal y delitos contra el medio ambiente:
Tráfico ilícito de armas, municiones y explosivos.
Tráfico ilícito de especies animales protegidas.
Tráfico ilícito de especies y esencias vegetales protegidas.
Delitos contra el medio ambiente.
Tráfico ilícito de sustancias hormonales y otros factores de crecimiento.

Además, con arreglo al apartado 2 del artículo 2, el hecho de solicitar a Europol que se haga cargo de una de las formas de delincuencia aquí enumeradas implica que tendrá, asimismo, competencia para ocuparse del blanqueo de dinero relacionado con la misma y de los delitos conexos.

Por lo que respecta a las formas de delincuencia enumeradas en el apartado 2 del artículo 2, a efectos del presente Convenio, se entenderá por:

Delincuencia relacionada con materiales nucleares y radiactivos: Los delitos enumerados en el apartado 1 del artículo 7 de la Convención sobre protección física de los materiales nucleares, firmada en Viena y en Nueva York el 3 de marzo de 1980 (RCL 1991\2562), y que se refieran a materiales nucleares o radiactivos, o a ambos, tal como se definen en el artículo 197 del Tratado Euratom y en la Directiva 80/836/Euratom, de 15 de julio de 1980, respectivamente.

Introducción ilegal de inmigrantes: Las acciones destinadas a facilitar deliberadamente, con fines de lucro, la entrada, la estancia o el trabajo en el territorio de los Estados miembros de la Unión Europea, con incumplimiento de las reglamentaciones y las condiciones aplicables en los Estados miembros.

Trata de seres humanos: El acto de someter a una persona al poder real e ilegal de otras personas mediante la violencia o mediante amenazas o abusando de una relación de autoridad o mediante engaño, en particular con objeto de entregarse a la explotación de la prostitución ajena, a formas de explotación y de violencias sexuales respecto de menores de edad o al comercio ligado al abandono de niños.

Delincuencia relacionada con el tráfico de vehículos robados: El robo o la sustracción de automóviles de turismo, de camiones, de semirremolques, de cargamentos de camiones o semirremolques, de autobuses, de motocicletas, de caravanas, de vehículos agrícolas, de vehículos para obras y de recambios de vehículos, así como la receptación de los citados objetos.

Actividades ilícitas de blanqueo de dinero: Los delitos enumerados en los apartados 1 a 3 del artículo 6 del Convenio del Consejo de Europa sobre reciclaje, identificación, secuestro y confiscación de los beneficios del delito, firmado en Estrasburgo el 8 de noviembre de 1990.

Las formas de delincuencia mencionadas en el artículo 2 y en el presente anexo serán valoradas por los servicios nacionales competentes según la legislación nacional de los Estados a los que pertenezcan.

DECLARACIONES

Ad apartado 1 del artículo 10.

«Cuando se elaboren las disposiciones de ejecución relativas al apartado 1 del artículo 10, la República Federal de Alemania y la República de Austria continuarán velando por que se afirme el siguiente principio:

Los datos relativos a las personas, a que se hace mención en el punto 1 de la primera frase del apartado 1 del artículo 10 y distintos de los enumerados en los apartados 2 y 3 del artículo 8, se almacenarán únicamente cuando, por la naturaleza o las circunstancias de los hechos o por cualquier otra consideración, haya motivos para suponer que deben iniciarse procedimientos penales contra dichas personas por delitos que sean competencia de Europol en virtud del artículo 2.»

Ad apartados 1 y 3 del artículo 14, apartado 2 del artículo 15 y apartado 8 del artículo 19.

1. «La República Federal de Alemania y la República de Austria procederán a la transmisión de los datos con arreglo al presente Convenio en el entendimiento de que, para la explotación y el tratamiento no automatizados de los datos, esperan que Europol y los Estados miembros respeten el espíritu de las disposiciones del presente Convenio relativas a la protección jurídica de los datos.»

2. «El Consejo declara, habida cuenta de los apartados 1 y 3 del artículo 14, del apartado 2 del artículo 15 y del apartado 8 del artículo 19 del Convenio, que en lo que se refiere al respeto del nivel de protección de los datos intercambiados entre los Estados miembros y Europol con respecto a su tratamiento no automatizado, Europol elaborará, a los tres años de inicio de sus actividades y con la participación, en sus respectivos ámbitos de competencias, de la autoridad común de control y de las autoridades nacionales de control, un informe que, tras su estudio por el Consejo de Administración, se someterá al examen del Consejo.»

Ad apartado 2 del artículo 40.

«Los siguientes Estados miembros convienen en que, en tal caso, someterán sistemáticamente la controversia al Tribunal de Justicia de las Comunidades Europeas:

El Reino de Bélgica.
El Reino de Dinamarca.
La República Federal de Alemania.
La República Helénica.
El Reino de España.
La República Francesa.
Irlanda.
La República Italiana.
El Gran Ducado de Luxemburgo.
El Reino de los Países Bajos.
La República de Austria.
La República Portuguesa.
La República de Finlandia.
El Reino de Suecia.»

Ad artículo 42.

«El Consejo declara que Europol debería establecer, con carácter prioritario, relaciones con los servicios competentes de los Estados con los cuales las Comunidades Europeas y sus Estados miembros hayan entablado un diálogo estructurado.»

Estados parte .....
Países ..... Fecha de- notificación .....
Alemania ..... 3-2-1998 .....
Austria ..... 30-1-1998 .....
Bélgica ..... 12-6-1998 .....
Dinamarca ..... 17-11-1997 .....
España ..... 9-6-1997 .....
Finlandia ..... 30-12-1997 .....
Francia ..... 6-1-1998 .....
Grecia ..... 11-6-1998 .....
Irlanda ..... 11-3-1998 .....
Italia ..... 30-4-1998 .....
Luxemburgo ..... 12-6-1998 .....
Países Bajos ..... 24-12-1997 .....
Portugal ..... 29-12-1997 .....
Reino Unido de Gran Bretaña e Irlanda del Norte ..... 10-12-1996 .....
Suecia ..... 5-12-1996 .....

El presente Convenio entrará en vigor, de forma general y para España, el 1 de octubre de 1998, de conformidad con lo dispuesto en su artículo 45.

MEMORIA DE 1998 - ANEXO VIII - INFORME DE ACTIVIDADES DE LA AUTORIDAD DE CONTROL COMÚN SCHENGEN
/Div.
SCHENGEN
ES

Autoridad de Control Común
Bruselas, 26 de marzo de 1999
SCH/Aut-Cont (99) 8, 2a rev.
Traducción: orig. PT/FR

3er INFORME DE ACTIVIDADES DE LA AUTORIDAD DE CONTROL COMÚN
Marzo de 1998 - Febrero de 1999

ÍNDICE:

Nota de síntesis

PRIMERA PARTE: INTRODUCCIÓN

SEGUNDA PARTE: UN AÑO DE ACTIVIDAD DE LA ACC

CAPÍTULO I: DICTÁMENES Y RECOMENDACIONES DE LA ACC

CAPÍTULO II: ACTIVIDADES DE CONTROL

CAPÍTULO III: CAMPAÑA DE INFORMACIÓN

CAPÍTULO IV: INTEGRACIÓN EN LA UNIÓN EUROPEA Y ACERVO DE LA ACC

CAPÍTULO V: FUNCIONAMIENTO DE LA ACC

TERCERA PARTE: RELACIONES DE LA ACC EN EL INTERIOR Y EL EXTERIOR DE LA ESTRUCTURA SCHENGEN

CUARTA PARTE: REACCIONES DE LAS AUTORIDADES SCHENGEN AL INFORME ANUAL DE LA ACC

QUINTA PARTE: EL FUTURO DE LA ACC EN EL NUEVO MARCO INSTITUCIONAL

SEXTA PARTE: ANEXOS

1. Las misiones de la ACC previstas en el Convenio

2. Dictámenes y recomendaciones de la ACC durante el ejercicio 1998-1999

3. Relación de los dictámenes de la ACC y reacciones de los órganos ejecutivos y técnicos

4. Pro Memoria
Las instancias comunes para la aplicación del Convenio
Objetivo y arquitectura del SIS
Oficinas Sirene
Protección de datos de carácter personal

5. Organigrama de los grupos de trabajo Schengen

6. Declaración de la ACC con motivo del 50 Aniversario de la Declaración Universal de Dere-

chos Humanos

7. Lista de los dictámenes, decisiones y recomendaciones con miras a la integración en la Unión Europea

8. Reglamento de la ACC

9. Principios generales aplicables a las visitas y controles del C.SIS

10. Lista de los miembros de la ACC

11. Descripciones en el SIS

12. Índice cronológico

13. Protocolo del Tratado de Amsterdam relativo a Schengen

DECLARATION OF THE JSA OBSERVER STATES

Having observer status in the JSA, the Nordic countries share the concerns of the full members as expressed in the annual report. They also share the main viewpoints expressed in the opinions referred. Among other things, it is of greatest importance that the advice and opinions given is observed and respected by the central as well as the national bodies in the Schengen system.

The presence of the Nordic national data and privacy protection commissions in the JSA is of utmost importance in the efforts aiming at ensuring common, public acceptance and support of the important work done in accordance with the Schengen Convention. The Nordic observers are of the opinion that the JSA need to have its resources strengthened in the future and hope that the integration in EU will enable this, without compromising the JSA status as an independent authority.

NOTA DE SÍNTESIS

La presentación del 3er informe anual de la Autoridad de Control Común de Schengen (marzo de 1998 - febrero de 1999) coincide con el año de transformación del marco institucional para la aplicación de los Acuerdos de Schengen, en virtud de la entrada en vigor del Tratado de Amsterdam.

Esta transformación implica nuevas normas, nuevos derechos y una mayor transparencia en la estructura de la organización Schengen y en el funcionamiento del sistema de información.

En continuidad con los años precedentes, 1998 fue un año de afirmación de la independencia de la Autoridad de Control Común, en cuanto órgano al que compete velar por los derechos de los ciudadanos frente al Convenio de Aplicación del Acuerdo de Schengen, en particular por lo que respecta a la protección de datos de carácter personal.

La ACC inició una amplia batalla por la transparencia y la información: fue ampliamente divulgado el informe anual; se inició en varios países la campaña "El Sistema de Información Schengen le interesa", con la difusión de un cartel y folletos informativos sobre los derechos de los ciudadanos; se promovió el 1er coloquio sobre "Los derechos de los ciudadanos frente a los sistemas de información policial", y se realizó una conferencia de prensa al objeto de presentar el informe.

Las comisiones de protección de datos nacionales presentaron a sus Parlamentos respectivos el informe anual, y algunas lo publicaron en sus páginas en Internet. El informe también se presentó a las instancias Schengen y se envió al Parlamento Europeo.

La ACC propuso nuevos mecanismos de interacción y de cooperación con los organismos ejecutivos de Schengen con vistas a agilizar la información común, y por primera vez, intervino defendiendo sus puntos de vista en una reunión del Comité Ejecutivo.

La ACC siguió las líneas orientadoras que trazara a comienzos de año: se emitieron dictámenes; se le informó sobre el estudio y el desarrollo técnico del futuro sistema; se llevó a cabo por primera vez una acción global de fiscalización de todas las Oficinas Sirene, realizándose recomendaciones con vistas al refuerzo de la seguridad en el intercambio de información complementaria; se dio publicidad a la actividad de la ACC y a los derechos de los ciudadanos; se insistió e hizo todo en pro de un funcionamiento eficaz de Schengen.

En el ámbito de su misión de control del sistema central, la ACC decidió realizar un control específico.

A pesar de todas las iniciativas y propuestas presentadas por la ACC, el Comité Ejecutivo no adoptó las medidas de refuerzo de nuestros recursos humanos, técnicos y financieros, tal y como había prometido. Para que haya un control democrático, no basta con la existencia formal de una autoridad independiente; es indispensable que ésta funcione con los medios e instrumentos necesarios. Lo anterior cobra particular importancia en el marco de la evolución de los sistemas europeos de información policial (Europol, Eurodac y Sistema de Información Aduanera) y del refuerzo de las medidas de cooperación en la lucha contra la gran criminalidad organizada.

Importa, por ello, profundizar los mecanismos de cooperación entre las autoridades de control comunes, que tienen como misión en cada uno de estos sistemas la salvaguardia de los valores fundamentales de la libertad y la ciudadanía. Es fundamental encontrar en el marco de la Unión Europea la exacta medida que permita seguir manteniendo una elevada seguridad en el SIS, y que éste sea objeto de un control independiente y efectivo.

Hacemos votos por que la integración de la Autoridad de Control Común en la Unión Europea sea realizada de forma armoniosa, sin perjuicio del mantenimiento de un control continuo e independiente. La experiencia y el acervo de la actividad de la ACC son necesarios para el futuro de los sistemas policiales europeos.

En este año de cambio, mi agradecimiento a todos los que han participado en los trabajos de la Autoridad de Control Común, a las autoridades de control nacionales, a los representantes de los Estados en el Comité Ejecutivo y en el Grupo Central, así como a los grupos técnicos y a la Secretaría de Schengen, por estos años de trabajo en común.

El trabajo realizado ha valido la pena, en aras de la construcción europea, la libertad, los derechos de los ciudadanos y la seguridad común.

Marzo de 1999

El Presidente
João Labescat

PRIMERA PARTE: INTRODUCCIÓN

La Autoridad de Control Común fue instituida el 26 de marzo de 1995. Estos cuatro años de funcionamiento permanente han constituido la primera experiencia de una entidad independiente de control común de un sistema policial de ámbito europeo. La labor en defensa de los ciudadanos que asumió la ACC desde el principio, adquiere particular relieve en 1998, que marca el 50 Aniversario de la Declaración Universal de los Derechos Humanos.

La actividad de la ACC ha acompañado las vicisitudes del funcionamiento de este sistema de información, el cual actualmente contiene datos de Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos y Portugal. Las misiones que los Estados confiaron a la ACC se han cumplido. Este último año de actividad es un ejemplo de ello.

Ya en junio de 1992 se había constituido, en virtud de una decisión ministerial, una Autoridad provisional (APCC), la cual dio los primeros pasos en la preparación de la aplicación de los principios sobre protección de datos.

El objetivo del Convenio de Aplicación del Acuerdo de Schengen es permitir la supresión de los controles en las fronteras interiores de los Estados miembros, creando de este modo un gran espacio de libre circulación de personas y manteniendo en el interior del mismo un nivel de seguridad por lo menos igual al que existía anteriormente.

Entre las medidas compensatorias previstas en el Convenio que apuntan a este objetivo figuran la armonización de la política en materia de expedición de visados, una política común en materia de determinación del Estado responsable del examen de las solicitudes de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico ilegal de estupefacientes, la armonización del nivel de control de las fronteras exteriores del territorio Schengen y la creación de un Sistema de Información Schengen (SIS).

Este sistema común establece una conexión entre todos los países que aplican el Convenio de Aplicación del Acuerdo de Schengen, y ofrece a sus usuarios (servicios encargados de misiones de policía, embajadas y consulados, servicios de extranjería, etc.) la posibilidad de disponer en tiempo real de la información necesaria para sus misiones que ha sido introducida en el sistema por cualquier de los Estados miembros que aplican 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 objetos (vehículos, armas, documentos, billetes de banco robados, sustraídos u ocultados fraudulentamente).

El funcionamiento del Sistema de Información Schengen presupone obligatoriamente la institución y funcionamiento de la Autoridad de Control Común para la protección de los datos de carácter personal (ACC), encargada de velar en particular por el respeto de las disposiciones del Convenio relativas a la unidad de apoyo técnico del SIS (artículo 115). A este órgano, compuesto por dos representantes de cada una de las autoridades de control de las Partes Contratantes, se le confió igualmente una función de asesoramiento y armonización de las prácticas o doctrinas nacionales.

Son miembros de la ACC los representantes de las autoridades de control de datos de los diez Estados que participan en el sistema. Las autoridades de Dinamarca, Finlandia, Islandia, Noruega y Suecia participan igualmente en la labor de la ACC con el estatuto de observadores.

En 1998, cumpliendo el programa de acción que fuera aprobado, la ACC centró su actividad en las siguientes áreas:

* por primera vez, llevó a cabo en todas las Oficinas Sirene una fiscalización global, formulando un conjunto de recomendaciones con vistas al refuerzo de la seguridad;

* preparó el control específico del sistema central, que será realizado en el primer semestre de 1999;

* hizo un seguimiento de los trabajos de desarrollo del SIS I + y de los estudios preliminares del SIS II;

* definió el acervo comunitario con vistas a la integración de Schengen en la Unión Europea;

* lanzó la campaña "El Sistema de Información Schengen le interesa", con la distribución de un cartel y folletos informativos sobre los derechos de los ciudadanos, particularmente en las áreas de entrada al espacio Schengen (aeropuertos, fronteras marítimas etc.);

* emitió dictámenes, en especial sobre el acceso a datos del sistema Schengen por parte de los servicios encargados del registro de vehículos;

* organizó el primero coloquio sobre "Los derechos de los ciudadanos frente a los sistemas policiales" (Lisboa).

La transparencia y la información sobre su labor y sobre los derechos de los ciudadanos ha sido una preocupación constante para la ACC. De la misma forma, ha procurado establecer un sistema más ágil de información mutua entre ella y los restantes organismos de Schengen. A tal efecto, la ACC invitó en varias ocasiones a responsables de diversos grupos de trabajo.

En la actualidad se hallan introducidas en el SIS cerca de nueve millones de descripciones que pueden ser consultadas en miles de terminales, por miles de policías y autoridades judiciales de diez países de la Unión Europea. En el año 1998, se registró un aumento del número de datos en el SIS con la integración de Austria, Italia y Grecia. Es necesario que en el nuevo marco institucional, el nivel de seguridad de todos los elementos del sistema de información siga siendo elevado y que el control independiente se mantenga.

SEGUNDA PARTE: UN AÑO DE ACTIVIDAD DE LA ACC

CAPÍTULO I : DICTÁMENES Y RECOMENDACIONES DE LA ACC

I.1 Seguridad de las Oficinas SIRENE: una acción coordinada en todos los países

El 12 de diciembre de 1997, la Autoridad de Control Común decidió proceder a una verificación de las medidas de seguridad adoptadas por las Oficinas SIRENE. Esta decisión se tomó a raíz de una fuga de documentos y de informaciones de una de las Oficinas Sirene, ocurrida en el mes de noviembre de aquel año.

Las comisiones nacionales de control de los diez Estados que aplican el Convenio realizaron, por lo tanto, el control de su Oficina SIRENE.

En cooperación con la Comisión para la protección de la vida privada de Bélgica, la Presidencia de la ACC participó igualmente en una reunión, el 31 de marzo de 1998, con responsables belgas de la cooperación policial internacional. En dicha reunión, se informó a la ACC sobre las iniciativas adoptadas y previstas con miras a reforzar la seguridad de la Oficina SIRENE en la que se había detectado dicha fuga.

Tomando como base los informes nacionales, la ACC elaboró un documento de síntesis relativo a la seguridad de las Oficinas Sirene. El papel de la ACC se consideró benéfico para estimular la armonización de las medidas de seguridad de los diferentes Estados.

La ACC subrayó que la red de Oficinas Sirene debe cumplir todos los requisitos del artículo 118 del Convenio de Aplicación (en materia de seguridad).

La ACC propuso un conjunto de recomendaciones al objeto de su observancia en las Oficinas SIRENE que todavía no las aplican, y de las que cabe destacar:

* la necesidad de mantener el nivel mas alto posible de seguridad física, en particular garantizando que el acceso a los datos quede limitado al personal autorizado;
* el encriptado de los datos siempre que haya intercambio de información y cuando sean archivados, la definición de normas comunes de seguridad aplicables al personal de las oficinas, así como la designación de un responsable de la seguridad;
* la promoción de acciones de formación específica sobre seguridad de la información, destinadas a los usuarios del sistema;
* la elaboración regular de informes sobre la seguridad para su presentación a las autoridades nacionales de control.

La ACC destacó la buena cooperación de todas las entidades nacionales implicadas y manifestó su satisfacción por el hecho de que esta acción de fiscalización, coordinada en todos los países, hubiese contribuido a la mejora sensible de la seguridad de la información, condición indispensable para asegurar la confianza de los ciudadanos y de las instituciones democráticas en el funcionamiento del sistema Schengen

Estas recomendaciones fueron aprobadas, junto con el informe de síntesis, el 11 de diciembre de 1998. Dicha síntesis se envió el 8 de enero de 1999 al Comité Ejecutivo, al Grupo Central y al Grupo de trabajo SIRENE. Se aprobó además un comunicado de prensa que la resumía. La ACC espera ahora las reacciones de los órganos ejecutivos de Schengen.

I.2. Dictamen sobre el acceso de los servicios encargados del registro de vehículos al SIS

El 16 de junio, el Grupo Central transmitió a la ACC una solicitud de dictamen formulada por el Grupo de trabajo SIRENE. Dicha solicitud versaba sobre las condiciones de acceso de los servicios encargados del registro de vehículos a los datos del SIS, y por la misma se invitaba a la ACC a dar su interpretación de la noción de datos de carácter personal. Según el grupo SIRENE, esta noción no cubría el número de bastidor de los vehículos.

El origen de tal solicitud se hallaba en el proyecto que preveía autorizar la consulta del SIS a los servicios encargados del registro de vehículos, al objeto de detectar los vehículos sustraídos que estén matriculados en el espacio Schengen, con ocasión de una solicitud de matriculación en el país de matriculación de origen o en otro país Schengen.

En su dictamen, aprobado el 6 de noviembre de 1998, la ACC hace constar que el acceso de los servicios encargados del registro de vehículos a los datos del SIS y la comparación de ficheros constituirían en varios Estados miembros infracciones al artículo 101 y a los apartados 2 y 4 del artículo 102 del CAAS. Con todo, la ACC estimó que, en caso de que los servicios encargados del registro de vehículos de ciertos Estados miembros cumplan las condiciones de competencia y de finalidad estipuladas por el Convenio y estén en condiciones de aplicar las medidas de seguridad referidas en el artículo 118 del Convenio, su acceso a los datos SIS sería admisible.

Dicho dictamen se transmitió al Grupo Central en cuanto Dictamen 98/5 de la ACC.

CAPÍTULO II : ACTIVIDADES DE CONTROL

II.1. Principios generales relativos a las visitas de control de la ACC al C.SIS

La ACC elaboró, en colaboración con el Ministerio del Interior francés, un conjunto de principios a fin de aclarar las modalidades de visita y de control de las instalaciones del sistema central (C.SIS). Estos principios se inscriben en las misiones previstas en el artículo 115 del Convenio de Schengen.

Tras un dilatado proceso de consultas mutuas, entre ellas una reunión celebrada en París entre la ACC y representantes del Ministerio del Interior francés, fue posible elaborar una propuesta concreta, la cual se examinó el 29 de junio de 1998 en presencia de representantes de dicho Ministerio.

Habiendo propuesto dichos representantes la introducción de modificaciones, la ACC examinó nuevamente el documento el 11 de septiembre de 1998, aprobándolo en la misma fecha. El 6 de noviembre de 1998, el Ministerio del Interior francés dio su aprobación al texto y lo sometió a los demás Estados Schengen para información.

El documento "Principios generales aplicables a las visitas y controles del C.SIS" (en anexo) define los tipos de visitas (de carácter general o de control), los mecanismos de información al Ministerio del Interior, la composición del grupo de visita o de control, la definición del programa de trabajo, el régimen de acceso a los documentos, y el sistema de evaluación de los informes técnicos y de garantía de su confidencialidad en la parte que respecta a la ACC.

La versión final de este documento pretende poner fin a interpretaciones restrictivas de la función de control de la ACC y es reflejo del espíritu de cooperación que pudo instaurarse con el Ministerio del Interior.

Este documento fue objeto de una comunicación al Grupo Central, en su reunión del 19 de febrero de 1999.

II.2. Control del C.SIS

Durante el año de 1998, la ACC preparó, junto con el Ministerio del Interior francés, los principios aplicables a las visitas

y al control del C.SIS (véase supra). El tiempo transcurrido desde el último control y el hecho de haberse integrado en el sistema tres nuevos países (Austria, Grecia e Italia) justificaba la realización de un nuevo control. La ACC decidió crear un grupo técnico, coordinado por el representante luxemburgués. En diversas ocasiones a lo largo del año, los expertos de las autoridades nacionales de control se reunieron para preparar este control, que se llevará a cabo en el primer semestre de 1999. Resultado del trabajo de este grupo ha sido la elaboración de una lista de los controles que han de efectuarse.

II.3 Grupos técnicos y expertos

El 27 de abril de 1998, el Presidente del Comité de Orientación y del Grupo de Trabajo Permanente expuso el estado de los trabajos relativos a la renovación y mejora del SIS (puesta en aplicación de la red Sirene fase II, así como preparación del SIS 1 + y del SIS II). Tal y como se anunció en dicha reunión, la ACC recibió en junio de 1998 varios documentos administrativos y técnicos relativos a la red SF II así como un CD-ROM sobre el C.SIS I.

Los miembros de la ACC lamentaron que en el momento en que la ACC solicitó ser asociada a los trabajos, ya no fuese posible -según el Presidente del Comité de Orientación- modificar las especificaciones técnicas para atender a sus demandas. Se anunció, no obstante, que éstas se tendrían en cuenta en el momento de la puesta en marcha del sistema.

Se les informó asimismo que no se había solicitado la certificación de seguridad del conjunto del sistema SIS II a fin de no provocar retrasos y un aumento de gastos. La certificación de cada componente seguirá siendo posible más adelante.

El 20 de noviembre de 1998, expertos de la ACC participaron en una reunión de información entre representantes de IBM y los expertos de los grupos de trabajo Schengen responsables del SIS II. Los expertos de IBM presentaron las diferentes opciones en cuanto a la futura arquitectura del sistema, así como los criterios de evaluación. Los expertos de la ACC no recibieron, sin embargo, informaciones de orden técnico o relativas a la seguridad, ni sobre las razones que justificaban la elección de 3 arquitecturas entre las 12 presentadas. Constataron que no era posible, en el momento de la presentación, anticipar las opciones futuras. Lamentaron, en particular, que IBM todavía no hubiese examinado los aspectos vinculados a la seguridad.

Basándose en el informe facilitado por sus expertos, la ACC pidió explicaciones sobre las razones que condujeron a la elección de estas tres opciones, así como la comunicación de documentos técnicos suplementarios.

Los coordinadores del proyecto respondieron a la invitación de la ACC, el 11 de diciembre de 1998. Presentaron un informe oral sobre el avance de los trabajos del estudio preliminar del SIS II. Resumieron las etapas preparatorias del procedimiento de adjudicación del estudio preliminar. Se dieron explicaciones detalladas a las delegaciones sobre el contenido de los estudios presentados por IBM y de las diferentes soluciones preconizadas. En cuanto la usurpación de identidad, problema planteado por la ACC y que fue objeto de dictamen, se anunció que se introduciría una solución en el SIS I+.

La ACC espera ahora poder tomar nota del pliego de condiciones a fin de conocer los criterios que han conducido a la elección de las arquitecturas, así como los criterios de seguridad. Una decisión tenía que adoptarse sobre la base del estudio detallado anunciado para el 22 de diciembre de 1998. A finales de febrero de 1999, la ACC todavía no había recibido dicha información.

CAPÍTULO III : CAMPAÑA DE INFORMACIÓN

III.1. Campaña de información de los ciudadanos sobre sus derechos frente al SIS

En 1997, la ACC decidió lanzar en todos los países una campaña de información dirigida a los ciudadanos, bajo el lema "El Sistema de Información Schengen le interesa". En efecto, la ACC había constatado que el ejercicio de los derechos de los ciudadanos, máxime los derechos de acceso y de verificación de datos, era reducido. Una de las razones de tal déficit es la falta de información pública.

Por ello, la ACC previó tal campaña en su plan de actividades y presupuesto, con el doble objetivo de dar a conocer los derechos de los ciudadanos consignados en el CAAS y contribuir a una mayor transparencia de los Acuerdos de Schengen.

La ACC elaboró folletos y carteles de cara a su difusión en las fronteras exteriores de Schengen por los servicios competentes en el plano nacional. Estos folletos y carteles se presentaron con ocasión de la reunión anual de Lisboa, en junio de 1998.

Por razones practicas, no fue posible lanzar inmediatamente las campañas de información. Las mismas dieron comienzo en diciembre de 1998 o a principios del año 1999 en algunos países (España, Grecia, Alemania, Portugal, Austria). Se anunció su lanzamiento en Bélgica, Luxemburgo e Italia, mientras que los Países Bajos tienen dificultades para la financiación de la campaña. Por su parte, la autoridad de control francesa vio cómo le negaban toda colabora - ción las autoridades competentes.

Conviene recordar que al principio, el Grupo Central había apoyado la campaña de la ACC, tanto con relación a la

impresión de los folletos como a su distribución.

III.2. Página Internet de la ACC

Movida por la misma inquietud de informar a los ciudadanos sobre sus derechos, la ACC decidió en 1998 crear una página en Internet. Los ciudadanos encontrarán en la misma información sobre las actividades de la ACC y sobre sus derechos. Este instrumento debería estar listo durante el año 1999.

III.3. Presentación del informe anual en la conferencia de prensa de Bruselas y reunión anual

La ACC presentó el informe anual en una conferencia de prensa que se celebró el 28 de abril en el Palacio de Egmont de Bruselas. Estuvieron presentes varios periodistas de agencias internacionales y dos cadenas de televisión. Este informe anual había sido transmitido con anterioridad a los representantes del Grupo Central.

La reunión anual se celebró en Lisboa los días 29 y 30 de junio de 1998. El objetivo principal de la ACC al promover esta reunión era contribuir a una mayor transparencia en el funcionamiento del Sistema de Información Schengen, con especial incidencia en los derechos de los ciudadanos. El informe anual de la ACC se presentó a la prensa.

El 30 de junio, la ACC organizó un coloquio sobre "Los derechos de los ciudadanos frente a los sistemas de información policial a través del modelo Schengen", en colaboración con la Comisión de Protección de Datos portuguesa. Las intervenciones incidieron en el papel de la ACC, la integración de Schengen en la Unión Europea, la cooperación entre los Estados, el intercambio de información de las Oficinas SIRENE, la integración de los sistemas de información policial, la protección de datos, y Europol y los sistemas de información policial en la Unión Europea. Asistió a la sesión de apertura el secretario de Estado adjunto del ministro de la Administración Interna (Armando Vara). Además del miembro del Gobierno portugués, hubo intervenciones del presidente del Grupo Central, del director general de la Dirección Justicia y Asuntos de Interior del Consejo de la Unión Europea, del coordinador adjunto de Europol, del presidente de la Autoridad de Control portuguesa y del presidente de la ACC. Intervinieron también el director general de la Policía Judicial portuguesa, la coordinadora de la Oficina Sirene portuguesa y el coordinador para los Asuntos de la Libre Circulación de Personas en el Espacio Europeo (Portugal). La reunión, abierta a los medios de comunicación, fue transmitida por Internet y tuvo gran eco en la prensa y la televisión. Participaron en el coloquio unas 100 personas. Además de altas autoridades del Estado portugués (Provedor de Justiça, Secretario de Estado para la Integración de las Minorías, Viceprocurador General de la República, Inspector General de la Administración Interna, Comandantes Generales de las Fuerzas de Seguridad), estuvieron presentes delegados de varios países del Grupo Central y de los Ministerios de Justicia (Italia, Austria, Noruega, Suecia).
La Comisión portuguesa editó las actas del coloquio en portugués e ingles.

CAPÍTULO IV : INTEGRACIÓN EN LA UNIÓN EUROPEA Y ACERVO DE LA ACC

A petición del Grupo Central, la ACC elaboró la lista de su acervo, en la perspectiva de la integración del acervo de Schengen en la Unión Europea. Se trata, en efecto, de definir el conjunto de las decisiones adoptadas en el marco de Schengen que formarán parte del conjunto de normas que rijan el funcionamiento de la ACC.

La elaboración de esta lista así como su transmisión directa por parte de la ACC a las instancias europeas era la continuación de una reunión del presidente de la ACC con el director general de la Dirección Justicia y Asuntos de Interior del Consejo de la Unión Europea, celebrada el 14 de febrero de 1998. La lista de los documentos constitutivos del acervo de la ACC, examinada en la reunión de esta última del 27 de abril de 1998, se envío al Consejo de la UE (Presidencia y DG JAI) el 18 de mayo de 1998. De la misma se transmitió copia al presidente del Grupo Central.

La lista incluye los dictámenes emitidos y los principios aprobados que ella considera como acervo. Se trata, en concreto, de los dictámenes emitidos con ocasión de la verificación de la correcta aplicación de las disposiciones del Convenio relativas al SIS o en el marco del examen de dificultades de aplicación o de interpretación que pueden sobrevenir con ocasión de la explotación del SIS, así como de los principios que consagran su independencia y que fueron aprobados por las instancias Schengen. En la lista de decisiones de la ACC consta igualmente el informe del control efectuado en el C.SIS, que tiene carácter confidencial.

En cuanto a la integración prevista del personal de la Secretaría Schengen en la Unión, la Autoridad de Control Común se pronunció en el sentido de que se realizase de forma equilibrada y justa. La ACC destacó que en el futuro, sería importante mantener el grado de conocimiento y de experiencia adquiridos a lo largo de estos años, lo que se considera fundamental para la actividad de la ACC.

En la reunión de la ACC del 11 de septiembre de 1998 se le informó de que los dictámenes y recomendaciones de la ACC no formarán parte del acervo de Schengen en cuanto tales, pero podrán ser confirmados por una decisión ulterior. A finales de febrero de 1999, la ACC todavía no había recibido oficialmente otra información.

Destacar que, de acuerdo con el Protocolo que integra el acervo de Schengen en el ámbito de la Unión Europea, previsto en el Tratado de Amsterdam, las decisiones y declaraciones adoptadas por el Comité Ejecutivo, así como los actos adoptados para la aplicación del Convenio por instancias a las que el Comité Ejecutivo haya atribuido competencias decisorias, constituyen acervo comunitario. Entre estas decisiones se encuentran algunas que se refieren a la ACC, en particular las que reconocen su estatuto independiente, la línea presupuestaria autónoma, los presupuestos anuales, y su acceso a los documentos y a la información Schengen.

En su reunión del 11 de diciembre de 1998, la ACC aprobó una nota recordando su acervo en el plano institucional y funcional, dando traslado de la misma al Grupo Central y al Comité Ejecutivo (con copia para el Consejo de la UE) para que la sometiera a examen del Grupo "Acervo" desde comienzos de 1999. La ACC encomendó a su Presidente que expusiera ante el Comité Ejecutivo el alcance de dicha nota. Como se ha señalado, el Comité Ejecutivo de diciembre de 1998 confió el examen de tal nota al Grupo Central.

CAPÍTULO V : FUNCIONAMIENTO DE LA ACC

V.1. Reuniones

La ACC celebró siete sesiones plenarias entre marzo de 1998 y marzo de 1999, así como dos reuniones de dos días, en Bruselas y Lisboa respectivamente.

Se promovieron además reuniones técnicas con vistas a la preparación del control del C.SIS y encuentros de técnicos de la ACC con responsables de la elaboración del estudio preliminar del SIS II (Lisboa y Bruselas).

El Presidente de la ACC estuvo presente en reuniones organizadas por el Grupo Central (Estrasburgo y Ostende) y, además, en la reunión del Comité Ejecutivo (Berlín).

V.2. Elecciones del presidente y del vicepresidente

El 11 de diciembre de 1998, los Sres. João Labescat y De Schutter fueron reelegidos por unanimidad presidente y vicepresidente, respectivamente.

V.3. Presupuesto de la ACC y apoyo de la Secretaría a la ACC

El principio de la asignación de una línea presupuestaria específica a la ACC fue reconocido por una decisión del Comité Ejecutivo adoptada en 1997, y constituye por lo tanto acervo en la perspectiva de la integración en la Unión Europea.

En su reunión del 27 de abril, la ACC aprobó su proyecto de presupuesto. Introdujo en el mismo una partida que permitiese reforzar el apoyo de la Secretaría a través de la contratación de una persona a tiempo completo, siguiendo una línea de rigor y de contención del gasto.

Un presupuesto así como el apoyo de una secretaría son elementos primordiales para garantizar la eficacia de la actividad de la ACC y el buen ejercicio de sus competencias. Los organismos ejecutivos se han negado a dotar a la ACC de los medios indispensables para su funcionamiento independiente.1

En su reunión de Lisboa del 29 de junio de 1998, la ACC observó que su solicitud de presupuesto para el año 1999 había sido transmitida al grupo de trabajo competente, el cual la había inscrito en el orden del día del Grupo Central, sensible a las consecuencias de una eventual integración de la Secretaría de Schengen en la del Consejo de la UE en el curso del año 1999. Según la ACC, su presupuesto para el año 1999 debía ser aprobado sin perjuicio de las consecuencias presupuestarias de esta eventual integración; es decir, la necesidad de prever la asunción de los gastos actualmente cubiertos por el presupuesto general.

A pesar de que con ocasión de un encuentro entre la Presidencia de la ACC y la Presidencia alemana de Schengen, esta última se había comprometió a apoyar su solicitud, la ACC supo en diciembre de 1998 que el Grupo Central había aprobado el presupuesto de la ACC para 1999, con la excepción de la partida prevista para reforzar su secretaría. Se acordó por lo tanto que el presidente de la ACC participaría en el Comité Ejecutivo de Berlín del 16 de diciembre de 1998 a fin de defender tal solicitud. El presidente expuso en particular las razones que justificaban la solicitud de presupuesto suplementario de la ACC para aumentar el apoyo que recibe actualmente de la Secretaría. Presentó además una nota de la ACC en la que se evaluaba el coste total de su funcionamiento, sin tener en cuenta las economías de escala de que benefician las reuniones Schengen que se celebran hasta la fecha en las instalaciones del Benelux (acervo institucional y funcional, véase supra). Los Ministros rechazaron la solicitud suplementaria de presupuesto.

A pesar de que equivalía a menos del 1% del presupuesto general, la propuesta fue rechazada. Por otra parte, si se compara la ayuda aportada por la Secretaría a la ACC en 1997 y 1998, se observa que la misma experimentó una disminución. En un marco general de cerca de 70 personas al servicio de la Secretaría, la ACC dispone únicamente de un asesor, el cual debe encargarse además de diferentes grupos de trabajo (dedicando a la ACC sólo 1/5 de su actividad). En estas decisiones el Comité Ejecutivo no ha tenido en cuenta las misiones encomendadas por el Convenio a la ACC.

Preocupada por esta falta manifiesta de apoyo de la parte de los órganos ejecutivos de Schengen, la ACC contiúa, no obstante, reclamando los recursos humanos, técnicos y financieros necesarios para el cumplimiento de sus misiones, actualmente y en el futuro marco institucional.

V.4. Reglamento interior

La ACC modificó su Reglamento interior el 27 de abril de 1998, a fin de tener en cuenta su independencia presupuestaria. Este reglamento fue completado por un nuevo artículo 11, titulado "Del presupuesto" (cf. SCH/Aut-cont (95) 25, 6ª rev.). Se consagra en él el principio aprobado por el Comité Ejecutivo de la existencia de una línea presupuestaria autónoma, cuyo importe debe ser acorde con las misiones realizadas anualmente por la ACC.

TERCERA PARTE: RELACIONES DE LA ACC EN EL INTERIOR Y EL EXTERIOR DE LA ESTRUCTURA SCHENGEN

1. Con la Comisión de Libertades Publicas del Parlamento Europeo

Ya en 1997, el presidente en ejercicio de la ACC había propuesto a la presidencia de la Comisión de Libertades Publicas del Parlamento Europeo la presentación a esta asamblea del informe anual de la ACC. Esta propuesta fue reiterada en 1998, sin que se haya dado curso a este ofrecimiento.
A dicha comisión parlamentaria se le enviaron varios ejemplares del informe anual.

2. Con el Grupo Central y el Comité Ejecutivo

La Presidencia de Schengen invitó a una delegación de la ACC a asistir a una reunión del Grupo Central que se desarrollaba en Estrasburgo el 4 de marzo de 1998, y en el curso de la cual se organizó una visita del C.SIS. Esta reunión de Estrasburgo permitió tomar nota del avance de los trabajos relativos a la mejora del SIS y a la puesta en aplicación de la red Sirene fase II.

En su carta del 12 de marzo de 1998 al Grupo Central (SCH/Aut-cont lettre (98) 4), el presidente de la ACC expresaba su agradecimiento al presidente del Grupo Central. Se trataba del primer encuentro de la ACC con el Grupo Central en composición plenaria, lo que le permitía a este último conocer el punto de vista de la ACC sobre el papel que desea desempeñar ante las instancias Schengen, en particular por lo que respecta las perspectivas futuras del SIS.

El Grupo Central aceptó asociar a la ACC a los trabajos sobre el estudio preliminar de la red Sirene fase II y del SIS I+. Esto permitirá a la ACC velar por que se tengan debidamente en cuenta en el futuro especificaciones técnicas que le permitan ejercer los controles previstos por el Convenio.

La ACC confirmó que, al igual que en el pasado, seguiría enviando sus dictámenes y decisiones a la presidencia del Grupo Central nada más aprobados. Sus actas también serán accesibles al Grupo Central desde su aprobación por la ACC.

Se acordó que, por su parte, el Grupo Central y los grupos técnicos procurarían poner a disposición de la ACC un máximo de documentos, en particular elaborando una lista de documentos técnicos aprobados por los grupos de trabajo y susceptibles de interesar a la ACC.

El 27 de abril de 1998, la ACC invitó a la Troika del Grupo Central a su reunión. Sólo el presidente en ejercicio pudo responder a esta invitación.

El presidente del Grupo Central confirmó la importancia que atribuía a los trabajos de la ACC, declarando su deseo de apoyarla en su campaña de información pública. Declaró que velaría por que los grupos de trabajo competentes examinasen los dictámenes y recomendaciones de la ACC. Anunció la presentación de un informe en respuesta a los dictámenes y recomendaciones de la ACC (en particular los emitidos a raíz del control del C.SIS en 1996), ya aprobado por el Grupo Central el 20 de abril de 1998. Indicó igualmente que respaldaría la solicitud de apoyo suplementario para la ACC, la cual suscitó la atención del Grupo Central y cuyo examen fue confiado al grupo de expertos financieros competente.

El Presidente participó, a instancia de la presidencia del Grupo Central, en el "Seminario sobre el SIS" (Ostende, 24 de junio de 1998). Pudo así completar la información dada por el presidente del Comité de Orientación a los Pecos, respecto a las exigencias del Convenio relativas a la protección de datos de carácter personal y a la existencia de una autoridad de control nacional independiente.

El Presidente de la ACC participó en la reunión del Comité Ejecutivo celebrada en Berlín el 16 de diciembre de 1998. De esta forma, pudo presentar a la Ministros diferentes documentos, a saber: la solicitud de presupuesto suplementario para la ACC al objeto de aumentar el apoyo que recibe actualmente de la Secretaría, y el documento relativo al acervo organizatorio de la ACC. Como ya se ha señalado, la primera petición fue rechazada, mientras que el acervo organizatorio, cuya aprobación y transmisión al Grupo "Acervo de Schengen" de la Unión Europea solicitaba la ACC, fue reenviado al Grupo Central.

3. Comisión permanente de aplicación del Convenio

El Comité Ejecutivo constituyó una comisión de visita a fin de verificar la buena aplicación del Convenio por los Estados Schengen. Alemania será el primer país visitado por dicha comisión. Uno de los grupos de visita creados a tal efecto procederá a diversas verificaciones en la Oficina SIRENE alemana, así como en los terminales SIS. La ACC recordó al Grupo Central las competencias que le confiere el Convenio, solicitando por lo tanto que la asociaran a tales controles. En respuesta, se invitó a su presidente a asistir a la reunión entre la Autoridad de Control alemana y el grupo de visita

SIS.

En su reunión del 12 de febrero de 1999, la ACC decidió insistir ante la presidencia del Grupo Central a fin de que representantes de la autoridades de control alemana puedan acompañar a esta comisión de visita durante toda su misión. Las verificaciones se refieren, en efecto, a aspectos tratados en los artículos 126 y siguientes, para los cuales la competencia de la autoridad nacional de control no ofrece lugar a dudas. El Grupo Central rechazó esta petición en su reunión del 19 de febrero de 1999.

Vista la negativa del Grupo Central, la ACC protestó formalmente ante el presidente del Comité Ejecutivo, llamando la atención hacia el hecho de que se atribuyeran a una comisión poderes de investigación ad hoc en el ámbito de los datos de carácter personal, olvidando que el Convenio prevé un sistema propio con vistas a garantizar tales principios. Se efectúan controles y verificaciones sin tener en cuenta los órganos y las entidades competentes al respecto. Estas verificaciones no pueden considerarse como una mera suma de diferentes partes, sino como un todo que integra los N. SIS, el C.SIS y las Oficinas Sirene.

La ACC manifestó su extrañeza por que delegaciones que todavía no participan en el sistema y que no tienen datos en él pudieran accedan a información de carácter personal, mientras que se aparta a la ACC y a las autoridades naciona - les de protección de datos, que son entidades independientes, de tales controles en el marco de la actividad de la comisión permanente.

CUARTA PARTE: REACCIONES DE LAS AUTORIDADES SCHENGEN AL INFORME ANUAL DE LA ACC

En el curso del año 1998, el Grupo Central había respondido al informe anual de la ACC a través de un informe que indicaba el estado de las reflexiones de los grupos de trabajo sobre los dictámenes de la ACC, o, en el caso de algunos de ellos, el curso que se les había dado. Este estado de los trabajos ponía de manifiesto que numerosos dictámenes de la ACC planteaban cuestiones técnicas a las que no era posible aportar respuesta, o que ésta sólo sería posible en el marco de la renovación del SIS. LA ACC no ha deseado entrar en una polémica estéril, y se ha limitado a tomar nota de dicho informe.

El informe de respuesta, elaborado por la Presidencia belga durante el primer semestre de 1998, fue remitido un año tras la presentación del 1er informe a los organismos ejecutivos por la ACC, lo que constituye un plazo demasiado largo. Algunas recomendaciones, relativas al control del C.SIS realizado en octubre de 1996, se debatieron en el seno del Comité de Orientación el 22 de julio de 1997, y sólo pasados nueve meses la ACC fue informada de su valoración. De la lista de recomendaciones cabe constatar que la mayoría están pendientes de ejecución y aplicación, a lo que se invoca la existencia de problemas técnicos y financieros (a pesar de haber sido tenidas en cuenta, de acuerdo con la información disponible, en el desarrollo previsto del sistema).

La ACC consideró, en cuanto al estado de evaluación de sus dictámenes, que debe obtener respuestas en tiempo útil y no esperar un año para conocer eventuales deliberaciones sobre sus propuestas. La misión de control de la ACC no es compatible con tales plazos.

A la ACC le extrañó que el Grupo Central hubiese adoptado el principio de respuesta anual, a semejanza de lo que ocurre en el Consejo de Europa. Sucede que el Sistema de Información Schengen funciona las 24 horas del día, los 365 días del año, y la ACC ejerce un poder de control sobre el mismo. No es una entidad consultiva, sino una autoridad.

La ACC consideró que las decisiones que se refieran a sus misiones deben ser comunicadas rápidamente, nada más adoptadas por los grupos competentes de Schengen.

El Presidente de la ACC dio a conocer esta posición al Grupo Central en la reunión de Bonn del 5 de noviembre.

El 11 de diciembre de 1998, la ACC tomó nota del informe del Comité de Orientación que comentaba el 2º informe anual de la ACC (SCH/OR-SIS (98) 133, 2ª rev. - Marzo de 1997 a Marzo de 1998 -). Este informe fue aprobado por el Grupo Central el 24 de noviembre de 1998.

La ACC constató que dicho informe contenía varias afirmaciones erróneas. Así, el Comité de Orientación niega que la ACC tenga competencia en materia de armonización de prácticas, cuando tal competencia le viene atribuida por el apartado 3 del artículo 115 del Convenio. Considera tal Comité que dicha competencia le incumbe a él.

Por otra parte, este informe subraya que el Convenio no prevé la obligación de poner en práctica las recomendaciones de la ACC, y deniega la asignación de una cuenta de usuario propia de la ACC, limitada a la función de auditoría del sistema informático, lo que se halla en contradicción con el apartado 2 del artículo 115. En efecto, es esencial para una auditoría de las características del SIS que exista tal función, exigencia de un sistema de control independiente, a menos que éste dependa siempre de la acción del que es controlado.

Los participantes aprobaron una respuesta que fue transmitida al Grupo Central el 3 de febrero de 1999 (SCH/Aut-cont-Lettre (98) 1).

En dicha respuesta, la ACC reafirma que es inaceptable que las respuestas de los órganos ejecutivos se reciban transcurridos doce meses -como fue el caso del informe anual de la ACC relativo a 1996- u ocho meses, en el caso del informe anual correspondiente a 1997.

QUINTA PARTE: EL FUTURO DE LA ACC EN EL NUEVO MARCO INSTITUCIONAL

Dentro de unos dos meses entrará en vigor el Tratado de Amsterdam. El marco institucional del funcionamiento de Schengen quedará modificado positivamente con el refuerzo de los derechos de los ciudadanos, el control democrático del Parlamento Europeo y la tutela jurisdiccional efectiva del Tribunal de Justicia. Es un paso trascendental para la ciudadanía europea y para la seguridad común.

En el seno de la Unión todavía se está deliberando sobre las modificaciones en el funcionamiento de los sistemas de información policiales y del respectivo control independiente.

La ACC presentó a la Unión Europea y al Grupo Central, tras habérsele solicitado, la relación de las materias que considera constituyen acervo comunitario. Asimismo, informó a estas entidades sobre su programa de trabajo en el futuro próximo, incluyendo una estimación presupuestaria, el apoyo de secretaría y el número de reuniones anuales.

En cuanto al acervo, destacar que una parte sustancial de las materias que se refieren al funcionamiento de la ACC son efecto jurídico directo del Convenio de Aplicación (en particular sus misiones y poderes) o tienen su base en decisiones del Comité Ejecutivo (p.ej. línea presupuestaria autónoma, presupuesto acorde a las misiones, acceso a los documentos y a la información).

La integración del SIS en la estructura comunitaria debe ir acompañada de la continuidad del control independiente de la ACC y su actividad no debe verse afectada por esta integración. Según declaraciones realizadas por un responsable de la Dirección General de Justicia y Asuntos de Interior de la UE, presente en una de las reuniones de la ACC, estaría garantizada una integración armoniosa.

Es preciso recordar que los sistemas de información europeos experimentarán una evolución sensible en el próximo año. Se acerca el momento de la aplicación de los Convenios de Europol, del sistema de información aduanero y del sistema Eurodac, siendo muy importante que se encuentre la mejor fórmula que permita que todos los sistemas funcionen en armonía, con un control independiente y eficaz.

El marco legislativo de la protección de datos en cada uno de los países de la Unión Europea se encuentra en estos momentos en profunda transformación.

La armonización legislativa en Europa y la profundización de la cooperación entre las autoridades nacionales de control, y entre éstas y la UE, tendrán indiscutiblemente como resultado una mayor eficacia del funcionamiento de los sistemas y un régimen más coherente de salvaguardia de los derechos.

SEXTA PARTE: ANEXOS

1. LAS MISIONES DE LA AUTORIDAD DE CONTROL PREVISTAS EN EL CONVENIO

Los Estados que ratificaron el Convenio han atribuido como misión principal a la ACC la de controlar la unidad de apoyo técnico del SIS, misión que sólo ella puede llevar a cabo (apartado 2 del artículo 115). También le incumbe formular dictámenes y velar por la armonización de las prácticas o de las doctrinas nacionales.

Dada su composición y las competencias que se le han otorgado, la ACC es una entidad independiente de la estructura Schengen, con verdaderos poderes, entre las cuales se encuentran las que resultan del control del C.SIS (acceso, verificación de la legalidad, elaboración de informes).

El Convenio de Aplicación del Acuerdo de Schengen especifica sus misiones:

* Emite dictámenes 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 (apartado 3 del artículo 106);

* Analiza las dificultades de aplicación o de interpretación que puedan surgir con motivo de la explotación del SIS;

* Estudia los problemas que se planteen durante el ejercicio de control independiente efectuado por las autoridades nacionales de control de las Partes contratantes;

* Estudia los problemas que se planteen durante el ejercicio del derecho de acceso al sistema;

* Elabora propuestas armonizadas con vistas a encontrar soluciones para los problemas existentes (apartado 3 del artículo 115);

* Elabora informes que remitirá a los organismos a los cuales las autoridades de control nacionales remiten sus informes (apartado 4 del artículo 115);

* Se le informa sobre 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 (apartado 2 del artículo 118).

Por lo que respecta a los intercambios de información fuera del SIS:

* Puede, 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 (letra f del apartado 3 del artículo 126);

* Puede, 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 (apartado 1 del artículo 127).

2. DICTÁMENES Y RECOMENDACIONES DE LA ACC

En el anterior informe (marzo de 1997 a marzo de 1998) pudo reunirse la mayor parte de los dictámenes emitidos en 1998, razón por la cual no vuelven a figurar en el presente informe, a pesar de su actualidad.

En este informe se incluye el dictamen sobre el acceso al SIS por parte de las autoridades encargadas del registro de vehículos y el informe sobre la seguridad de los Oficinas SIRENE.

DICTAMEN Nº 98/5 DE LA AUTORIDAD DE CONTROL COMÚN A LA ATENCIÓN DEL COMITÉ EJECUTIVO

Asunto : Acceso al Sistema de Información Schengen (SIS) por parte de las autoridades encargadas del registro de vehículos.

I. De conformidad con el artículo 93 del Convenio de Aplicación de Acuerdo de Schengen, el principal objetivo del Sistema de Información Schengen consiste en preservar el orden y la seguridad públicos de las Partes Contratantes. Este instrumento se utiliza asimismo en el procedimiento de expedición de visados, para la expedición de permisos de residencia y la aplicación de la legislación en materia de extranjería en el marco de dicho Convenio.

Según el artículo 101.4 del Convenio, la elaboración de la lista de autoridades habilitadas para consultar directamente los datos del SIS es responsabilidad de cada una de las Partes Contratantes, comunicándose dicha lista al Comité Ejecutivo. La lista debe elaborarse respetando los criterios definidos por el artículo 101.1 y 2 por lo que respecta al tipo de instancias implicadas y a las misiones que se los asignen a nivel nacional. En concreto, el derecho a consultar directamente los datos está reservado exclusivamente a las instancias competentes para los controles fronterizos y demás comprobaciones policiales y aduaneras, así como, por lo que respecta al artículo 96, para la expedición de visados y de permisos de residencia y la administración de los extranjeros.

A día de hoy, las autoridades competentes para el registro de vehículos no figuran en esta lista, puesto que se trata en la mayoría de los Estados miembros de autoridades administrativas que tienen un ámbito de competencias diferente. Las autoridades encargadas del registro de vehículos solicitan ahora, al menos en algunos Estados miembros, tener acceso a los datos relativos a los objetos buscados previstos por el artículo 100, pues consideran que en caso contrario existiría una deficiencia en el sistema de búsqueda por lo que respecta a los vehículos cuya matrícula se ha solicitado en el país mientras que han sido robados en el extranjero. Es innegable que el acceso de dichas autoridades al SIS constituye una necesidad real.

II. VALORACIÓN JURÍDICA

II.a. Tipo de datos: Conviene recordar en primer lugar que el número de bastidor forma parte de los datos relativos a los objetos buscados en el sentido del artículo 100. En su dictamen de 7 de marzo de 1997, la Autoridad de Control Común ha indicado que la información relativa a ciertas características de los vehículos, como por ejemplo la marca, el tipo, el color y las características técnicas, no deben considerarse datos de carácter personal en la medida en que no tienen relación con la matrícula, con su propietario o con el conductor del vehículo. En el punto f) de su Dictamen 98/3, de 3 de febrero de 1998, la Autoridad de Control Común clasifica no obstante el número de bastidor como dato de carácter personal, habida cuenta de que puede conducir a la identificación del propietario o del conductor del vehículo.
Si no puede establecerse ninguna relación entre el número de bastidor de un vehículo y su propietario, la ACC considera que el número de bastidor de un vehículo no es en cuanto tal un dato de carácter personal. Con todo, las normas sobre explotación y uso del SIS (Capítulo 2 del Título IV del Convenio) son aplicables al margen de si se trata o no de datos personales, lo que significa que el artículo 101 - que especifica las autoridades con competencia exclusiva para consultar directamente el SIS - sigue siendo de aplicación incluso si el destinatario de la información no puede identificar a una persona.

II.b. Instancias habilitadas para consultar el SIS: Para la mayor parte de los Estados miembros no cabe duda de que el acceso a los datos del SIS por parte de las autoridades encargadas del registro de vehículos sería ilícito. De conformidad con el artículo 101.1 del Convenio, el acceso a los datos integrados en el SIS está reservado exclusivamente a las instancias competentes para los controles fronterizos y las comprobaciones policiales y aduaneras ejercidas en el interior del país, así como para la coordinación de las mismas. Ahora bien, las autoridades encargadas del registro de vehículos no tienen competencia en la mayoría de los Estados miembros para efectuar comprobaciones policiales, sino

que se trata de meras instancias administrativas.

II.c. Finalidad de la consulta al SIS: Según el artículo 102.4, los datos no podrán utilizarse con fines administrativos. Por otra parte, el Convenio prevé "medidas que adoptar" para cada tipo de descripción. Se deduce de ello que, so pena de infringir el principio de finalidad, sólo deberán estar autorizadas a consultar el SIS las autoridades competentes para adoptar dichas medidas. Según la información a la que ha tenido acceso la ACC, las verificaciones que los servicios encargados del registro de vehículos desean efectuar gracias a la consulta al SIS con de carácter administrativo. Dichos servicios no son competentes para adoptar las medidas indicadas, y tampoco tendrían la posibilidad concreta de hacerlo.

III. CONCLUSIONES

1. El acceso de los servicios de matriculación de vehículos a los datos del SIS y la comparación de ficheros constituirían en varios Estados miembros infracciones a los artículos 101 y 102.2 y 4 del Convenio de Schengen.

2. No obstante, si los servicios de matriculación de ciertos Estados miembros cumplen las condiciones de competencia y de finalidad impuestas por el Convenio, y se hallan en condiciones de aplicar las medidas de seguridad estipuladas en el artículo 118 del Convenio, la ACC considera admisible el principio de dicho acceso, a condición de que tales datos sean utilizados para los fines previstos en el artículo 100.

INFORME DE LA ACC SOBRE LA SEGURIDAD DE LOS OFICINAS SIRENE

En su reunión del 12 de diciembre de 1997, la Autoridad de Control Común decidió proceder a una verificación de las medidas de seguridad adoptadas por las Oficinas SIRENE. Esta decisión se tomó a raíz de una fuga de documentos producida cierto tiempo atrás en una Oficina SIRENE.

Todos los miembros de la ACC de los países que aplican el Convenio procedieron por lo tanto a la realización de controles de sus Oficinas SIRENE y transmitieron el informe respectivo a la Secretaría de la ACC.

Los informes de las autoridades nacionales describen la situación en los ámbitos de la seguridad física y de las conexiones entre la Oficina SIRENE y el N.SIS; describen igualmente las funciones de trazado que permiten por un lado identificar la oficina y el terminal, pero también identificar el operador que tuvo acceso a una aplicación (como por ejemplo una actualización), así como las condiciones de acceso a los datos del SIS y a los archivos manuales.

Basándose en estas constataciones, la ACC concluye que se han realizado esfuerzos para mejorar la seguridad del sistema, pero que deben proseguirse.

La ACC recuerda en efecto los siguientes principios:

* las oficinas SIRENE deben respetar todas las condiciones recogidas en el artículo 118 del Convenio de Aplicación de Schengen;
* el nivel de seguridad de las Oficinas SIRENE nacionales no puede ser inferior al del SIS.

Partiendo de estos principios, la ACC propone que se adopten las siguientes disposiciones en los Estados miembros en los que aún no sean de aplicación :

1. Mantener la seguridad física al más alto nivel, actualizando las técnicas utilizadas. En los países donde se hayan constatado lagunas, aportar las modificaciones necesarias con la mayor brevedad e informar a la Autoridad de Control nacional.

2. Cifrar las conexiones entre el SIRENE y el N.SIS y someter este cifrado al control de los miembros de las autoridades de control.

3. a) Crear un sistema de trazado de todas las operaciones posibles que se refieran a la base de datos del N.SIS y de la Oficina SIRENE (número de consultas, horario, tipo de datos consultados, etc.).
b) Realizar una explotación regular de los ficheros de trazado para la detección de anomalías, en particular en cuanto al número de consultas.

4. Limitar y controlar el acceso a los archivos manuales de los expedientes.

5. Cifrar la información recogida en soporte informático.

6. a) Reforzar las medidas tendentes a garantizar que el acceso esté efectivamente limitado a los datos para los cuales los operadores disponen de autorización, concretamente, en particular verificando regularmente sus autorizaciones de acceso y cambiando regularmente los códigos de acceso.
b) Proceder a verificaciones regulares de los motivos de una consulta al SIS.

7. Designar a un responsable de la seguridad y definir normas de seguridad comunes a las diferentes Oficinas SIRENE, aplicables a su personal.

8. Organizar una gestión de la información impresa para restringir la obtención de impresiones de pantalla que contengan información de la base de datos SIRENE y de las descripciones SIS.

9. Fomentar la organización de cursos de formación para los usuarios de las Oficinas SIRENE centrados en la seguridad de la información.

10. Recomendar que los N.SIS y las Oficinas SIRENE elaboren informes de seguridad, a intervalos regulares, por ejemplo anualmente.

La futura evolución del sistema de comunicación de datos entre los Estados, concretamente en lo relativo a desarrollo del SIS, deberá hacerse necesariamente respetando las condiciones de seguridad, ya se opte por un modelo centralizado o por un modelo descentralizado.

Por último, la ACC subraya la cooperación de todas las instancias nacionales implicadas y se congratula de que esta operación de verificación emprendida de forma coordinada en todos los Estados haya contribuido a mejorar considerablemente la seguridad de la información. Esto constituye una condición indispensable para la confianza del ciudadano y de las instituciones democráticas en el funcionamiento del sistema Schengen.

3. RELACIÓN DE LOS DICTÁMENES DE LA ACC Y REACCIONES DE LOS ÓRGANOS EJECUTIVOS TÉCNICOS

	Contenido	Realizaciones	Comentarios
Control del C.SIS en marzo de 1994 y dictamen de 18.05.1994	- Velar por el transporte y la conservación de las copias de salvaguarda de los datos. - Reforzar la fiabilidad de los enlaces C.SIS – N.SIS - Instalar una separación física entre las instalaciones del C.SIS y las del Ministerio francés del Interior localizadas en el mismo edificio.	- La República Francesa adoptó las medidas que consideraba más apropiadas. - El 4 de marzo de 1998, durante una visita del Grupo Central y el Presidente de la ACC al C.SIS, se presentaron algunas obras de acondicionamiento del recinto.	Según la información de la ACC, estas obras no se realizaron.
Dictamen de 22 de febrero de 1995 sobre la base jurídica de las Oficinas SIRENE	Al no contener el Convenio base jurídica para las Oficinas SIRENE, resulta conveniente crear dicha base, ya sea modificando el Convenio, ya modificando las legislaciones nacionales de forma armonizada.	El 27 de junio de 1996, el Grupo Central consideró que existía base jurídica apropiada, que los Estados miembros resolverían la cuestión del método de trabajo, la estructura y el estatuto formal de estas oficinas, y que las autoridades nacionales garantizaban el control del funcionamiento del SIS y de las Oficinas SIRENE, así como la información a la ACC.	Quince meses después de tener conocimiento de este asunto, el Grupo Central refuta los argumentos de la ACC.
Visita de control al C.SIS en octubre de 1996 Recomendación nº 1:	Velar por que los ficheros de las Partes contratantes sean idénticos.	Crear un nuevo procedimiento de comparación de los datos que ya no ponga de manifiesto las diferencias detectadas por la ACC.	1998: se anuncia un nuevo procedimiento de comparación de datos.
Recomendación nº 2:	Encargar una certificación ITSEM/ITSEC del sistema informático y aplicar las medidas de seguridad recomendadas o, al menos, garantizar al mínimo el grado de seguridad previsto	- Resulta imposible efectuar a posteriori la certificación del actual sistema. Imposible activar las funciones de trazado. - Las especificaciones técnicas definidas en el marco del procedimiento de licitación para la renovación del C.SIS preverán que cada componente del nuevo sistema se ajuste obligatoriamente a los criterios ITSEC y a la norma 4-C2/E2. Se certificarán o se podrán certificar los sistemas a petición de los Estados Schengen.	El Grupo Central declara que no puede encargar la certificación del actual sistema. El futuro sistema podrá certificarse.
Recomendación nº 3:	Reducir el número de "superusuarios" del C.SIS, que disponen de un acceso privilegiado al sistema para acceder y modificar el contenido de cualquier fichero registrado en el sistema informático y borrar las huellas de esta acción.	- El personal empleado en el C.SIS es objeto de estrictos procedimientos de contratación y de control de seguridad - Se preverá en las especificaciones de los nuevos sistemas un reparto preciso de los diferentes cometidos de gestión, para que puedan atribuirse las funciones sobre la base de estos cometidos - Esta medida permitiría así la necesaria reducción del número de "superusuarios"	Se comunica a la ACC que, en el futuro se reducirá el número de superusuarios.
Recomendación nº 4:		Las especificaciones técnicas definidas en el marco del procedimiento de licitación para la renovación del C.SIS preverán que los licitadores indiquen los recursos suplementarios	

4. PRO MEMORIA

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 especiales (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 Convenio2.

Las instancias Schengen están asistidas por una secretaría, puesta a su disposición por el BENELUX, con sede en Bruselas.

En el anexo figura un organigrama.

OBJETIVO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN SCHENGEN (SIS)

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 particulares, 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).

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.

En 1998, todos los miembros de la ACC de los países que aplican el Convenio procedieron a la realización de controles de sus Oficinas SIRENE y transmitieron el informe respectivo a la Secretaría de la ACC (se trata de los informes SCH/Aut-cont (98) 9 de Francia, 13 y 40 de Bélgica, 15 de
Italia, 21 de Alemania, 28 de Grecia, 31 de Portugal, 33 de Países Bajos, 35 de España y 36 de Austria. Luxemburgo y Países Bajos también presentaron su informe sobre la seguridad de las Oficina SIRENE).

El nivel de seguridad de las Oficinas SIRENE nacionales no puede ser inferior al del SIS. Partiendo de estos principios, la ACC propone que se adopten las siguientes disposiciones en los Estados miembros en los que aún no sean de aplicación:

- Mantener la seguridad física al más alto nivel, actualizando las técnicas utilizadas. En los países donde se hayan constatado lagunas, aportar las modificaciones necesarias con la mayor brevedad e informar a la Autoridad de Control nacional.

- Cifrar las conexiones entre el SIRENE y el N.SIS y someter este cifrado al control de los miembros de las autoridades de control.
a) Crear un sistema de trazado de todas las operaciones posibles que se refieran a la base de datos del N.SIS y de la Oficina SIRENE.
b) Realizar una explotación regular de los ficheros de trazado para la detección de anomalías, en particular en cuanto al número de consultas.
-
Limitar y controlar el acceso a los archivos manuales de los expedientes.
- Cifrar la información recogida en soporte informático.
- Reforzar las medidas tendentes a garantizar que el acceso esté efectivamente limitado a los datos para los cuales los operadores disponen de autorización, concretamente, en particular verificando regularmente sus autorizaciones de acceso y cambiando regularmente los códigos de acceso.

- Proceder a verificaciones regulares de los motivos de una consulta al SIS.

- Designar a un responsable de la seguridad y definir normas de seguridad comunes a las diferentes Oficinas SIRENE, aplicables a su personal.
- Organizar una gestión de la información impresa para restringir la obtención de impresiones de pantalla que contengan información de la base de datos SIRENE y de las descripciones SIS.
- Fomentar la organización de cursos de formación para los usuarios de las Oficinas SIRENE centrados en la seguridad de la información.
- Recomendar que los N.SIS y las Oficinas SIRENE elaboren informes de seguridad, a intervalos regulares, por ejemplo anualmente.

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 duplica-

ciones 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

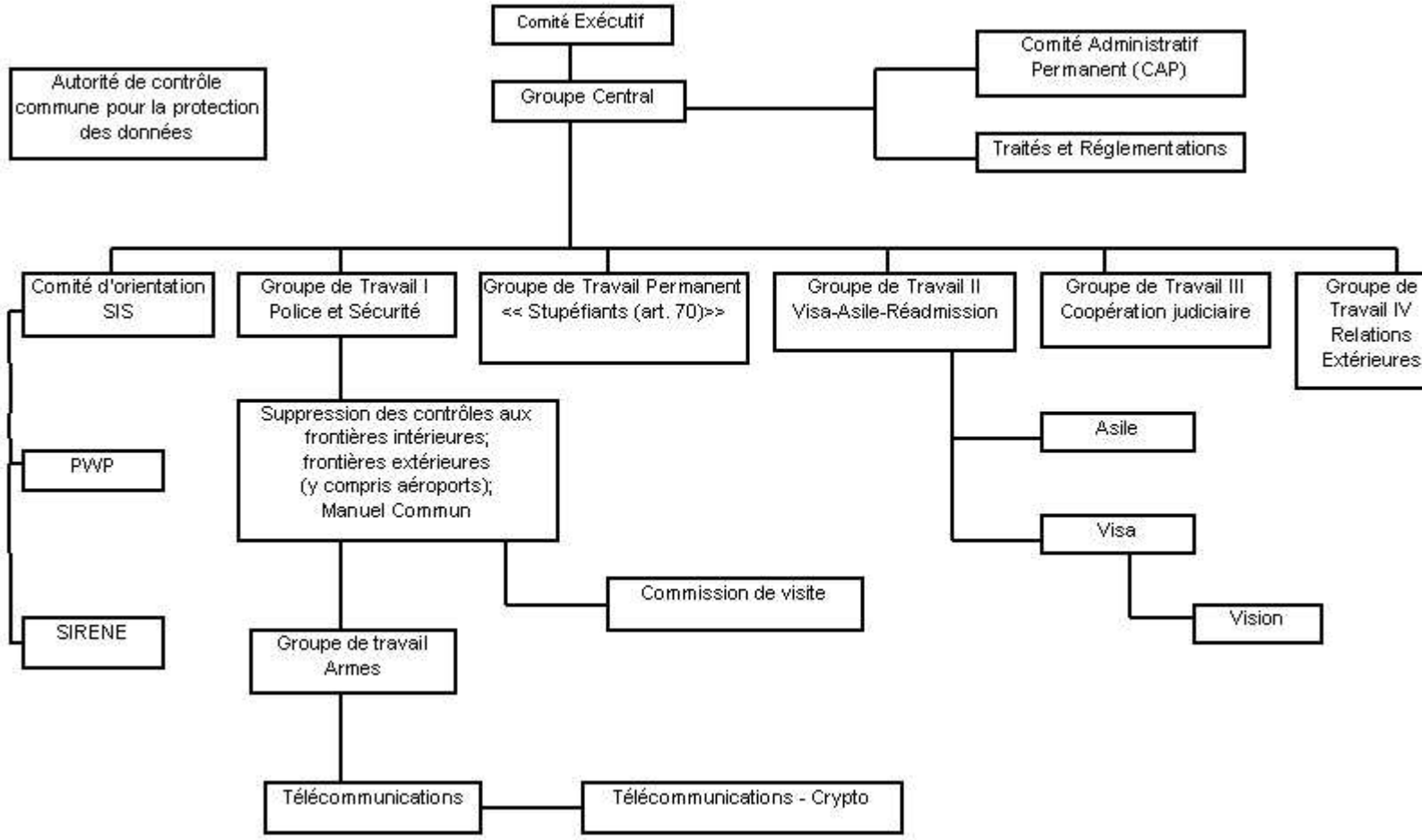
El Título VI (Artículo 126 y siguientes) del Convenio, titulado "protección de datos de carácter personal", se dedica a las normas aplicables a los intercambios de informaciones que no se hayan de introducir en el SIS pero que intervienen para la aplicación del Convenio (ver punto 2.1. b y c).

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.

5. ORGANIGRAMA DE LOS GRUPOS DE TRABAJO SCHENGEN



6. DECLARACIÓN DE LA ACC CON MOTIVO DEL 50 ANIVERSARIO DE LA DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS

Con ocasión del 50 aniversario de la Declaración Universal de los Derechos Humanos, celebrado este 10 de diciembre de 1998, la Autoridad de Control Común de Schengen reunida en Bruselas el 11 de diciembre expresa su compromiso con la defensa de los derechos de los ciudadanos en relación con el Sistema de Información de Schengen, afirmando así concretamente los grandes valores de libertad y derechos humanos consagrados en la Declaración universal.

7. LISTA DE LOS DICTÁMENES, DECISIONES Y RECOMENDACIONES CON MIRAS A LA INTEGRACIÓN EN LA UNIÓN EUROPEA

Lista de decisiones, recomendaciones, dictámenes e informes de la Autoridad de Control Común de Schengen con vistas a la integración del acervo de Schengen, de acuerdo con el Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea, previsto en el Tratado de Amsterdam.

Documento	Asunto	Referencia
Reglamento Interior	El Reglamento asegura la independencia de la ACC, establece la composición y el modo de elección de la Presidencia, define las normas de funcionamiento y la forma de ejercer sus misiones.	SCH/Aut-cont (95) 25, 6ª rev.
Línea presupuestaria autónoma	Línea autónoma de la ACC, a propuesta de esta última, garantizada en el presupuesto global de Schengen.	SCH/Com-ex (97) PV 1 rev. (reunión de los Ministros del 25 de abril de 1997); SCH/Com-ex (97) 1 (decisión del Comité Ejecutivo de 25 de abril de 1997); SCH/Com-ex (98) 9 (proyecto de decisión de los Ministros de 21 de abril de 1998)
Presupuestos de la ACC 1997 y 1998	Definen los importes y los criterios de distribución adecuados a las misiones.	SCH/Aut-cont (96) 4ª rev. + SCH/Aut-cont (98) budget 1
Decisión de la ACC relativa a las leyes de protección de datos de Grecia	Declaración de la ACC sobre la entrada en vigor de las leyes de protección de datos de carácter personal en Grecia.	SCH/Aut-cont (97) PV 3 (reunión ACC del 27 de marzo de 1997) y SCH/Aut-cont (97) L 5.
Decisiones de la ACC relativas a las leyes de protección de datos de Italia	Declaración de la ACC sobre la entrada en vigor de las leyes de protección de datos de carácter personal en Italia.	SCH/Aut-cont (97) PV 7 (reunión ACC del 4 de julio de 1997) y SCH/Aut-cont (97) 35.
Lista de autoridades habilitadas a consultar directamente el SIS	Art. 101.4 del Convenio de Aplicación. Decisión de la ACCP.	SCH/Aut-cont (95) PV 1 (reunión de la ACCP del 22 de febrero de 1995).
Recomendaciones de la ACC sobre el C.SIS	Recomendaciones relativas a la seguridad del C.SIS y a la fiabilidad de las transmisiones entre los N.SIS y el sistema central.	SCH/Aut-cont (94) dec. 1 (18 de mayo de 1994).
Dictamen sobre el ejercicio del derecho de acceso y principios de cooperación en la verificación de datos	Definición de los principios de la cooperación entre las autoridades nacionales de control con ocasión del ejercicio de los derechos de acceso y verificación.	SCH/Aut-cont (96) 16, 2ª rev.
Recomendaciones de la ACC sobre el funcionamiento del Sistema de Información	Recomendaciones sobre la seguridad del SIS recogidas en el informe confidencial de 27 de marzo de 1997, y de las que se reproducen algunos pasajes en el informe de actividades 1995/1997.	SCH/Aut-cont (96) 40, 2ª rev. (diciembre de 1996, versión final del 27 de marzo de 1997) (CONFIDENCIAL).SCH/Aut-cont (97) 27, 2ª rev. (Informe de actividades 1995/1997, del 17 de marzo de 1997, páginas 24 a 28).
Dictamen sobre el proyecto piloto relativo a los vehículos robados	Principios que deben respetarse en materia de intercambio de información del SIS en operaciones entre Estados Schengen con respecto a aquéllos que aún no apliquen el Convenio.	Dictamen de 7 de marzo de 1997 (SCH/Aut-cont (96) 22 rev.).
Dictamen sobre el Convenio de cooperación en los procedimientos por	Enumeración de las menciones relativas a la protección de los datos que	

Observación: el informe del 27 de marzo de 1997 sobre el control del C.SIS contiene recomendaciones sobre la seguridad del SIS, así como la reacción del Ministerio del Interior francés a algunas de ellas (SCH/Aut-cont (96) 40, 2ª rev.).
Tanto la ACC como el Grupo Central han considerado este documento **confidencial**. Por tanto, la ACC lo ha entregado al Presidente del Comité Ejecutivo y a los miembros del Grupo Central, que lo han remitido a sus correspondientes expertos.
En las páginas 24 - 28 del Informe de actividades 1995/1997 (SCH/Aut-cont (97) 27, 2ª rev.) figuran algunos extractos de dicho informe

8. REGLAMENTO DE LA ACC

aprobado por la ACC el 2 de febrero de 1996
modificado en su artículo 2 por decisión de la ACC en su reunión de 4.7.97
modificado el 27 de abril de 1998 con la adición de un nuevo artículo 11

La Autoridad de Control común

Visto el artículo 115 del Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes, firmado el 19 de junio de 1990, en adelante denominado "el Convenio".

adopta, el 19 de octubre de 1995, el siguiente Reglamento interior.

Artículo 1 - Misiones

1. La ACC cumplirá, de conformidad con el presente Reglamento interior, aquellas misiones que el Convenio le encomiende , así como aquellas misiones relativas a la protección de datos de carácter personal que considere relacionadas con la aplicación del Convenio.

2. En el ejercicio de sus misiones, la Autoridad de Control común podrá intervenir o bien de oficio o bien a petición de una Autoridad de Control nacional de un Estado Schengen, de una Parte contratante o de una instancia del Sistema Schengen, de conformidad con las disposiciones del Convenio.

Artículo 2 - Composición.

1. La Autoridad de Control Común, de conformidad con lo dispuesto en el artículo 115 del Convenio, estará compuesta por dos representantes de la Autoridad de Control nacional, según lo previsto en el artículo 114 del Convenio, de cada Parte contratante en la que el Convenio haya entrado en vigor de conformidad con el artículo 140 del mismo. Por Parte contratante se entiende asimismo aquella Parte que haya concluido con los Estados Parte en el Acuerdo y en el Convenio de Schengen, un Acuerdo de cooperación relativo a la supresión de los controles de personas en las fronteras comunes, siempre y cuando el Acuerdo de cooperación esté en vigor.
Cada delegación dispondrá de un voto.

2. La Autoridad de Control Común, por decisión unánime de sus miembros, podrá conceder el estatuto de observador con voz pero sin voto, a los representantes de las autoridades nacionales de control contempladas en el artículo 114 del Convenio, o expertos independientes de una Parte contratante que aún no cumpla las condiciones de la última frase del apartado 2 del artículo 140. Por Parte contratante se entiende asimismo aquella Parte que haya concluido con los Estados Parte en el Acuerdo y en el Convenio de Schengen, un Acuerdo de cooperación sobre la supresión de los controles en las fronteras comunes, siempre y cuando dicho Acuerdo haya sido ratificado, aprobado o aceptado por todas las Partes contratantes, aunque aún no haya entrado en vigor.

3. Los miembros de la Autoridad de Control Común, así como los observadores, no podrán ser miembros de un Grupo de Trabajo o de otra Autoridad -distinta de la Autoridad de Control nacional para la protección de datos de carácter personal- instituidos en virtud del Convenio. No obstante, podrán acompañar como expertos a sus delegaciones nacionales.

1. Cuando un miembro de la Autoridad de Control común no pueda asistir a una reunión, podrá ser sustituido por una persona designada por la Autoridad de Control nacional de conformidad con el presente artículo.

5. Cada miembro de la Autoridad de Control común podrá verse acompañado de un experto que le asista.

Artículo 3 - Presidencia

1. La Autoridad de Control Común elegirá a su Presidente y a su Vicepresidente de entre sus miembros por mayoría de dos tercios de las Delegaciones contempladas en el primer apartado del artículo 2. Sus mandatos tendrán una duración de un año, renovable una vez.

2. El Vicepresidente será miembro de una Delegación distinta a la del Presidente; sustituirá al Presidente en caso de ausencia o impedimento de éste.

3. Si se produce una vacante antes de la expiración del mandato del Presidente o del Vicepresidente, se procederá a su sustitución. El miembro elegido como suplente ejercerá sus funciones durante el período de mandato restante.

Artículo 4 - Función del Presidente

1. El Presidente representa a la Autoridad de Control común. Velará por su correcto funcionamiento. Convocará a la Autoridad de Control común y fijará el lugar, el día y la hora de las reuniones. Abrirá y cerrará las reuniones. Dirigirá los debates. Elaborará el orden del día provisional.

2. Con vistas a preparar las deliberaciones de la Autoridad de Control común, el Presidente podrá designar a uno o varios ponentes de entre sus miembros, para un tema determinado.

Artículo 5 - Funcionamiento

1. La Autoridad de Control común se reunirá al menos dos veces al año. Se reunirá asimismo por iniciativa del Presidente, y siempre que al menos tres delegaciones de las contempladas en el primer apartado del artículo 2 formulen una petición motivada en este sentido, verbalmente durante una reunión o por escrito. Finalmente, se reunirá en los casos previstos por el Convenio.

2. Salvo en los casos que el Presidente considere urgentes, las convocatorias se transmitirán al menos catorce días antes de la fecha de la reunión. La convocatoria incluirá el orden del día provisional y, en la medida de lo posible, los documentos necesarios para el debate.

3. La Autoridad de Control común adoptará el orden del día definitivo al principio de cada reunión.

Artículo 6 - Quórum y normas de mayoría

1. Las reuniones de la Autoridad de Control común sólo tendrán validez cuando al menos dos tercios de las delegaciones contempladas en el primer apartado del artículo 2 estén presentes.

2. Sin perjuicio de lo dispuesto en el artículo 13, se adoptarán los actos de la Autoridad de Control común cuando la mitad más una de las delegaciones presentes contempladas en el primer apartado del artículo 2 se manifiesten a favor.

3. Cada delegación podrá presentar una nota de explicación de voto.

4. La Autoridad de Control común deliberará en base a documentos y proyectos redactados en las lenguas nacionales de todos los Estados Schengen.

Artículo 7 - Publicidad y destinatarios de los actos

1. Salvo decisión contraria de la Autoridad de Control común, las reuniones de esta no serán públicas

2. La Autoridad de Control común determinará los destinatarios de sus actos y se pronunciará sobre la eventual publicidad de estos, sin perjuicio de lo dispuesto en el apartado 4 del artículo 115 del Convenio .

Artículo 8 - Procedimiento escrito

1. Los actos de la Autoridad de Control común podrán adoptarse mediante procedimiento escrito, siempre que todas las delegaciones acepten este principio durante una reunión.

2. En caso de urgencia, el Presidente podrá recurrir de oficio al procedimiento escrito.

3. En ambos casos, el Presidente transmitirá un proyecto a todos los miembros de la Autoridad de Control común. Se considerará que las delegaciones que no hayan presentado objeciones en un plazo, que deberá determinar el Presidente, de al menos catorce días a partir de la fecha de recepción del proyecto, aceptan dicho proyecto.

4. Se pondrá fin al procedimiento escrito en el caso previsto en el segundo apartado del presente artículo, cuando una Delegación solicite, en un plazo de cinco días hábiles a partir de la fecha de recepción del proyecto, que este sea objeto de debate en el seno de la Autoridad de Control común.

Artículo 9 - Grupos de trabajo, expertos, verificaciones in situ

1. La Autoridad de Control común podrá instituir grupos de trabajo cuya misión definirá

2. La Autoridad de Control común podrá recurrir a expertos. Podrá elaborar una lista de expertos a los que recurrir con

prioridad.

3. En relación con el control de la función de apoyo técnico, la Autoridad de Control común podrá designar a uno o varios de sus miembros para proceder a verificaciones in situ. Si lo considerara urgente, el Presidente podrá proceder de oficio a dicha designación. En tal caso, informará inmediatamente a los miembros de la Autoridad de Control común. Los miembros encargados de efectuar las verificaciones podrán verse asistidos de los expertos inscritos en la mencionada lista.

4. Los Grupos de trabajo, los expertos y los miembros de la Autoridad encargados de proceder a verificaciones rendirán cuentas de los resultados de sus misiones a la Autoridad de Control común.

Artículo 10 - Secretaría

1. Asumirán la Secretaría de la Autoridad de Control común, bajo responsabilidad de su Presidente, las personas y servicios puestos a disposición por la Autoridad competente de la cooperación Schengen.

2. La Secretaría llevará un registro de actos adoptados por la Autoridad de Control común.
3. El correo destinado a la Autoridad de Control común se dirigirá a la Secretaría, a la atención del Presidente.

Artículo 11 - Presupuesto de la Autoridad de Control Común

La Autoridad de Control Común dispondrá de un presupuesto, inscrito como línea presupuestaria autónoma en el presupuesto Schengen, para poder ejecutar su programa de trabajo anual en el marco de las misiones que le encomienda el Convenio.

Artículo 12 - Actas

1. Se elaborará un acta de cada reunión de la Autoridad de Control común.

2. La Secretaría redactará el proyecto de acta, bajo responsabilidad del Presidente. Este acta se someterá a la aprobación de la Autoridad de Control común en la siguiente reunión.

3. Los miembros y observadores podrán rectificar el acta ulteriormente en función de las observaciones que formularan en la reunión en cuestión.

Artículo 13 - Confidencialidad

Sin perjuicio de la aplicación del segundo apartado del artículo 7, los miembros de la Autoridad de Control común, los observadores, los expertos y los miembros de la Secretaría deberán respetar la confidencialidad. Esta obligación no se aplicará ni ante las Autoridades de control nacionales, ni ante las demás autoridades a quienes presenten sus informes, de conformidad con el Derecho nacional, los miembros y observadores.

Artículo 14 - Modificación del Reglamento

La Autoridad de Control común adoptará, por unanimidad, las disposiciones destinadas a modificar el presente Reglamento. Salvo disposición en sentido contrario, estas entrarán en vigor una semana después de su adopción.

9. PRINCIPIOS GENERALES EN LAS VISITAS DE CONTROL DE LA ACC AL C.SIS

Los presentes principios pretenden clarificar las modalidades de visita y de control al emplazamiento del C.SIS en Estrasburgo por parte de la Autoridad de Control Común (ACC).
Dichas visitas se inscriben en el marco de las misiones que se desprenden del artículo 115 del Convenio de Aplicación del Acuerdo de Schengen.

1) Tipología de las visitas

Cabe diferenciar dos tipos de visita:

- la visita de información que, por lo general, incluye la visita a los edificios, la presentación general del SIS y la actividad del C.SIS, sin consulta propiamente dicha a la base de datos.
  Podrá efectuarla la ACC en su composición plenaria;

- la visita de control cuyo objeto es comprobar la correcta ejecución de las disposiciones del Convenio de Aplicación; en principio la efectuará un grupo restringido especialmente mandatado por la ACC para esta misión.

- El cometido de este grupo de control será verificar la integridad, calidad, continuidad, exclusividad y confidencialidad del C.SIS en el marco del Convenio.

2) Información al Ministerio del Interior

La ACC informará al Ministerio del Interior (Dirección General de la Policía Nacional, Servicio de libertades públicas y asuntos jurídicos, Departamento de transmisiones e informática) de que va a acudir al C.SIS en Estrasburgo.
La ACC precisará la naturaleza de la visita, su objetivo, la lengua de trabajo y los medios previstos para solucionar los problemas de tipo lingüístico, la fecha prevista y la composición del grupo de visita.

3) Composición del grupo de visita

La ACC determinará la composición del grupo de visita o de control, que podrá incluir tres categorías de personas:
- los miembros de la ACC y la Secretaría General,
- los miembros y agentes de las autoridades nacionales de control para la protección de datos,
- los expertos externos.

Se elaborará una lista de todas estas personas y se transmitirá al Ministerio del Interior. En las visitas de control pueden participar únicamente los miembros efectivos de la ACC, la Secretaría General y las personas habilitadas y mandatadas por la ACC.
En caso de recurrir a expertos no incluidos en la lista de expertos prevista por el artículo 9 del Reglamento interior de la ACC, ésta informará de ello al Ministerio del Interior con un mes de antelación.

4) Desarrollo de la visita de control

Al inicio de la visita de control se comunicará a los responsables del centro el programa de trabajo previamente definido por la ACC para que dichos responsables puedan adoptar las disposiciones útiles para responder a las solicitudes formuladas por la ACC.

5) Consulta del sistema informático

La persona encargada de la gestión del C.SIS dispondrá todos los medios necesarios para satisfacer en tiempo real las peticiones de consulta del sistema informático formuladas por la Autoridad de Control Común. Se ocupará, en particular, de poner a disposición de la ACC un técnico encargado de proceder a las operaciones manuales necesarias para responder a las peticiones antes mencionadas.

6) El acceso a los documentos

La ACC tiene acceso a todos los documentos referentes al C.SIS, de utilidad para su misión.
La ACC respetará el carácter confidencial de los documentos.
Los documentos clasificados "secreto defensa" no pueden salir del recinto del C.SIS, si bien la ACC tiene acceso a los mismos.
La entrega de copias de documentos está sujeta a la firma de un recibo.

7) Los informes técnicos

En la medida en que pueden revelar aspectos operativos del sistema, los informes técnicos son y serán siempre confi - denciales.

Estos informes se transmitirán a los responsables del C.SIS para posibles observaciones, antes de su transmisión a las autoridades Schengen.

10. LISTA DE LOS MIEMBROS DE LA ACC

Belgique

M. B. DE SCHUTTER
Commissie voor de bescherming van de persoonlijke levenssfeer
C/o Vrije Universiteit Brussel
Pleinlaan 2 - 1050 Brussel
Tel : 00 32 2 629 26 31
Fax : 00 32 2 629 26 62

Mme B. HAVELANGE
Commission de la protection de la vie privée
Bld de Waterloo 115 - 1000 Bruxelles
Tel : 00 32 2 542 72 00
Fax : 00 32 2 542 72 12

Pays-Bas

MM. P.J. HUSTINX & P.A. MICHAEL
Registratiekamer
Prins Clauslaan 20
Postbus 93374
25090 AJ's-Gravenhage
Tel : 00 31 70 381 13 00
Fax : 00 31 70 381 13 01

España

M. Juan Manuel Fernandez LÓPEZ
M. Miguel Angel López HERRERO
Agencia de Protección de Datos
Paseo de la Castellana, 41
28046 Madrid
Tel : 00 34 91 308 39 68/308 47 02
Fax : 00 34 91 308 46 92

Allemagne

M. J. JACOB, commissaire fédéral à la protection des données
Représenté par :
M. W. von POMMER ESCHE
Chef du département auprès du commissaire fédéral à la protection des données
Riemenschneiderstraße, 11
Tel : 00 49 228 81 99 50
Fax : 00 49 228 81 99 550

M. R. HAMM, commissaire du Land de Hesse à la protection des données
Représenté par :
Mme A. SCHRIEVER-STEINBERG
Uhlandstr. 4
65189 Wiesbaden
Tel : 00 49 611 1408 0
Fax : 00 49 611 37 85 79

France

M. A. TÜRK et Mme F. FOURETS
Suppléant M. O. COUTOR
CNIL
Rue Saint Guillaume, 21
75340 Paris Cedex 07
Tel : 00 33 1 53 73 22 22
Fax : 00 33 1 53 73 22 00

Portugal

M. J.A.M. LABESCAT da SILVA
M. Nuno Albuquerque MORAIS SARMENTO
Rua de S. Bento 148 3° Andar
1200 Lisbonne
Tel : 00 351 1 392 84 00
Fax : 00 351 1 397 68 32

Luxembourg

M. R. FABER et M. J.P. REITER, représentants effectifs

M. J. WAGNER et M. G. WIVENES, représentants suppléants
Secrétariat de l'Autorité de contrôle " Police "
Ministère de la Justice
L-2934 Luxembourg
Tel : 00 352 478 45 62
Fax : 00 352 227 661

Autriche

Mme W. KOTSCHY
Mme E. SOUHRADA-KIRCHMAYER
Ballausplatz 1
A - 1014 Wien
Österreich
Tel : 00 43 1 531 15/2525
Fax : 00 43 1 53 115/2690

Italie

M. S. Neri
Tel : 00 390 667 60 46 93
Fax : 00 390 95 62 12 20
Fax : 00 390 6 676 096 78

M. BUTTARELLI
Garante per la protezione dei dati personali
Secretary general
Largo del Teatro Valle, 6
00186 Roma
Tel : 00 39 06 68 18 61
Fax : 00 39 06 68 18 669

Grèce

M. C. DAFERMOS
Suppléant M. G. DELYANNIS - D. KRINTZALIS
Autorité de protection des données à caractère personnel
Av. Omirou 8
Athenes 11 527
Tel : 00 301 33 52 604/5
Fax : 00 301 33 52 617

Islande : en tant qu'observateur

Ms. S. JÖHANNESDOTTIR
Mr. T. ÖRLYGSSON
Data protection Commission
Ministry of Justice
Armarhvoll
150 Reykjavik
Islance
Tel : 00 354 560 90 10
Gax : 00 354 552 73 40

Danemark : en tant qu'observateur

Ms. Lotte N. JØRGENSEN
Registertilsynet
Christians Brygge 28 - 1553 KØBENHAVN V
Danemark
Tel : 00 45 33 14 38 44
Fax : 00 45 33 13 38 43

Suède : en tant qu'observateur

M.Ulf WIDEBÄCK
General-Director
Ms. B.M. WESTER

Supervisory Director
Datainspektionen
Box 8114
S - 104 20 Stockholm
Sweden
Tel : 00 46 8 657 61 00
Fax : 00 46 8 650 86 13

Norvège : en tant qu'observateur

M. G. APENES & Mme G. SLETTEMARK
Datatilsynet
Postboks 8177 Dep. 00 34 Oslo
Tel : 00 47 22 39 69 00
Fax : 00 47 22 42 23 50

Finlande : en tant qu'observateur

Mr. AARNIO - Head of Finnish delegation
Ms. M. KLEEMOLA
Office of the Data Protection Ombudsman
PL 315 Finland 00 181 Helsinki
Tel : 00 358 9 18 251
Fax : 00 358 9 18 25 7835

11. DATOS INTRODUCIDOS EN EL SIS

DATOS INTRODUCIDOS EN EL SISTEMA DE INFORMACIÓN SCHENGEN (05MAR.99)

REGISTROS ACTUALIZADOS	AUSTRIA	BÉLGICA	ALEMANIA	ESPAÑA	FRANCIA	GRECIA	ITALIA	LUXEMBURGO	PAÍSES BAJOS	PORTUGAL	TOTAL
BILLETES BANCO (BK)	47	0	210.841	0	534.310	0	77.147	246	658	87	823.336
DOC. VÍRGENES (DB)	58	1.242	58.888	9.366	7.362	81	4.940	5	166	96	82.204
ARMAS (FA)	913	993	118.030	16.000	57.584	8.329	0	683	674	10.219	213.425
DOC.IDENTIDAD (IC)	53.961	1.565	1.531.072	11.306	1.583.359	749	1.668.496	3.109	435.691	4.498	5.293.806
VEHÍCULOS (VE)	8.500	31.524	233.897	121.523	232.820	37.289	448.852	1.737	41.315	17.573	1.175.030
PERSONAS (WP)	30.276	4.852	726.205	22.574	166.403	48.305	227.812	730	9.879	2.019	1.239.055
TOTAL	**93.755**	**40.176**	**2.878.933**	**180.769**	**2.581.838**	**94.753**	**2.427.247**	**6.510**	**488.383**	**34.492**	**8.826.856**

DATOS INTRODUCIDOS EN EL SISTEMA DE INFORMACIÓN SCHENGEN (05MAR.99)

REGISTROS ACTUALIZADOS	TOTAL
BILLETES DE BANCO (BK)	823.336
DOCUMENTOS VÍRGENES (DB)	82.204
ARMAS (FA)	213.425
DOCUMENTOS DE IDENTIDAD (ID)	5.293.806
VEHÍCULOS (VE)	1.175.030
PERSONAS BUSCADAS (WP)	1.239.055
TOTAL	**8.826.856**

12. ÍNDICE CRONOLÓGICO

1985

El acuerdo de Schengen fue firmado el 14 de junio de 1985 por los gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa. Se aplicó a título provisional al día siguiente de su firma y entró en vigor el 2 de marzo de 1986.

1990

Las mismas Partes contratantes firmaron el 19 de junio de 1990 el Convenio de Aplicación del Acuerdo de Schengen, en el que se desarrolla la cooperación policial, aduanera y judicial a los fines del control en las fronteras exteriores comunes.

Una de las medidas fundamentales de este dispositivo de cooperación fue la creación de un sistema informático común, el Sistema de Información de Schengen (Título IV del Convenio).

La puesta en aplicación de este sistema exigió la constitución de una autoridad de control común, inspirada en los modelos nacionales de autoridades de control independientes competentes en este ámbito.

1992

Fue instituida una Autoridad de Control Común Provisional - ACCP. Esta autoridad, presidida por el Sr. Faber (Luxemburgo), estaba compuesta por uno o dos representantes de las autoridades nacionales de control de los cinco Estados fundadores de los Acuerdos, y por uno o dos expertos independientes nombrados por los Estados signatarios en cuyo territorio el Convenio todavía no estaba en aplicación.

Entre el 29 de junio de 1992 y el 22 de febrero de 1995, la ACCP celebró doce reuniones en Bruselas.

1993

Portugal y España ratificaron el Acuerdo y el Convenio de Aplicación de Schengen.

1994

La Autoridad de Control Común Provisional realizó la primera visita al sistema central, en Estrasburgo.

Se elaboró un cuestionario sobre la naturaleza de las normas de protección de datos aplicables en cada uno de los Estados Schengen.

Se eligió presidente al Sr. Pommer Esche (Alemania), jefe de departamento al servicio del Delegado Federal para la Protección de Datos.

1995

El Convenio entró en aplicación (26 de marzo) en siete Estados: Alemania, Bélgica, España, Francia, Luxemburgo, Países Bajos y Portugal. En la misma fecha quedó constituida la Autoridad de Control Común. EL Sistema de Información Schengen entró en funcionamiento.

Entre el 17 de mayo y el 14 de diciembre del mismo año, la ACC celebró cinco reuniones, bajo la presidencia del Sr. Von Pommer Esche.

El 14 de diciembre, la ACC eligió presidente al Sr. Turk (Francia), senador y miembro de la Comisión Nacional de la Informática y las Libertades, y como vicepresidente al Sr. J. Labescat (Portugal), abogado y miembro de la Comisión Nacional de Protección de Datos.

1996

El 2 de febrero se aprobó el Reglamento interior de la Autoridad de Control Común.

El 19 de diciembre, Dinamarca, Finlandia y Suecia firmaron el Acuerdo de Adhesión al Convenio de Schengen. Islandia y Noruega concluyeron un Acuerdo de Cooperación que prevé la aplicación del Convenio en su territorio

La ACC se reunió en nueve ocasiones a lo largo de ese año. Representantes independientes de Austria, Italia y Grecia participan en los trabajos de la ACC con el estatuto de observadores.

La ACC aprobó los principios de cooperación entre las autoridades nacionales de control por lo que respecta al ejercicio del derecho de acceso.

1997

La ACC se reunió diez veces entre marzo de 1997 y marzo de 1998. A excepción de su reunión anual, celebrada en Lisboa en abril de 1997, todas las reuniones tuvieron lugar en Bruselas.

Además de las reuniones plenarias, la ACC celebró cinco reuniones en comité restringido. También tuvieron lugar encuentros entre algunos de sus miembros y representantes del Ministerio del Interior francés.

La ACC vio reconocido su relevante papel por las instancias ejecutivas de Schengen. Se le garantizó un presupuesto a través de una línea presupuestaria autónoma, y pasó a recibir con mayor regularidad la información indispensable para el ejercicio de sus misiones.

El 11 de febrero de 1997 se llevó a cabo un control del sistema central. A raíz del mismo, la ACC elaboró un informe en el que realizaba un conjunto de recomendaciones sobre el funcionamiento del sistema.

La ACC formuló dictámenes sobre el proyecto piloto sobre vehículos robados, sobre el Convenio de cooperación en los procedimientos por infracción a la legislación de tráfico y en la ejecución de las sanciones pecuniarias impuestas, y sobre la duplicación de una parte de las descripciones del SIS.

La ACC aprobó su primer informe de actividades (marzo de 1995 - marzo de 1997), presentándolo públicamente en una conferencia de prensa que tuvo lugar en Lisboa en el mes de abril.

A finales de 1997, el número de Estados miembros que aplican el Convenio aumentó a diez: Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos y Portugal. Los representantes de las autoridades nacionales de protección de datos de los Estados nórdicos (Dinamarca, Finlandia, Islandia, Noruega y Suecia) participan en los trabajos de la ACC en calidad de observadores.

Los Sres. J. Labescat y M. B. De Schutter fueron elegidos presidente y vicepresidente de la ACC, respectivamente.

1998

La ACC formuló dictámenes sobre la conservación de expedientes tras la supresión de una descripción, sobre la usurpación de identidad y sus consecuencias a nivel del SIS para el titular legítimo de la identidad usurpada, sobre la transmisión de datos relativos a vehículos robados (del SIS al banco de datos de la Interpol), sobre el control de la admisibilidad de la consulta al SIS, y sobre el acceso a datos del SIS por parte de los servicios encargados del registro de vehículos.

La ACC llevó a cabo, por primera vez, un control global en todas las Oficinas Sirene, realizando un conjunto de recomendaciones con vistas al refuerzo de la seguridad.

Hizo un seguimiento de los trabajos de desarrollo del SIS (+) y de los estudios preliminares del SIS II.

Definió el acervo comunitario con vistas a la integración de Schengen en la Unión Europea.

Impulsó la realización, en Lisboa, del primer coloquio sobre "Los derechos de los ciudadanos frente a los sistemas de información policial", así como una conferencia de prensa.

Lanzó la campaña "El Sistema de Información Schengen le interesa", haciendo distribuir, en particular en las áreas de entrada al espacio Schengen (aeropuertos, fronteras marítimas, etc.), un cartel y folletos informativos sobre los derechos de los ciudadanos.

El Presidente de la ACC participó por primera vez en una reunión del Comité Ejecutivo y estuvo presente en un encuentro del Grupo Central desarrollado en Estrasburgo.

13. PROTOCOLO DEL TRATADO DE AMSTERDAM RELATIVO A SCHENGEN

LAS ALTAS PARTES CONTRATANTES,

TOMANDO NOTA de que los acuerdos relativos a la supresión gradual de los controles en las fronteras comunes, firmados en Schengen por determinados Estados miembros de la Unión Europea el 14 de junio de 1985 y el 19 de junio de 1990, así como los acuerdos relacionados y las normas adoptadas en virtud de los mismos, tienen como finalidad potenciar la integración europea y hacer posible, en particular, que la Unión Europea se convierta con más rapidez en un espacio de libertad, seguridad y justicia,

DESEANDO incorporar dichos acuerdos y normas al marco de la Unión Europea,

CONFIRMANDO que lo dispuesto en el acervo de Schengen sólo puede aplicarse en la medida en que sea compatible con el derecho de la Comunidad y de la Unión,

TENIENDO EN CUENTA la posición especial de Dinamarca,

TENIENDO EN CUENTA que Irlanda y el Reino Unido de Gran Bretaña e Irlanda del Norte no son partes contratantes de los citados acuerdos ni los han firmado; que, no obstante, debería preverse la posibilidad de que dichos Estados miembros acepten algunas o todas las disposiciones de los mismos,

RECONOCIENDO que, en consecuencia, es necesario acogerse a lo dispuesto en el Tratado de la Unión Europea y en el Tratado constitutivo de la Comunidad Europea en lo que se refiere a una cooperación reforzada entre determinados Estados miembros y que dichas disposiciones deberían utilizarse únicamente como último recurso,

TENIENDO EN CUENTA la necesidad de mantener una relación especial con la República de Islandia y con el Reino de Noruega, Estados que han confirmado su intención de suscribir las disposiciones mencionadas, con arreglo al Acuerdo firmado en Luxemburgo el 19 de diciembre de 1996,

HAN CONVENIDO en las siguientes disposiciones, que se incorporarán como anexo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea:

ARTÍCULO 1

El Reino de Bélgica, el Reino de Dinamarca, la República Federal de Alemania, la República Helénica, el Reino de España, la República Francesa, la República Italiana, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos, la República de Austria, la República Portuguesa, la República de Finlandia y el Reino de Suecia, signatarios de los acuerdos de Schengen, quedan autorizados a establecer entre sí una cooperación reforzada en el ámbito de aplicación de dichos acuerdos y disposiciones relacionadas, recogidos en el anexo del presente Protocolo y denominados en lo sucesivo "acervo de Schengen". Esta cooperación se llevará a cabo en el marco institucional y jurídico de la Unión Europea y respetando las disposiciones pertinentes del Tratado de la Unión Europea y del Tratado constitutivo de la Comunidad Europea.

ARTÍCULO 2

1. A partir de la fecha de la entrada en vigor del Tratado de Amsterdam, el acervo de Schengen, incluidas las decisiones que haya adoptado hasta la fecha el Comité Ejecutivo creado por los acuerdos de Schengen, será inmediatamente aplicable a los trece Estados miembros a que se refiere el artículo 1, sin perjuicio de lo dispuesto en el apartado 2 del presente artículo. A partir de la misma fecha, el Consejo sustituirá a dicho Comité Ejecutivo.

El Consejo adoptará, por unanimidad de los miembros a que se refiere el artículo 1, cualquier medida que resulte necesaria para la ejecución del presente apartado. El Consejo determinará, por unanimidad y conforme a las disposiciones pertinentes de los Tratados, la base jurídica de cada una de las disposiciones o decisiones que constituyan el acervo Schengen.

Con respecto a dichas disposiciones y decisiones y de acuerdo con la mencionada determinación, el Tribunal de Justicia de las Comunidades Europeas ejercerá las competencias que le otorgan las disposiciones aplicables pertinentes de los Tratados. En todo caso, el Tribunal de Justicia no tendrá competencia alguna sobre las medidas o decisiones relativas al mantenimiento de la ley y el orden público así como a la salvaguarda de la seguridad interior.

En tanto no se adopten las medidas mencionadas y sin perjuicio de lo dispuesto en el apartado 2 del artículo 5, las disposiciones o decisiones que integran el acervo de Schengen se considerarán actos basados en el título VI del Tratado de la Unión Europea.

2. Lo dispuesto en el apartado 1 será aplicable a los Estados miembros que hayan firmado Protocolos de adhesión a los acuerdos de Schengen a partir de las fechas que el Consejo decida por unanimidad de los miembros a que se refiere el artículo 1, a menos que los requisitos para la adhesión de cualquiera de estos Estados al acervo de Schengen se cumplan antes de la entrada en vigor del Tratado de Amsterdam.

ARTÍCULO 3

Después de la determinación mencionada en el párrafo segundo del apartado 1 del artículo 2, Dinamarca mantendrá los mismos derechos y obligaciones en relación con los demás signatarios de los acuerdos de Schengen que antes de la mencionada determinación con respecto a aquellas partes del acervo de Schengen cuya base jurídica quede determinada en el título III bis del Tratado constitutivo de la Comunidad Europea.

Por lo que respecta a aquellas partes del acervo de Schengen cuya base jurídica quede determinada en el título VI del Tratado de la Unión Europea, Dinamarca seguirá teniendo los mismos derechos y obligaciones que los demás signatarios de los acuerdos de Schengen.

ARTÍCULO 4

Irlanda y el Reino Unido de Gran Bretaña e Irlanda del Norte, que no están vinculados por el acervo de Schengen, podrán solicitar en cualquier momento participar en algunas o en todas las disposiciones de dicho acervo.

El Consejo decidirá sobre tal solicitud por unanimidad de los miembros a que se refiere el artículo 1 y del representante del gobierno del Estado de que se trate.

ARTÍCULO 5

1. Las propuestas e iniciativas para desarrollar el acervo de Schengen estarán sometidas a las correspondientes disposiciones de los Tratados.

En este contexto, en el caso de que Irlanda, el Reino Unido o ambos no hayan notificado al Presidente del Consejo por escrito y en un plazo razonable que desean participar, se considerará que la autorización a la que se refieren el artículo 5 A del Tratado constitutivo de la Comunidad Europea y el artículo K.12 del Tratado de la Unión Europea se ha concedido a los Estados miembros a que se refiere el artículo 1 y a Irlanda o al Reino Unido cuando cualquiera de ellos desee participar en los ámbitos de cooperación de que se trate.

2. Las disposiciones pertinentes de los Tratados a que se refiere el párrafo primero del apartado 1 se aplicarán aún cuando el Consejo no haya adoptado las medidas contempladas en el párrafo segundo del apartado 1 del artículo 2.

ARTÍCULO 6

La República de Islandia y el Reino de Noruega serán asociados a la ejecución del acervo de Schengen y en su desarrollo futuro con arreglo al Acuerdo firmado en Luxemburgo el 19 de diciembre de 1996. A tal efecto se adoptarán procedimientos adecuados mediante un acuerdo que el Consejo celebrará con dichos Estados, por unanimidad de los miembros a que se refiere el artículo 1. Dicho acuerdo contendrá disposiciones sobre la participación de Islandia y Noruega en cualquier repercusión financiera que se derive de la aplicación del presente Protocolo.

El Consejo celebrará, por unanimidad, un acuerdo independiente con Islandia y Noruega para determinar los derechos y obligaciones entre Irlanda y el Reino Unido de Gran Bretaña e Irlanda del Norte, por un lado, e Islandia y Noruega por otro, en los ámbitos del acervo de Schengen que se apliquen a estos Estados.

ARTÍCULO 7

El Consejo decidirá, por mayoría cualificada, las disposiciones para la integración de la Secretaría de Schengen en la Secretaría General del Consejo.

ARTÍCULO 8

A efectos de las negociaciones para la admisión de nuevos Estados miembros en la Unión Europea, se considerará que el acervo de Schengen y otras medidas adoptadas por las instituciones en su ámbito han de aceptarse en su totalidad como acervo por todo Estado que sea candidato a la adhesión.

ANEXO ACERVO DE SCHENGEN

1. El Acuerdo, firmado en Schengen el 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica del Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes.

2. El Convenio, firmado en Schengen el 19 de junio de 1990, entre el Reino de Bélgica, la República Federal de Alemania, la República Francesa, el Gran Ducado de Luxemburgo y el Reino de los Países Bajos, de aplicación del Acuerdo de Schengen relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985, junto con su Acta Final y declaraciones comunes.

3. Los Protocolos y acuerdos de adhesión al Acuerdo de 1985 y al Convenio de aplicación de 1990 con Italia (firmado en París el 27 de noviembre de 1990), España y Portugal (firmados en Bonn el 25 de junio de 1991), Grecia (firmado en

Madrid el 6 de noviembre de 1992), Austria (firmado en Bruselas el 28 de abril de 1995) y Dinamarca, Finlandia y Suecia (firmados en Luxemburgo el 19 de diciembre de 1996), junto con sus actas finales y declaraciones.

4. Decisiones y declaraciones adoptadas por el Comité Ejecutivo creado por el Convenio de aplicación de 1990, así como actos adoptados para la aplicación del Convenio por instancias a las que el Comité Ejecutivo haya atribuido competencias decisorias.

MEMORIA DE 1998 - ANEXO IX - CONSEJO DE EUROPA: RECOMENDACIÓN Nº R(97) 18 Y EXPOSICIÓN DE MOTIVOS DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS RELATIVA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, RECOGIDOS Y TRATADOS CON FINES ESTADÍSTICOS

Recomendación nº R (97) 18 y Exposición de los motivos

DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS RELATIVA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, RECOGIDOS Y TRATADOS CON FINES ESTADÍSTICOS

(adoptada por el Comité de Ministros el 30 de septiembre de 1997, en la 602º reunión de Delegados de Ministros)

Exposición de motivos

El Comité de Ministros, al amparo del artículo 15.b del Estatuto del Consejo de Europa;

Considerando que el objetivo del Consejo de Europa es de realizar una unión más estrecha entre sus miembros;

Consciente de las necesidades, tanto en el sector público como en el privado, de estadísticas fiables para el análisis y la comprensión de la estructura y de la evolución de la sociedad contemporánea, y para la definición de las políticas y de las estrategias para las medidas que han de adoptarse en prácticamente todos los ámbitos de la vida cotidiana;

Reconociendo que la producción de estadísticas fiables depende, en gran medida, de la recogida de datos tan completos como fuere posible y el tratamiento de los mismos mediante medios informáticos cada vez más eficientes;

Consciente del hecho que dichos datos pueden referirse a personas naturales identificadas o identificables ("datos de carácter personal");

Consciente de la necesidad de desarrollar técnicas que permitan garantizar el anonimato de las personas concernidas;

Considerando las preocupaciones de la comunidad internacional de los profesionales de la estadística con respecto a la protección de datos de carácter personal, así como el desarrollo de las recomendaciones internacionales en materia de deontología profesional de los mismos;

Considerando asimismo los principios fundamentales de la estadística oficial adoptados por la comunidad internacional en el marco de la Organización de las Naciones Unidas;

Constatando el desarrollo progresivo de las normas jurídicas, nacionales y supranacionales, tanto en materia de actividades estadísticas como en el campo de la protección de datos de carácter personal;

Recordando a este respecto los principios generales relativos a la protección de datos del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Estrasburgo 1981, Serie de tratados europeos nº 108);

Recordando asimismo las exenciones admitidas en favor de las actividades estadísticas en el Convenio con respecto al ejercicio, por las personas concernidas, de ciertos derechos enunciados en el mismo;

Constatando que las exenciones, en dicho sentido, están igualmente previstas, por varios Estados miembros, en las legislaciones existentes o en proceso de elaboración en materia de protección de datos;

Considerando que conviene hallar un equilibrio entre la necesidad de la producción de estadísticas, por una parte, y la indispensable protección de la persona, por otra, concretamente cuando se utilizan tratamientos automatizados de datos;

Consciente de la necesidad de establecer procedimientos adecuados con el objeto de conciliar los intereses de las diferentes partes interesadas;

Consciente de que el progreso realizado en los métodos estadísticos y el desarrollo que ha tenido lugar en la tecnología de la información, desde 1983, necesitan la revisión de varias disposiciones de la Recomendación nº R (83) 10 relativa a la protección de datos de carácter personal utilizados para fines de investigación científica y de estadística;

Recomienda a los gobiernos de los Estados miembros:

1. Tomar medidas para que se reflejen los principios expuestos en el anexo de la presente recomendación en su derecho y en las prácticas de dichos Estados;

2. Asegurar una amplia difusión de los principios expuestos en el anexo de la presente recomendación entre las personas, autoridades públicas y organismos que realizan la recogida y el tratamiento de datos de carácter personal con fines estadísticos, tanto en los sectores públicos como privados, así como entre las instancias competentes en

materia de protección de datos;

3. Incitar a dichas personas, autoridades públicas y organismos a que introduzcan, si aún no lo han hecho, códigos deontológicos inspirados por el anexo a la presente recomendación;

Decide que la presente recomendación reemplaza a la Recomendación nº R (83) 10, relativa a la protección de datos de carácter personal utilizados para fines de investigación científica y de estadística, en la medida en que la presente recomendación se aplique a la recogida y al tratamiento automatizado de datos de carácter personal para fines estadísticos.

Anexo de la Recomendación nº R (97) 18

1. Definiciones

Para los fines de la presente recomendación:

La expresión "datos de carácter personal" se refiere a toda la información sobre una persona natural identificada o identificable (persona concernida1). Una persona física no será considerada como "identificable" si dicha identificación necesitare plazos y actividades poco razonables. Si una persona natural no fuere identificable, los datos se considerarán anónimos.

La expresión "datos de identificación" atañe a los datos de carácter personal que permitieren la identificación directa de la persona concernida y que fueren necesarios para la recogida, el control y el apareamiento de los datos, pero que luego no fueren utilizados para establecer resultados estadísticos.

La expresión "datos sensibles" se refiere a los datos de carácter personal que revelaren la raza, ideas políticas, convicciones religiosas u otras convicciones, al igual que los datos de carácter personal relativos a la salud, a la vida sexual o referentes a condenas penales, así como otros datos definidos como sensibles por el derecho interno.

La expresión "tratamiento" se refiere a toda operación o conjunto de operaciones efectuadas, parcial o totalmente, con ayuda de procedimientos automatizados, y aplicados a datos de carácter personal, como por ejemplo, el registro, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación, apareamiento o interconexión, así como la supresión o destrucción.

El término "comunicación" se refiere al acto de hacer accesibles los datos de carácter personal a terceros, sean cuales fueren los medios o los soportes utilizados.

La expresión "con fines estadísticos" se refiere a todas aquellas operaciones de recogida y de tratamiento de datos de carácter personal necesarias para las investigaciones estadísticas o para la producción de resultados estadísticos. De dichas operaciones se excluye toda utilización de la información obtenida para decisiones o medidas relativas a una persona determinada.

La expresión "resultados estadísticos" designa una información obtenida por el tratamiento de datos de carácter personal con objeto de caracterizar un fenómeno colectivo en una población considerada.

La expresión "responsable del tratamiento" se refiere a la persona natural o jurídica, a la autoridad pública o a cualquier otro organismo que, solo o con la colaboración de otros, determina las finalidades y los medios -concretamente la organización- de la recogida y del tratamiento de datos de carácter personal.

2. Ámbito de aplicación

2.1. La presente recomendación se aplica a la recogida y al tratamiento automatizado de datos de carácter personal con fines estadísticos.

Se aplica también a los resultados estadísticos, en la medida en que éstos permitieren identificar a las personas interesadas.

2.2. Se alienta a los Estados miembros a extender la aplicación de la presente recomendación a los tratamientos no automatizados de datos de carácter personal con fines estadísticos.

2.3. No debe efectuarse un tratamiento de datos de carácter personal de manera no automatizada con el fin de eludir las disposiciones de la presente recomendación.

2.4. Los Estados miembros pueden extender la aplicación de los principios mencionados en la presente recomendación igualmente a la recogida y al tratamiento de datos relativos a agrupaciones de personas, asociaciones, fundaciones, sociedades, corporaciones, o a cualquier otro organismo que agrupare, directa o indirectamente, a personas naturales que ostentare o no personalidad jurídica.

3. Respeto de la intimidad

3.1. El respeto a los derechos y a las libertades fundamentales, y concretamente al derecho a la vida privada, debe garantizarse en el momento de la recogida y del tratamiento de datos de carácter personal con fines estadísticos, al igual que:

a. En el momento de la conservación de estos datos para una utilización futura;

b. En el momento de la difusión de los resultados estadísticos;

c. Y, en el momento de la posible modificación de datos de carácter personal cuando dicha modificación se impusiere para mejorar la representatividad de resultados estadísticos o por razones de confidencialidad.

3.2. El derecho o la práctica de carácter interno deben someter a secreto profesional a las personas que, con motivo de la realización de una actividad estadística, tuvieren conocimiento de datos de carácter personal.

3.3. Los datos de carácter personal, recogidos y tratados con fines estadísticos, deben ser convertidos en anónimos desde el momento en que ya no fueren necesarios bajo forma identificable.

4. Condiciones generales que rigen la recogida y el tratamiento con fines estadísticos

Finalidad

4.1 Los datos de carácter personal obtenidos y tratados, con fines estadísticos, deberán emplearse únicamente para tal fin. No deberán utilizarse para adoptar una decisión o una medida relativa a la persona concernida o para completar o corregir los ficheros cuyos datos de carácter personal no tuvieren fines estadísticos.

4.2 El tratamiento automatizado, con fines estadísticos, de los datos de carácter personal con fines no estadísticos no será incompatible con la/las finalidad(es) para las que se recogieron inicialmente los datos, en la medida en que estuvieren previstas las garantías apropiadas, en particular, para evitar la utilización de los datos para apoyar decisiones o medidas relativas a la persona concernida.

Licitud

4.3 Los datos de carácter personal podrán obtenerse y tratarse con fines estadísticos:

a. Si estuviere previsto en la ley; o

b. En la medida en que la ley lo autorizare, y

i. si la persona concernida o su representante legal lo hubiere consentido conforme a lo dispuesto en al principio 6; o

ii. si se hubiere informado a la persona de la recogida o tratamiento de sus datos y no se hubiere opuesto a ello, siempre que el tratamiento no afectare a datos sensibles; o

iii. si las circunstancias de la recogida y el objetivo de la encuesta son de tal naturaleza que permitieren que una persona pueda responder en nombre y en lugar de otras, conforme a lo dispuesto en el principio 6, siempre que no existiere, de forma manifiesta, riesgo alguno de intromisión en la intimidad de dichas personas, y, en especial, que el tratamiento no afectare a datos sensibles.

4.4 A fin de evitar que los mismos datos no se recojan de nuevo, los datos de carácter personal recogidos con fines no estadísticos podrán tratarse igualmente para fines estadísticos si fuere necesario:

a. Para ejecutar una misión de interés público o derivante del ejercicio de la autoridad pública; o

b. Para la consecución de interés legítimo perseguido por el responsable del tratamiento automatizado, con la condición de que los derechos y las libertades fundamentales de la persona concernida no se vieren perjudicados.

En las mismas condiciones, los datos recogidos con fines estadísticos pueden también utilizarse con otros fines estadísticos.

4.5 Los datos de carácter personal no podrán obtenerse con carácter coercitivo con vistas a un tratamiento con fines estadísticos, excepto si el derecho interno lo exigiere.

4.6 Los datos de carácter personal o conjuntos de datos de carácter personal podrán aparejarse o relacionarse con fines estadísticos si el derecho interno estableciere garantías apropiadas para impedir su tratamiento y comunicación con fines no estadísticos.

Proporcionalidad

4.7 La obtención y el tratamiento de los datos de carácter personal deberán limitarse sólo a los datos necesarios para las finalidades estadísticas perseguidas. En particular, los datos de identificación sólo deben recogerse y tratarse si ello fuere necesario.

Datos sensibles

4.8 Si se trataren datos sensibles para fines estadísticos dichos datos deberían ser recogidos proteger sin que las personas interesadas sean identificables.

Si el objetivo legítimo y específico del tratamiento de los datos personales para fines estadísticos hiciere necesario la identificación de las personas interesadas, el derecho interno deberá prever las garantías adecuadas, incluyendo medidas específicas para separar los datos de identificación, desde la recogida, salvo cuando fuere manifiestamente poco razonable o impracticable.

5. Información sobre las personas

Primera recogida de datos

5.1 Si recogieren datos de carácter personal para fines estadísticos, se deberá informar sobre los aspectos siguientes a las personas a las que se preguntare:

a. El carácter obligatorio o facultativo de las respuestas y el fundamento jurídico, en su caso, de la recogida de los datos;

b. El o los fines de la recogida y tratamiento de los datos;

c. El nombre y el estatuto de la persona u organismo responsable de la recogida y/o tratamiento de los datos;

d. El hecho de que dichos datos se mantendrán como confidenciales y serán empleados únicamente con fines estadísticos;

e. La posibilidad de obtener más información si se pidiere.

En lo que respecta a sus peticiones y/o según las modalidades definidas por el derecho interno, se deberá asimismo informar sobre los aspectos siguientes a las personas interesadas:

f. Si se realizare una encuesta facultativa, acerca de las formas en que se puede rehusar o revocar el consentimiento y, cuando la encuesta fuere obligatoria, sobre las eventuales sanciones;

g. Si llegare el caso, acerca de las condiciones del ejercicio del derecho de acceso y de rectificación;

h. Acerca de las categorías de personas u organismos a los que se podrá dar información sobre los datos de carácter personal;

i. Sobre las garantías para asegurar que la confidencialidad y protección de los datos de carácter personal;

j. Acerca de las categorías de los datos que se hubieren recogido y tratado.

5.2. Si no se preguntare de forma directa a las personas concernidas, se les deberá informar de la existencia de la recogida de datos, salvo si ello resultare, de forma manifiesta, poco razonable o impracticable. Dichas personas deberán disponer de la posibilidad de informarse de forma apropiada de los aspectos mencionados en el principio 5.1.

5.3. Se deberá informar a las personas interrogadas, estuvieren concernidas o no, como muy tarde, en el momento de la recogida de datos. Las modalidades y la extensión de la información deberán ser apropiadas y adaptarse a las circunstancias.

Se podrá diferir la facilitación de información, o parte de la misma, si se considerare necesario con vistas a la obtención del objetivo legítimo de la encuesta, según su objeto y naturaleza. Dicha información tendrá que facilitarse a partir del momento en que no existiere tal necesidad, salvo cuando resultare, de forme manifiesta, poco razonable o impracticable. En dichos casos, y cuando los datos hubieren sido recogidos de la persona concernida, dicha información habrá de facilitarse en un momento posterior.

Recogida secundaria

5.4. El tratamiento o la comunicación, con fines estadísticos, de los datos de carácter personal, recogidos con fines no estadísticos, exigirá una publicidad adecuada. Las personas concernidas deberán poder tener la posibilidad de informarse adecuadamente de los elementos mencionados en el principio 5.1, a menos que:

a. Resultare imposible facilitar la información exigida o si ello implicare esfuerzos desproporcionados; o que

b. El derecho interno no previere expresamente el tratamiento automatizado o la comunicación de los datos con fines estadísticos.

En los casos considerados en las letras a y b habrá que prever las garantías adecuadas.

Personas legalmente incapaces

5.5. Si la persona concernida no estuviere ni legalmente capacitada ni en disposición de decidir de forma libre, y si el derecho interno no le permitiere actuar en su propio nombre, la información deberá entregarse a la persona con capacidad legal para actuar en interés de la persona concernida.

Si la persona legalmente incapaz pudiere comprender debería ser informada antes de que los datos que la conciernen se recogieren o trataren de forma automatizada.

6. Consentimiento

6.1. Si se requiriere el consentimiento de la persona concernida éste tendrá que ser libre, consciente e indubitado.

La persona concernida deberá ostentar la posibilidad de revocar su consentimiento para una encuesta única, antes de que se separen los datos de identificación de los demás datos recogidos; también podrá interrumpir su cooperación con una encuesta escalonada en el tiempo, en todo momento y sin que dicha acción surta efectos retroactivos.

6.2. Si la recogida o el tratamiento de datos sensibles lo exigiere, el consentimiento de la persona deberá ser explícito, libre y consciente. No podrá considerarse que el objetivo legítimo de la encuesta no requiere dicho consentimiento, salvo que un motivo importante de interés público justificare dicha exención.

6.3. Se requerirá el consentimiento de la persona que legalmente pueda actuar en nombre de la persona concernida, el de una autoridad o el de cualquier otra persona o instancia designada por la ley, si se previere el tratamiento, con fines estadísticos, de los datos de carácter personal que interesaren a la persona legalmente incapaz que no tuviere capacidad para decidir libremente.

Si, de acuerdo con el principio 5.5 arriba transcrito, se informare a la persona legalmente incapaz de la intención de recoger y de tratar de forma automatizada los datos de carácter personal que le interesaren, su deseo podría tomarse en cuenta a menos que el derecho interno se opusiere a ello.

6.4. No habrá de sancionarse la negativa a responder, salvo cuando estuviere previsto en el derecho interno.

7. Derechos de acceso y de rectificación

7.1. Cualquier persona podrá obtener la comunicación de los datos de carácter personal que la concernieren y que detentare el responsable del tratamiento y conseguir, en su caso, la rectificación.

7.2. No obstante, cuando no existiere, de forma manifiesta, riesgo alguno de atentar contra la intimidad de la persona concernida, dicho derecho podrá restringirse, de acuerdo con lo dispuesto en el derecho interno, si los datos de carácter personal fueren tratados únicamente con fines estadísticos y si existieren medidas apropiadas específicas con vistas a la prevención de cualquier identificación por terceras personas, tanto partiendo de los datos individuales como de los resultados estadísticos.

8. Anonimato

8.1 Los datos de carácter personal recogidos con fines estadísticos serán convertidos en anónimos en cuanto finalicen las operaciones de recogida, control o clasificación, excepto:

a. Si los datos de identificación siguieren siendo necesarios para fines estadísticos y que se hubieren adoptado las medidas contempladas en el principio 10.1; o

b. Si la propia naturaleza del tratamiento estadístico necesitare poner en marcha las otras operaciones de tratamiento antes de que los datos pasaren a ser anónimos, y siempre que se pusieren en práctica las medidas de protección previstas en los artículos 15.1 a 15.3.

9. Recogida primaria de datos de carácter personal con fines estadísticos

9.1 La recogida de datos de carácter personal deberá ser leal, sobre todo en lo relativo a la información de las personas y a su libertad para contestar.

9.2 La recogida de datos de carácter personal se realizará obteniendo los mismos de la persona interesada o, dependiendo de la naturaleza de la encuesta, podrá hacerse obteniéndolos de un miembro de su hogar. La recogida de datos de carácter personal obteniéndolos de una persona diferente al interesado o a un miembro de su hogar, al igual que la realizada obteniendo los datos de entidades jurídicas, como empresas o colectividades públicas, no deberá realizarse excepto cuando la legislación interna lo permitiere y estableciere medidas de protección apropiadas, o cuando, de modo manifiesto, no existiere riesgo alguno de conculcar los derechos y libertades fundamentales de las personas interesadas.

9.3. La recogida de datos de carácter personal, con fines estadísticos, realizada sin hacer preguntas no deberá referirse a datos de identificación ni relacionarse con datos de identificación, excepto si la legislación interna incluyere medidas de protección adecuadas y
a. Contemplare la recogida con datos de identificación; o

b. Permitiere la puesta en relación con datos de identificación para la realización de muestras.

9.4. Los datos referentes a los que no respondieren que fueren pertinentes para la planificación o ejecución de la encuesta, y la información sobre las razones de la ausencia de respuesta, no podrán ser utilizados salvo para asegurar la representatividad del estudio.

9.5. En el caso de que, en la recogida de datos de carácter personal, se recurriere a encuestadores o a otras personas que recibieren directamente las respuestas proporcionadas, deberá prestarse especial atención a la elección de las personas y a la organización y métodos escogidos para la encuesta, con el fin de garantizar el respeto de la finalidad de la encuesta, de la confidencialidad de los datos y a la protección de la intimidad.

9.6 El responsable del tratamiento deberá adoptar las medidas apropiadas que permitan a la persona encuestada asegurarse de la legitimidad de la persona que recogiere sus datos.

10. Datos de identificación

10.1 Si los datos de identificación se recogieren y trataren con fines estadísticos, deberán separarse y conservarse a parte de los otros datos de carácter personal, excepto si, de modo manifiesto, no fuere razonable o fuere impracticable.

10.2. Los datos de identificación podrán ser utilizados para crear un archivo de direcciones con fines estadísticos si el derecho interno lo previere, siempre que la persona concernida fuere informada y no se opusiere a ello, o si los datos provinieren de un archivo accesible al público.

11. Conservación de los datos

11.1. A menos que se convirtieren en anónimos o que la ley interna previere su conservación, con el fin de archivo y con las garantías apropiadas, los datos de carácter personal recabados y tratados con fines estadísticos deberán ser destruidos o borrados siempre que ya no fueren necesarios para dichos fines.

En especial, los datos de identificación deberán ser destruidos o borrados desde el momento en que ya no fueren necesarios para:

a. Las operaciones de recogida, control y clasificación de datos; o

b. Asegurar la representatividad de la encuesta; o

c. Realizar una nueva encuesta con las mismas personas.

12. Comunicación

12.1. Los datos de carácter personal recabados con fines estadísticos no deberán ser comunicados con fines no estadísticos.

12.2. Aquellos datos de carácter personal que fueren tratados con fines estadísticos determinados podrán ser comunicados para otros fines estadísticos siempre y cuando se especificaren dichos fines y se limitaren en el tiempo.

12.3. Salvo que el derecho interno previere salvaguardias para la comunicación, las comunicaciones, de conformidad con lo dispuesto en el principio 12.2, deberán dar lugar a documento escrito que reflejará los derechos y los deberes de las partes. Cuando se comunicaren los datos, el responsable de su tratamiento deberá, en particular:

a. Estipular que dicho tercero no podrá comunicar por sí mismo los datos en cuestión sin el beneplácito expreso de dicho responsable del tratamiento;

b. Estipular que dicho tercero tomará las medidas de seguridad apropiadas, de conformidad con lo dispuesto en los principios 15.1 y 15.3 de la presente recomendación;

c. Asegurarse que cualquier publicación de los resultados estadísticos, obtenidos por dicho tercero, se realizará de conformidad con lo dispuesto en el capítulo 14 de la presente recomendación.

12.4. Además, los datos sensibles sólo podrán comunicarse si la ley lo previere o si el interesado o su representante legal lo hubiere consentido de forma explícita, siempre que el derecho interno no lo prohibiere.

13. Flujo transfronterizo de los datos

13.1. Los principios de la presente recomendación son aplicables a la comunicación transfronteriza de los datos de carácter personal para fines estadísticos.

13.2. La comunicación transfronteriza de los datos de carácter personal hacia un Estado que hubiere ratificado el Convenio nº 108i y que dispusiere de una legislación que asegurare una protección de datos equivalente, como mínimo, no debería estar sometida a condiciones particulares de protección de la intimidad y de los derechos y de las libertades fundamentales de las personas.

13.3. No debería haber limitaciones en la comunicación transfronteriza de datos de carácter personal con fines estadísticos hacia un Estado que no hubiere ratificado la el Convenio nº 108 si éste asegurare un nivel de protección conforme a los principios de dicho Convenio y de la presente recomendación.

13.4. A menos que el derecho interno dispusiere diversamente, la comunicación transfronteriza de datos de carácter personal para fines estadísticos hacia un Estado que no asegurare una protección conforme a los principios del Convenio nº 108 y de la presente recomendación no debería, por regla general, tener lugar salvo que:

a. Se tomaren las medidas necesarias, incluidas aquéllas de naturaleza contractual, con respecto a los principios del Convenio y de la presente recomendación; o que,

b. La persona concernida hubiere dado su expreso consentimiento.

14. Resultados estadísticos

14.1. Los resultados estadísticos deberán únicamente ser publicados o ser accesibles a terceros, si se hubieren tomado medidas para asegurar que las personas concernidas ya no son identificables basándose en dichos resultados, a menos que la difusión o la publicación no supusiere manifiestamente algún riesgo que atentare contra la intimidad de dichas personas.

15. Seguridad de los datos

15.1. Los responsables de los tratamientos deberán velar por asegurar la confidencialidad de los datos de carácter personal mediante medidas técnicas y organizativas apropiadas. Aquéllos tomarán concretamente medidas contra el acceso, la modificación, la comunicación o cualquier otra forma de tratamiento no autorizado.

15.2. Si los datos deben ser conservados bajo forma identificable, se deberá hacer uso de los recursos organizativos y técnicos, particularmente los informáticos, para prevenir una identificación no autorizada de la persona interesada.

15.3. Se tomarán medidas para impedir que las personas concernidas puedan volver a ser identificadas y que los datos de carácter personal recogidos con fines estadísticos puedan ser utilizados para fines no estadísticos.

15.4. Los profesionales, las empresas y los organismos encargados de la realización de estadísticas deberán perfeccionar técnicas y procedimientos que permitan asegurar el anonimato de las personas concernidas.

16. Códigos deontológicos

16.1. Los profesionales, las empresas y los organismos, encargados de la realización de estadísticas, deberán adoptar y hacer públicos códigos deontológicos conformes a la presente recomendación y que contengan, concretamente, información acerca de:

a. Otras categorías de personas y de organismos que tuvieren acceso a los datos de carácter personal;

b. Las medidas de protección, de confidencialidad y de seguridad de dichos datos, así como de la ética estadística; y,

c. Los responsables del tratamiento estadístico.

17. Desarrollo técnico, cooperación y asistencia

Con el fin de asegurar un amplio acceso a los instrumentos informáticos y a los conocimientos técnicos apropiados para una protección eficaz de los datos de carácter personal recogidos para fines estadísticos, las instancias gubernamentales competentes deberán colaborar estrechamente en el desarrollo de dichos instrumentos y conocimientos y establecer programas internacionales de cooperación, de intercambio de experiencias, transferencia de conocimientos y de asistencia técnica.

18. Autoridades de control

Los Estados miembros encargarán a una o más autoridades independientes de vigilar la aplicación del derecho interno que desarrollare los principios enunciados en la presente recomendación.

1 Nota del traductor: En versión castellana de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, se utiliza el término "el interesado" y "datos personales". En esta traducción se ha preferido el término "persona concernida" o "persona interesada" al ser el utilizado en la traducción oficial del Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, tal y como se publicó en el "BOE" de 15 de noviembre de 1985. Análogamente, se ha preferido la traducción de "datos de carácter personal" frente a la de "datos personales". Sin embargo, para aquellos términos no contenidos en dicho Convenio se han utilizado las equivalencias entre términos franceses y castellanos establecidas por la Directiva citada.
1. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Estrasburgo, 28 de enero de 1981 (Serie de tratados europeos nº 108).

MEMORIA DE 1998 - DOCUMENTOS DEFINITIVOS APROBADOS POR EL GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE

Consejo de Europa - DIRECCIÓN DE ASUNTOS JURÍDICOS
División del Derecho Público e Internacional - Sección "Protección de datos"
Tel.: (33) 3 88 41 25 51 - Fax: (33) 3 88 41 27 64

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV

Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

DG XV D/5057/97 final
WP 7
Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales
Documento de Trabajo:
Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?
Adoptado por el Grupo de Trabajo el 14 de enero de 1998

DOCUMENTO DE TRABAJO
EVALUACIÓN DE LA AUTORREGULACIÓN INDUSTRIAL: ¿EN QUÉ CASOS REALIZA UNA CONTRIBUCIÓN SIGNIFICATIVA AL NIVEL DE PROTECCIÓN DE DATOS EN UN PAÍS TERCERO?

Introducción

El apartado 2 del artículo 25 de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (95/46/CE) establece que el nivel de protección que ofrece un país tercero se evaluará atendiendo a *todas las circunstancias* que concurran en una transferencia o en una categoría de transferencias de datos. Se hace referencia específica no sólo a las normas de Derecho, sino también a las "normas profesionales y las medidas de seguridad en vigor en dichos países." El texto de la Directiva exige por lo tanto que se tengan en cuenta las normas no jurídicas que puedan existir en el país tercero en cuestión, siempre que estas normas *estén vigentes. En este contexto debe evaluarse la función de la autorregulación industrial.*

¿Qué es la autorregulación?

El término "autorregulación" puede significar cosas distintas para diferentes personas. A efectos del presente documento, deberá entenderse por código de autorregulación (u otro instrumento) cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión. Ésta es una definición amplia que abarcaría desde un código de protección de datos voluntario desarrollado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos o banqueros, que suelen tener una fuerza cuasi jurídica.

¿Es el organismo responsable del código representante del sector?

Tal como sostendrá este documento, un importante criterio para juzgar el valor de un código es el grado hasta el cual pueden hacerse cumplir sus normas. En este contexto, la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos, tiene probablemente menos importancia que la fuerza de la asociación en cuanto a su capacidad de, por ejemplo, imponer sanciones a sus miembros por incumplimiento del código. No obstante, existen diversas razones secundarias que hacen que los códigos que abarcan a todo un sector industrial o una profesión sean instrumentos de protección más útiles que los desarrollados por pequeñas agrupaciones de empresas dentro de un sector industrial. En primer lugar figura el hecho de que, desde el punto de vista del consumidor, un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código para la protección de datos, es 3 algo confuso. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos sean objeto de tratamiento. En segundo lugar, especialmente en sectores tales como el marketing directo, donde es práctica corriente transferir los datos personales entre diferentes empresas del mismo sector, pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de ambigüedad en cuanto a la naturaleza de las normas aplicables, y también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

Evaluación de la autorregulación - el enfoque más adecuado

Dada la gran variedad de instrumentos que entran dentro de la noción de autorregulación, está claro que existe una necesidad de diferenciar entre las diversas formas de autorregulación en términos de su impacto real en el nivel de protección de datos aplicable cuando se transfieren datos personales a un país tercero. El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos (tengan éstas categoría de autorregulación o de regulación) debe ser el enfoque general establecido en el documento de debate "Primeras orientaciones sobre las transferencias de datos personales a países terceros - Posibles formas de evaluar su adecuación". La piedra angular de este enfoque es el examen no sólo del contenido del instrumento (deberá contener una serie de principios básicos), sino también de su eficacia en cuanto a lograr:

- un buen nivel de obediencia general
- apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento
- una reparación adecuada (incluida la compensación, cuando corresponda).

Evaluación del contenido de un instrumento de autorregulación

Esta es una tarea relativamente sencilla. Se trata de garantizar que estén presentes los "principios de contenido" necesarios establecidos en el documento "Primeras orientaciones" (véase el extracto adjunto). Esta es una evaluación objetiva. Se trata de ver cual es el contenido del código, y no cómo se elaboró éste. El hecho de que un sector industrial o profesión haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante por sí mismo, aunque evidentemente, si en su desarrollo se han tenido en cuenta las opiniones de los individuos cuyos datos sean objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje más fielmente los principios básicos necesarios para la protección de datos.
La transparencia del código es un elemento crucial; en particular, el código debería redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones. Además, el código debería prohibir la transferencia de datos a empresas que no pertenezcan al sector y que no se rijan por el código, a menos que se prevean otras protecciones adecuadas.

Evaluación de la eficacia de un instrumento de autorregulación

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas por los que se garantiza la adhesión al código y por los que se resuelven los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales para juzgar la eficacia de la protección, para que pueda tenerse en cuenta un código de autorregulación en la evaluación de la adecuación de su protección.

Un buen nivel de obediencia general

Típicamente, un código profesional o industrial será desarrollado por un organismo representante del sector industrial o profesión en cuestión, y se aplicará a los miembros de dicho organismo representante específico. El nivel de cumplimiento del código dependerá del grado de conocimiento de la existencia del código y su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz, de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y, quizás lo más importante, de la naturaleza y la aplicación de las sanciones en caso de incumplimiento. Por tanto, son importantes las siguientes preguntas:

- ¿Qué medidas adopta el organismo representante para asegurarse de que sus miembros conocen el código?
- ¿Exige el organismo representante a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
- ¿Presentan dichas pruebas las propias empresas o proceden de una fuente externa (tal como un auditor acreditado)?
- ¿Investiga el organismo representante las supuestas o presuntas violaciones del código?
- ¿Es el cumplimiento del código una condición para formar parte del organismo representante o es dicho cumplimiento meramente "voluntario"?
- En caso de que un miembro viole el código, ¿con qué tipos de sanciones disciplinarias cuenta el organismo representante (expulsión u otras)?
- ¿Es posible para un individuo o empresa continuar trabajando en la profesión o sector industrial concreto, incluso después de haber sido expulsado del organismo representante?
- ¿Puede hacerse cumplir el código de otras maneras, por ejemplo en los tribunales o en un tribunal especializado? Los códigos profesionales tienen fuerza jurídica en algunos países. En algunas circunstancias, también puede ser posible aplicar las leyes generales relativas a prácticas comerciales correctas o incluso de competencia para aplicar los códigos de conducta de los sectores industriales.

Al examinar los tipos de sanciones existentes, es importante distinguir entre una sanción "reparadora" que únicamente exige que un responsable del tratamiento, en caso de incumplimiento, modifique sus prácticas con el fin de adecuarlas a lo establecido en el código, y una sanción que vaya más lejos, castigando al responsable por su incumplimiento. Sólo la segunda categoría de sanción "punitiva" tiene repercusión en el comportamiento futuro de los responsables del tratamiento, proporcionando un incentivo para que se cumpla sistemáticamente el código.

La falta de sanciones auténticamente disuasorias y punitivas es por tanto un fallo esencial en un código. Sin dichas

sanciones, es difícil entender cómo puede lograse un nivel satisfactorio de obediencia global, a no ser que se establezca un sistema riguroso de control externo (tal como una autoridad pública o privada competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

Apoyo y ayuda a los individuos cuyos datos sean objeto de tratamiento

Un requisito esencial para un sistema de protección de datos adecuado y eficaz es que no se abandone a los individuos que se enfrentan a un problema relativo a sus datos personales, sino que se les proporcione un apoyo institucional que permita hacer frente a sus dificultades. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:

- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Conlleva el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez sobre una supuesta violación de un código es un punto clave. Claramente, dicha persona u organismo deberá ser independiente respecto al responsable del tratamiento. No obstante, esto por sí mismo no basta para garantizar la imparcialidad. Idealmente, el árbitro debería asimismo no pertenecer a la profesión o sector en cuestión, por la razón de que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya violado el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

Reparación adecuada

Si el código de autorregulación resulta violado, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (p. ej. corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, permitir el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico o moral que se cause (llamado "distress" en el Derecho del Reino Unido y de EEUU).
Muchas de las cuestiones relativas a las sanciones que se han enumerado en la sección "Un buen nivel de obediencia general" son pertinentes aquí. Tal y como se ha explicado anteriormente, las sanciones tienen una doble función: castigar al infractor (y fomentar así el cumplimiento de las normas por parte del infractor y de los demás), y remediar una violación de las normas. Nos ocuparemos ahora de la segunda función. Por lo tanto, podrían plantearse también las siguientes preguntas:

- ¿Es posible comprobar que un miembro que manifiestamente haya violado el código, ha modificado sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación con arreglo al código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una violación de contrato, o puede hacerse cumplir en virtud del Derecho público (p. ej. protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

Conclusiones

La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el documento "Primeras orientaciones".
Para que un instrumento de autorregulación pueda considerarse un elemento válido para una "protección adecuada" debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
El instrumento debe ser transparente e incluir el contenido básico de los principios esenciales de la protección de datos.
El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograr esto es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada.

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV

Mercado Interior y Servicios Financieros
Libre circulación de la información, Derecho de sociedades e información financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

DG XV D/5005/98 final
WP 9

Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales

Documento de trabajo:
Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países
Aprobado por el Grupo de Trabajo el 22 de abril de 1998

Utilización de disposiciones contractuales
en caso de transferencia de datos personales a terceros países

1. Introducción

En el documento de debate adoptado el 26 de junio de 1997 y titulado "First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy" (Primeras orientaciones sobre las transferencias de datos personales a terceros países - Posibles métodos para evaluar la adecuación), el Grupo de Trabajo se comprometió a examinar, con ocasión de sus futuros trabajos, las circunstancias en que una solución contractual *ad hoc* puede resultar adecuada para proteger a las personas en caso de transferencia de datos personales a un tercer país en que el nivel de protección no sea, en general, suficiente. El presente documento pretende servir de base para dicho examen.
La Directiva sobre protección de datos (95/46/CE) establece en su artículo 25.1 el principio con arreglo al cual sólo deben efectuarse transferencias de datos personales a terceros países si el país considerado ofrece un nivel adecuado de protección. El artículo 26.1 contiene una serie de excepciones a tal norma, que no se examinan en el presente documento. El objeto de éste es estudiar la posibilidad adicional de excepción al principio de "protección adecuada" del artículo 25 establecida en el artículo 26.2. Esta última disposición permite a un Estado miembro autorizar una transferencia o un conjunto de transferencias a un tercer país que no garantice una protección adecuada "cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos". Esta disposición especifica, asimismo, que "dichas garantías podrán derivarse, en particular, de cláusulas contractuales". Además, el artículo 26.4 faculta a la Comisión para declarar, de conformidad con el procedimiento previsto en el artículo 31, que determinadas cláusulas contractuales tipo ofrecen garantías suficientes, a efectos de lo dispuesto en el artículo 26.2.
La idea de utilizar un contrato para regular las transferencias internacionales de datos personales no proviene, obviamente, de la Directiva. Ya en 1992, el Consejo de Europa, la Cámara Internacional de Comercio y la Comisión Europea iniciaron conjuntamente un estudio del tema . Más recientemente, un número creciente de expertos y analistas, inspirados quizá por la referencia explícita de la Directiva, han comentado el uso de
contratos en estudios y artículos. Los contratos también han seguido utilizándose en el "mundo real" con el objeto de resolver los problemas de protección planteados por el envío de datos personales desde algunos Estados miembros de la UE. En Francia, se viene haciendo un uso extensivo de ellos desde finales de la década de los ochenta. En Alemania, el reciente caso de la "Bahncard", en el que estaba implicado Citibank, recibió una considerable publicidad

2. Utilización de contratos en las transmisiones de datos intracomunitarias.

Antes de examinar los requisitos que deben cumplir las cláusulas contractuales en el contexto de la transmisión de datos a terceros países, es importante aclarar la diferencia existente entre la situación de los países no comunitarios y la que prevalece dentro de la Comunidad. En este último caso, el contrato es el mecanismo utilizado para definir y regular el reparto de responsabilidades en materia de protección de datos, cuando en el tratamiento de los datos en cuestión interviene más de una entidad. De acuerdo con la Directiva, una entidad, el "responsable del tratamiento", debe asumir la responsabilidad principal por el cumplimiento de los principios sustantivos de protección de datos. La segunda entidad, el "encargado del tratamiento", sólo es responsable de la seguridad de los datos. Una entidad se considera responsable del tratamiento si está capacitada para decidir sobre la finalidad y los medios del mismo, en tanto que el encargado del tratamiento es simplemente el organismo que presta materialmente el correspondiente servicio. La relación entre ambos se rige por lo dispuesto en el artículo 17.3 de la Directiva, en el que se establece lo siguiente:

La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable
del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento.
- que las obligaciones del apartado 1 [las normas sustantivas sobre seguridad de los datos], tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

Se desarrolla así el principio general enunciado en el artículo 16, con arreglo al cual toda persona que esté bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, deberá abstenerse de procesar datos personales salvo cuando reciba instrucciones del responsable (o cuando lo exija la ley). En caso de transferencia de datos a terceros países, también intervendrá, en general, más de una entidad. En este caso, se establece una relación entre la entidad que transfiere los datos (el "remitente") y la que los recibe en el otro país (el "receptor"). En tal contexto, una de las finalidades del contrato debe seguir siendo la de determinar el reparto de responsabilidades entre ambas partes en lo que atañe a la protección de los datos. No obstante, el contrato no debe limitarse a ello: ha de ofrecer garantías adicionales a los interesados, puesto que el receptor del país no comunitario no está sujeto a una serie de normas de protección de datos obligatorias que proporcionen garantías adecuadas.

3. Objetivo de una solución contractual

En el contexto de las transferencias a terceros países, el contrato es, por consiguiente, un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Comunidad (y, por tanto, fuera del ámbito de aplicación de la Directiva y, de hecho, del marco general del Derecho comunitario 3), a un país en el que el nivel general de protección no es suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección general adecuada, incluyendo los elementos esenciales de la misma que no existan en una situación concreta determinada.

4. Requisitos específicos de una solución contractual

5. El punto de partida para analizar el significado de la expresión "garantías suficientes" utilizada en el artículo 26.2, es el concepto de "protección adecuada", que ya se desarrolló con cierto detenimiento en el documento de debate anteriormente mencionado. Este documento expone un planteamiento consistente en una serie de principios básicos para la protección de datos, junto con los tres requisitos siguientes: que el nivel de aplicación de estos principios en la práctica sea satisfactorio; que se ofrezca a las personas afectadas apoyo y asistencia en el ejercicio de sus derechos; y que quienes resulten perjudicados tengan a su disposición procedimientos de recurso apropiados cuando no se apliquen los principios.

i) *Normas sustantivas de protección de datos*

El primer requisito de una solución contractual es, pues, que obligue a las partes de la transferencia a garantizar que se aplique íntegramente el conjunto de principios básicos de protección de datos desarrollado en el documento de debate al tratamiento de los datos transferidos al país no comunitario. Dichos principios básicos son los siguientes:

1) **Delimitación de la finalidad del tratamiento**: los datos deben procesarse con una finalidad específica y únicamente deben utilizarse o comunicarse con posterioridad en la medida en que no sea incompatible con la finalidad de la transferencia. Las únicas excepciones a esta regla serían las necesarias en una sociedad democrática por alguno de los motivos enumerados en el artículo 13 de la Directiva (seguridad del Estado, investigación de delitos, etc.)

2) **Calidad y proporcionalidad de los datos**: los datos deben ser exactos y, en su caso, estar actualizados. Asimismo, deben ser adecuados, pertinentes y no excesivos con respecto a la finalidad que persiga su transferencia o su posterior tratamiento.
3) **Transparencia**: las personas deben ser informadas del objeto del tratamiento y de la identidad del responsable del mismo en el tercer país, así como de cualesquiera otros elementos que resulten necesarios por motivos de equidad. Las únicas excepciones permitidas deberían ajustarse al artículo 13 o el artículo 11.2 de la Directiva, que permite a los organismos que no hayan obtenido los datos directamente del interesado quedar exentas del requisito de facilitar información cuando ello resulte imposible o suponga un esfuerzo desproporcionado.
4) **Seguridad**: el responsable del tratamiento debe tomar cuantas medidas de seguridad de orden técnico y organizativo resulten adecuadas para hacer frente a los riesgos del tratamiento. Ninguna persona que esté bajo su autoridad, incluido el encargado del tratamiento, debe procesar datos salvo por orden de aquél.
5) **Derecho de acceso, rectificación y oposición**: el interesado debe tener derecho a obtener una copia de los datos que a él se refieran que sean objeto de tratamiento, así como a rectificar dichos datos cuando se demuestre que son inexactos. En determinadas situaciones, debe disfrutar asimismo de la posibilidad de oponerse al tratamiento de los datos. Las únicas excepciones a tales derechos deberían ser las que se derivan del artículo 13 de la Directiva.
6) **Restricciones sobre las transferencias posteriores a personas ajenas al contrato**: la transferencia de los datos personales del receptor a un tercero no debe permitirse, salvo si existe una forma de vincular por contrato a ese tercero y ofrecer las mismas garantías de protección de datos a los interesados. Además, en determinados casos, deben aplicarse los siguientes principios complementarios:

1) **Datos sensibles**: cuando se trate de datos de carácter "sensible" (es decir, que entren en las categorías enumeradas en el artículo 8), deberán preverse garantías adicionales, tales como la exigencia del consentimiento expreso del interesado.
2) *Marketing* directo: cuando los datos transferidos estén destinados a ser utilizados en operaciones de *marketing* directo, debe ofrecerse al interesado la posibilidad de optar en cualquier momento por que sus datos no se empleen con tales fines.
3) **Decisión individual automatizada**: cuando el objeto de la transferencia sea la adopción de una decisión automatizada, en el sentido de lo dispuesto en el artículo 15 de la Directiva, el interesado debe tener la posibilidad de conocer la lógica en la que se basa tal decisión, y han de tomarse otras medidas para salvaguardar sus intereses legítimos. El contrato debe estipular pormenorizadamente la forma en que el receptor de los datos transferidos ha de aplicar los anteriores principios (es decir, deben especificarse los fines de la transferencia, la categoría de los datos, el plazo límite de conservación, las medidas de seguridad, etc.). En circunstancias distintas, por ejemplo, cuando exista en el tercer país considerado una ley general de protección de datos similar a la Directiva, es probable que haya otros mecanismos por los que se precise la forma en que se aplican en la práctica las normas sobre protección de datos (códigos de conducta, notificación, función consultiva de la autoridad supervisora). En el caso de un contrato esto no es así. Por tanto, en el supuesto de que la transferencia se base en un contrato, los detalles son imprescindibles.

ii) Efectividad de las normas sustantivas

El documento de debate antes señalado fija tres criterios para evaluar la efectividad de un sistema de protección de datos, a saber:

1) Que el **nivel de cumplimiento de las normas** obtenido a través del sistema sea satisfactorio (ningún sistema puede garantizar la aplicación de las normas al 100%, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento son muy conscientes de sus obligaciones y los interesados, de sus derechos y de los medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es obvio, los procedimientos de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Que el sistema **ofrezca a los interesados apoyo y asistencia** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de estructura o mecanismo que permita investigar las quejas de forma independiente.

3) Que el sistema ofrezca a quienes resulten perjudicados **vías adecuadas de recurso**, en el caso de que no se observen las normas. Éste es un elemento clave. El sistema debe ofrecer la posibilidad de obtener una resolución imparcial y de que, en su caso, se paguen indemnizaciones y se impongan sanciones. Al evaluar la efectividad de una solución contractual deben aplicarse los mismos criterios, lo cual, como es obvio, resulta complicado, pero no imposible. Para ello es necesario hallar medios que permitan suplir la falta de mecanismos de supervisión y control y ofrecer a los interesados, que pueden no ser partes del contrato, apoyo y asistencia y, en última instancia, vías de recurso. Cada uno de estos aspectos debe examinarse detenidamente. Por motivos de facilidad, el análisis se ha realizado invirtiendo el orden de los mismos.

Vías de recurso a disposición de los interesados

Ofrecer a una persona un recurso legal (es decir, el derecho a exigir que un órgano independiente se pronuncie sobre su queja y a recibir, si procede, una indemnización), por medio de un contrato entre el "remitente" de los datos y su "receptor" no es cosa fácil.

Será, en gran parte, determinante la legislación nacional aplicable al contrato. Cabe suponer que, en general, la legislación aplicable será la del Estado miembro en el que esté establecido el remitente. La normativa contractual de algunos Estados miembros permite reconocer derechos a terceros, en tanto que, en otros Estados miembros, esto no es posible.

No obstante, por lo general, cuanto más limitadas sean las posibilidades del receptor de elegir los fines con los que puede procesar los datos, los medios y las condiciones para hacerlo, mayor será la seguridad jurídica para los interesados. Habida cuenta de que nos estamos refiriendo a casos en los que la protección general es inadecuada, la solución óptima consistiría en que el contrato especificara la forma en que el receptor debe aplicar los principios básicos de protección de datos con un grado de detalle suficiente para impedir que éste disponga, en la práctica, de una autonomía de decisión con respecto a los datos transferidos, o a la manera en que se procesarán posteriormente. El receptor vendrá obligado a seguir exclusivamente las instrucciones del remitente y, aun cuando los datos se hayan transferido materialmente fuera de la UE, la capacidad para tomar decisiones con respecto a los mismos seguirá correspondiendo a la entidad establecida en la Comunidad que haya efectuado la transferencia. El remitente seguirá siendo así el responsable del tratamiento, en tanto que el receptor será un simple subcontratista del tratamiento. En tales circunstancias, dado que los datos estarán bajo el control de una entidad establecida en un Estado miembro de la UE, el tratamiento realizado en el tercer país seguirá estando sujeto a la normativa de dicho Estado miembro 6 , y además el responsable del tratamiento continuará respondiendo, en virtud de la legislación de ese Estado, de los daños causados como consecuencia de un tratamiento ilegal de los datos. Este tipo de solución no dista mucho de la adoptada en el "Acuerdo interterritorial", por el que se resolvió el caso "Bahncard" de Citibank mencionado con anterioridad. En este caso, el acuerdo contractual fijó pormenorizadamente las condiciones de tratamiento de los datos, en particular las relacionados con la seguridad de los datos, excluyendo cualquier otro uso por el receptor.
De esta forma, el tratamiento de datos efectuado en el tercer país quedó sujeto a la legislación alemana y se garantizó a los interesados un recurso legal. Como es lógico, habrá casos en los que esta solución no será válida. Es posible que el receptor de los datos no preste simplemente un servicio de tratamiento al responsable radicado en la UE. De hecho, puede, por ejemplo, haber alquilado o comprado los datos para utilizarlos en su propio beneficio y con fines propios. En tales circunstancias, el receptor necesitará cierta libertad para procesar los datos como desee y se convertirá así de pleno derecho en "responsable del tratamiento".

Ante una situación semejante no es posible confiar en la aplicabilidad automática y continua de la legislación de un Estado miembro y en la permanente responsabilidad por daños del remitente de los datos. Deben idearse otros mecanismos más complejos para ofrecer al interesado un recurso legal adecuado. Como ya se ha mencionado antes, algunos ordenamientos jurídicos permiten conferir derechos a terceros en un contrato, lo cual podría servir para establecer derechos en favor de los interesados en un contrato abierto y público entre el remitente y el receptor. La situación del interesado mejoraría aún más si, dentro del contrato, las partes se comprometieran a someterse a un arbitraje vinculante en el supuesto de que el interesado impugnara su observancia de las disposiciones. Algunos códigos sectoriales autorreguladores incluyen tales mecanismos de arbitraje, por lo que cabe pensar en utilizar los contratos en conjunción con dichos códigos.

Otra posibilidad es que el remitente, por ejemplo, en el momento en que obtenga inicialmente los datos del interesado, celebre un contrato independiente con éste en el que se estipule que el remitente responderá de cualesquiera daños o

perjuicios que se deriven del incumplimiento por parte del receptor de los datos del conjunto de principios básicos acordados para la protección de los datos. De esta forma, el interesado dispondrá de una vía de recurso frente al remitente por las faltas cometidas por el receptor. Correspondería entonces al remitente iniciar una acción contra el receptor por ruptura de contrato, para recuperar las posibles indemnizaciones por daños que se hubiera visto obligado a pagar al interesado. Esta compleja solución tridireccional es posiblemente más factible de lo que puede parecer. El contrato con el interesado podría formar parte de las condiciones generales con arreglo a las cuales un banco o una agencia de viajes, por ejemplo, presta sus servicios a la clientela. Además tiene la ventaja de ser transparente: el interesado puede así tener pleno conocimiento de los derechos de que disfruta.

Por último, como alternativa al contrato con el interesado, cabría también pensar en la posibilidad de que los Estados miembros adoptasen disposiciones legales por las que se atribuyera a los responsables del tratamiento que transfirieran datos fuera de la Comunidad la continua responsabilidad por los daños causados como consecuencia de los actos del receptor de la transferencia.

Apoyo y asistencia a los interesados

Una de las mayores dificultades a las que se enfrentan las personas cuyos datos son transferidos a un país extranjero radica en su incapacidad para determinar la raíz de su problema concreto y, por tanto, en su imposibilidad de juzgar si se han aplicado correctamente las normas sobre protección de datos o si existen motivos para entablar una acción judicial. Por ello, una protección adecuada supone la existencia de algún tipo de mecanismo institucional que haga posible un examen independiente de las quejas. Los poderes de control e investigación de la autoridad supervisora de un Estado miembro se limitan al tratamiento de datos efectuado en el territorio de este último. Si los datos se transfieren a otro Estado miembro, el sistema de asistencia mutua entre autoridades de supervisión garantizará que se estudie correctamente la queja presentada por una persona en el primer Estado miembro. Si se transfieren a un tercer país, en la mayor parte de los casos no habrá tal garantía. La pregunta que debemos plantearnos es, pues, qué tipo de mecanismos compensatorios cabría idear en el supuesto de que la transferencia de datos se basara en un contrato.

Una posibilidad sería exigir sencillamente una cláusula contractual que confiriera a la autoridad supervisora del Estado miembro en el que estuviera establecido el remitente de los datos el derecho de controlar el tratamiento realizado por el encargado del mismo en el tercer país. En la práctica, y siempre que se considere oportuno, este control podría efectuarlo un agente (por ejemplo, una empresa de auditoría especializada) designado por dicha autoridad. Ahora bien, uno de los problemas que entraña este planteamiento es que la autoridad supervisora no suele ser parte en el contrato, por lo que, en algunos países, le resultaría imposible invocar tal cláusula para tener acceso al tratamiento. Otra posibilidad es que el receptor de los datos en el tercer país se comprometa jurídica y directamente con la autoridad supervisora del Estado miembro afectado a autorizar el acceso de la misma o de un agente designado en el supuesto de que existan sospechas de que se han incumplido los principios para la protección de los datos. Dentro de esta cláusula, podría exigirse también que las partes en la transferencia informaran a la autoridad supervisora de cualesquiera quejas recibidas de los interesados. De seguirse este planteamiento, la existencia del citado compromiso sería una condición previa para que pudiera autorizarse la transferencia de los datos. Sea cual sea la solución elegida, es difícil determinar con certeza si resulta oportuno, factible, o incluso viable desde el punto de vista de los recursos disponibles, que una autoridad supervisora de un Estado miembro asuma la responsabilidad de examinar y controlar el tratamiento de datos efectuado en un tercer país.

Nivel satisfactorio de cumplimiento de las normas

Aun cuando el interesado no presente una queja concreta ni tope con dificultades particulares, es necesario poder confiar en que las partes del contrato se atienen realmente a sus cláusulas. El inconveniente de la solución contractual radica en la dificultad de imponer sanciones por incumplimiento suficientemente serias como para producir el efecto disuasorio necesario para crear tal clima de confianza. Incluso en aquellos casos en que siga ejerciéndose un control efectivo sobre los datos desde dentro de la Comunidad, el receptor de la transferencia puede no estar sujeto directamente a ninguna penalización si procesa los datos sin atenerse a lo dispuesto en el contrato. Por el contrario, la responsabilidad recaería en el remitente de los datos establecido en la Comunidad, el cual tendría entonces que entablar una acción legal independiente contra el receptor para resarcirse de sus posibles pérdidas. Esta forma de responsabilidad indirecta podría no ser suficiente para inducir al receptor a cumplir el contrato al pie de la letra.

En tales circunstancias, es probable que, en la mayor parte de los casos, la solución contractual deba completarse, al menos, con la posibilidad de llevar a cabo de algún modo una verificación externa de las actividades de tratamiento del receptor, tal como una auditoría efectuada por un organismo de normalización o una empresa especializada.

5. El problema de la primacía del Derecho

Una de las dificultades específicas que plantea el enfoque contractual es la posibilidad de que las normas jurídicas generales del tercer país de que se trate obliguen al receptor de la transferencia, en determinadas circunstancias, a comunicar los datos personales a las autoridades (policiales, judiciales o fiscales, por ejemplo) y de que tales requisitos legales prevalezcan sobre todo contrato firmado por el encargado del tratamiento. En lo que respecta a los encargados del tratamiento en la Comunidad, esta posibilidad se contempla en el artículo 16 de la Directiva, con arreglo al cual éstos únicamente pueden procesar datos siguiendo las instrucciones del responsable del tratamiento, *salvo en virtud de un imperativo legal*. No obstante, de acuerdo con la Directiva, estas notificaciones de datos (que, por su naturaleza, persiguen fines incompatibles con los previstos al recabar los datos) deben limitarse a lo imprescindible para atender a los imperativos de orden público de las sociedades democráticas, enunciados en el artículo 13.1 de la Directiva. El artículo 6 del Tratado de Amsterdam garantiza también la salvaguarda de los derechos fundamentales establecidos en

el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. En terceros países, es posible que no siempre existan tales restricciones sobre la capacidad de los poderes públicos para exigir de las empresas y otros organismos que operen en su territorio la comunicación de datos personales.

Esta dificultad no es fácil de superar. Demuestra sencillamente las limitaciones de la solución contractual. En algunos casos, un contrato es un instrumento demasiado endeble para ofrecer garantías suficientes en relación con la protección de datos, y no deberían autorizarse las transferencias de datos a determinados países.

6. Consideraciones de carácter práctico de cara a la utilización de contratos

El anterior análisis demuestra la necesidad de que los contratos contengan cláusulas pormenorizadas y debidamente adaptadas a la transferencia de datos de que se trate. Esta necesidad de fijar detalladamente la finalidad y las condiciones concretas del tratamiento al que se someterán los datos transferidos no excluye la posibilidad de desarrollar un modelo estándar de contrato, pero supone que todo contrato basado en el mismo se adecue a las circunstancias particulares del caso. El análisis realizado indica también que existen serias dificultades de orden práctico para llevar a cabo investigaciones en relación con el incumplimiento de un contrato, cuando el tratamiento se efectúa fuera de la UE y cuando el país en cuestión no dispone de ningún tipo de organismo de supervisión. Si se añaden ambas consideraciones, podemos concluir que habrá situaciones en las que una solución contractual resulte adecuada, y otras en las que quizá un contrato no pueda ofrecer "garantías suficientes". Dada la necesidad de que el contrato se adapte rigurosamente a las particularidades de la transferencia, esta solución resultará especialmente adecuada en caso de transferencias de datos similares y repetitivas. Los problemas relacionados con la supervisión suponen que la solución contractual sea más eficaz cuando las partes del contrato sean grandes operadores que estén ya sometidos a inspección y regulación públicas. Las grandes redes internacionales, tales como las utilizadas para las transacciones con tarjetas de crédito y las reservas en líneas aéreas, presentan ambas características, por lo que, en este caso, los contratos pueden resultar de máxima eficacia. En tales circunstancias, podrían, incluso, completarse con convenios multilaterales que ofrezcan una mayor seguridad jurídica.
Del mismo modo, cuando las partes de la transferencia sean filiales o miembros del mismo grupo de empresas, es probable que aumenten considerablemente las posibilidades de investigar un eventual incumplimiento del contrato, dada la fuerte vinculación existente entre el receptor en el tercer país y el remitente establecido en la Comunidad. Otro caso en el que convendría claramente desarrollar soluciones contractuales es, por tanto, el de las transferencias efectuadas dentro de una misma empresa.

Principales conclusiones y recomendaciones

En la Comunidad se utilizan contratos para determinar el reparto de responsabilidades en materia de protección de datos entre el responsable del tratamiento y el subcontratista encargado de llevarlo a cabo. En el supuesto de que se utilice un contrato en relación con transferencias de datos a terceros países, debe esperarse mucho más del mismo: ha de ofrecer a la persona a la que se refieran los datos salvaguardas adicionales, puesto que el receptor establecido en el tercer país no está sujeto a una serie de normas obligatorias en la materia que garanticen un nivel de protección adecuado.

Para evaluar la idoneidad de las salvaguardas ofrecidas por una solución contractual debe partirse de la misma base que para evaluar el nivel general de protección en un tercer país. Una solución contractual debe contener todos los principios básicos para la protección de datos y ofrecer los medios necesarios para que pueda velarse por su observancia.

El contrato debe fijar pormenorizadamente la finalidad, los medios y las condiciones del tratamiento de los datos transferidos, así como la forma en que se aplicarán los principios básicos de protección de datos. Los contratos que limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma ofrecen una mayor seguridad jurídica. Por consiguiente, en la medida de lo posible, el contrato debería servir para atribuir al remitente de los datos un poder decisorio sobre el tratamiento efectuado en el tercer país.

Si el receptor disfruta de cierta autonomía en relación con el tratamiento de los datos transferidos, la situación es más compleja y es posible que un simple contrato entre las partes de la transferencia no siempre permita a las personas a las que se refieren los datos ejercer sus derechos. Puede resultar necesario un mecanismo por el cual el remitente establecido en la Comunidad conserve la responsabilidad por los daños que pudieran derivarse del tratamiento llevado a cabo en el tercer país.

El contrato debería excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente por el receptor a organismos no vinculados por el contrato, a menos que pueda obligarse a terceros mediante disposiciones contractuales a respetar los mismos principios de protección de datos.

La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación.

En el supuesto de que la persona a la que se refieren los datos tope con algún problema, como consecuencia, en su caso, del incumplimiento de las cláusulas sobre protección de datos contenidas en el contrato, resulta, en general, difícil asegurarse de que la queja del interesado se investiga convenientemente. Las autoridades supervisoras de los Estados miembros experimentarán dificultades de orden práctico a la hora de llevar a cabo tales indagaciones.

Las soluciones contractuales resultan probablemente más adecuadas para las grandes redes internacionales (tarjetas de crédito, reservas de billetes de avión), que se caracterizan por un elevado volumen de transferencias de datos similares y repetitivas, y por la existencia de un número relativamente reducido de grandes empresas que operan en sectores ya sujetos a supervisión y regulación públicas. Otro caso en el que la utilización de contratos presenta un potencial considerable es el de las transferencias de datos entre distintas sucursales o empresas del mismo grupo.

Los países en los que las prerrogativas con que cuentan los poderes públicos para acceder a la información son más amplias de lo que autorizan las normas sobre protección de los derechos humanos aceptadas a nivel internacional no constituyen un destino seguro para las transferencias basadas en cláusulas contractuales.

Bruselas, 28 de abril de 1998
Por el Grupo de Trabajo
El Presidente
P.J. HUSTINX

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre circulación de la información, Derecho de sociedades e información financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

XV D/5009/98 final
WP 10

Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales

Recomendación 1/98 sobre los sistemas informatizados de reserva de las líneas aéreas (SIR)

Aprobada por el Grupo de Trabajo el 28 de abril de 1998

Recomendación sobre los sistemas informatizados de reserva de las líneas aéreas (SIR)

EL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES.

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 19951 ,

Vistos el artículo 29 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su Reglamento Interno y, en particular, sus artículos 12 y 14,

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

INTRODUCCIÓN

En virtud de la letra b) del apartado 1 del artículo 6 de la Directiva 95/46/CE, los Estados miembros deben disponer que los datos personales sean "recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines"; de acuerdo con la letra e) de ese mismo apartado 1, los datos deben conservarse "en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente".El artículo 8 de la Directiva obliga a los Estados miembros a prohibir el tratamiento de datos personales que revelen, entre otras cosas, el origen racial o étnico, las opiniones políticas o el estado de salud. Pueden establecerse excepciones a este principio siempre que se ajusten a alguno de los supuestos enumerados en los apartados 2 y 3 del artículo 8, siendo uno de tales supuestos el que el interesado haya dado su consentimiento explícito.

Con arreglo a la Directiva, el interesado disfruta de una serie de derechos específicos, entre los que se incluyen el derecho a ser informado sobre el tratamiento de sus datos personales (artículos 10 y 11) y el derecho de acceso a los datos, de rectificación y supresión de los mismos (artículo 12).Habida cuenta de las características específicas de las reservas en líneas aéreas, y de las recientes iniciativas de la Comisión a este respecto2 , el Grupo de Trabajo decidió crear un subgrupo para los sistemas informatizados de reserva (SIR). El subgrupo se reunió en dos ocasiones y decidió someter los resultados de sus debates al Grupo de Trabajo con vistas a la adopción de la presente recomendación.

EXPOSICIÓN DE MOTIVOS

El sector del transporte aéreo se caracteriza por un uso muy desarrollado de los sistemas informáticos. Existen bases de datos que contienen datos personales en muchos contextos, y en particular en las compañías aéreas, las agencias de viajes y los sistemas informatizados de reserva. Algunas de las bases de datos (en particular, aunque no de forma exclusiva, las de los SIR) están ubicadas fuera de la Comunidad.

Dado el carácter internacional de la aviación, las soluciones de tipo general son, en principio, las más adecuadas. A

juicio del Grupo de Trabajo, deben considerarse previamente los siguientes aspectos:

1. Información y derecho de acceso:

– La mayor parte de los datos personales son recogidos por las agencias de viajes y las compañías aéreas. Por motivos de orden práctico, y sin perjuicio de la definición de "responsable del tratamiento" que figura en la Directiva 95/46/CE, el problema del derecho del interesado de acceder a sus datos debería, por tanto, resolverse principalmente a través de dichas partes.

– No obstante, determinados aspectos relacionados con el acceso pueden también regularse directamente a través del SIR, lo cual podría hacerse en el proyecto de Reglamento sobre el código de conducta de los SIR propuesto por la Comisión. El código de conducta para los sistemas informatizados de reserva confirma el derecho de los pasajeros a ser informados acerca de las circunstancias del tratamiento de datos. Convendría reforzar este derecho mediante la involucración de los abonados (p.ej., las agencias de viajes) y las compañías aéreas.

2. Supresión de los datos

– Es conveniente asegurarse de que los datos personales queden fuera de línea para el SIR en cuanto dejen de utilizarse a efectos del viaje.

– Si bien dichos datos pueden ser necesarios para la resolución de litigios y deben, por tanto, archivarse durante algún tiempo, deberían utilizarse exclusivamente con ese fin y destruirse con posterioridad. Ello no excluye la posibilidad de que los abonados y las compañías aéreas obtengan el consentimiento de las personas que viajan con frecuencia para procesar sus datos de acuerdo con lo dispuesto en la Directiva 95/46/CE.

CONCLUSIONES

Considerando lo anterior, el Grupo de Trabajo recomienda lo siguiente:

Que la propuesta de Reglamento por el que se modifica el Reglamento 2299/89 del Consejo, relativo a un código de conducta para los sistemas informatizados de reserva, se complete con las siguientes disposiciones:

– Una obligación clara de facilitar **información** al consumidor acerca del tratamiento de datos personales en el SIR. Esta información, que podría facilitarse, por ejemplo, mediante folletos estándar, debería incluir la denominación y dirección del vendedor del sistema, la finalidad del tratamiento, el plazo de conservación y los procedimientos por los cuales el interesado puede ejercer el derecho de acceso a los datos.

– La obligación para los abonados (p.ej., las agencias de viajes) y las compañías aéreas de obtener el consentimiento expreso de los interesados para recoger datos sensibles (pasajeros minusválidos, comidas aptas para musulmanes, etc.). Si el SIR incluye un sistema de expedición directa de billetes, el vendedor del sistema3 debería quedar sujeto a tal obligación.

– La obligación para las partes antes mencionadas de responder rápidamente a una solicitud de **acceso** presentada por un pasajero que desea ver sus propios datos.

– La exigencia para los SIR de que todos los datos personales obtenidos se archiven fuera de línea en un plazo no superior a 72 horas tras la conclusión del viaje4 y se destruyan en un plazo máximo de 3 años. El acceso a tales datos únicamente debe autorizarse a efectos de la resolución de litigios en materia de facturación. No obstante la obligación de destruir los datos en el plazo de 3 años, los datos personales podrán conservarse durante el tiempo que resulte necesario para zanjar una demanda de daños y perjuicios o para dar cumplimiento a un requisito legal (p.ej., normas contables y fiscales).

– La exigencia de que se efectúen las modificaciones oportunas para ampliar el ámbito de aplicación de la auditoría prevista en el artículo 21 bis.

Que se estudien, además, con carácter prioritario los problemas específicos planteados por las reservas en línea efectuadas al margen de los SIR (p.ej., agencias de viajes o compañías aéreas que expiden directamente billetes por Internet) y que la Comisión proponga sin demora soluciones adecuadas. A este respecto, se invita a la Comisión a precisar si la Directiva 97/66/CE5 es aplicable a este extremo y en qué medida.

Los destinatarios de la presente recomendación, aprobada por el Grupo de Trabajo el ....., son la Comisión Europea, el Parlamento Europeo, el Consejo de la Unión Europea y el Comité Económico y Social.

Bruselas, 28 de abril de 1998

Por el Grupo de Trabajo
El Presidente
P.J. HUSTINX

1 DO L 281 de 23.11.1995, p. 31.
2 Propuesta de Reglamento (CE) del Consejo por el que se modifica el Reglamento (CEE) nº 2299/89 del Consejo

relativo a un código de conducta para los sistemas informatizados de reserva (SIR); COM (97) 246 final de 9 de julio de 1997.
3 De acuerdo con la definición contenida en el código de conducta arriba mencionado, por "vendedor de sistemas" se entiende "una empresa que, junto con sus filiales, asegure la explotación o la comercialización de un sistema informatizado de reservas".
4 Tal como se indica en la exposición de motivos, el derecho de los abonados y las compañías aéreas a procesar datos sensibles relativos a sus clientes habituales en su propio sistema informático, con el consentimiento expreso de los interesados, no se ve alterado.
5 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 (DO L 24 de 30.1.1998, p. 1).

COMISIÓN EUROPEA
DIRECCCIÓN GENERAL XV

Mercado Interior y Servicios Financieros
Libre circulación de la Información, Derecho de Sociedades e Información Financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

XV D/5032/98
WP 11

Grupo de Trabajo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales

DICTAMEN 1/98
Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS)

Adoptado por el Grupo de Trabajo el 16 de junio de 1998

Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS) Dictamen del Grupo de Trabajo

El Proyecto de Plataforma de Preferencias de Privacidad (P3P por *Platform for Privacy Preferences*) concibe la privacidad informática y la protección de datos como algo que debe ser objeto de un acuerdo entre el usuario de Internet cuyos datos se recaban y el sitio Internet que registra dichos datos. La filosofía parte de la idea de que el usuario da su consentimiento para que un sitio Internet registre sus datos personales (el objetivo de la Norma de Perfiles Abierta -conocida por su sigla en inglés OPS por *Open Profiling Standard*- es garantizar la transmisión segura de un perfil normalizado de datos personales), a condición de que las prácticas en materia de privacidad informática declaradas por el sitio como, por ejemplo, el propósito para el cual se registran los datos y si estos datos se utilizan o no para fines secundarios o se pasan a terceros, satisfagan las exigencias del usuario. El Consorcio World Wide Web ha querido poner a punto un vocabulario único a través del cual se puedan articular las preferencias del usuario y las prácticas del sitio Internet. No se considera la posibilidad de adaptar este vocabulario a las necesidades y al contexto legislativo de regiones geográficas específicas. Sorprendentemente, dada la intención de que el P3P sea aplicable a escala mundial, el vocabulario no se ha elaborado tomando como referencia los niveles más elevados que se conocen en materia de protección de datos y de la intimidad, sino que ha intentado formalizar un modelo común de un nivel inferior.

Estas decisiones en materia de política informática hacen prever que la puesta en práctica de la P3P y de la OPS en la Unión Europea dará lugar a una serie de problemas concretos que se abordan a continuación. Es fundamental resolver estos aspectos si se quiere que la P3P y la OPS tengan una incidencia positiva en la protección de la intimidad y en el entorno en línea.

Una plataforma técnica para la protección de la intimidad no bastará por sí sola para proteger la intimidad personal en la Red. Es necesario aplicarla en un contexto de normas de protección de datos que sean ejecutables y deparen a todas las personas un nivel mínimo y no negociable de protección de la intimidad. Recurrir a la P3P y a la OPS sin que exista tal marco jurídico presenta el riesgo de pasar la responsabilidad básicamente al usuario necesitado de protegerse, una evolución que minaría el principio sentado internacionalmente de que el cumplimiento de los principios de la protección de datos incumbe al 'controlador de datos' (Directrices OCDE 1980, Convenio del Consejo de Europa nº 108 de 1981, Directrices NNUU 1990, Directivas comunitarias 95/46/CE y 97/66/CE). Tal inversión de responsabilidades también presupone un nivel de conocimientos sobre los riesgos que el tratamiento de datos entraña para la intimidad de las personas, algo que no resulta realista esperar de la mayoría de los ciudadanos.

Existe el riesgo de que la P3P, una vez puesta en práctica en la próxima generación de *software* de navegación, pueda llevar a los operadores radicados en la UE a creer erróneamente que podrían quedar eximidos de algunas de sus obligaciones legales (p.e. dar a los usuarios acceso a sus datos personales) si el usuario consiente en ello como parte de la negociación en línea. De hecho, las empresas, organizaciones y personas establecidas en la UE y que prestan servicios a través de Internet estarán obligados en cualquier caso a observar las normas fijadas en la Directiva sobre protección de datos 95/46/CE (incorporada en las respectivas legislaciones nacionales) en lo que respecta al registro y tratamiento de datos personales. Así pues, la P3P podría causar confusión no sólo entre los operadores en cuanto a sus obligaciones, sino también entre los usuarios de Internet en cuanto a la naturaleza de sus derechos de protección de datos. Por tanto, el *software* de navegación vendido o distribuido en la UE debe estar concebido y configurado de tal manera que resulten imposibles los acuerdos en línea contrarios a la legislación vigente en materia de protección de datos.

Para los usuarios radicados en la UE que entren en contacto con sitios Internet establecidos en países extracomunitarios, la preocupación principal es que la organización a la que comunican sus datos personales no esté sujeta a la directiva europea o a ninguna normativa de protección de datos efectivamente aplicada. El factor determinante para decidir si proporcionar o no datos a tales sitios será no sólo conocer el contenido aproximado de las normas aplicables sino también saber si en caso de incumplimiento existen sanciones y, lo más importante, si existe una vía de recurso simple y eficaz cuando alguien infrinja las normas. Teóricamente, una plataforma en línea dedicada a las preferencias de privacidad debería ser capaz de proporcionar tal información a los usuarios. No obstante, el vocabulario de la P3P tal como está constituido en este momento no exige -y ni siquiera permite- que se facilite a los usuarios información sobre sanciones y vías de recurso. Por consiguiente, para que la P3P pueda ser una herramienta útil para obtener en línea el consentimiento informado para las transferencias de datos personales de usuarios de la UE (como exige la letra a) del apartado 1 del artículo 26 de la Directiva), se hace necesario volver a examinar el vocabulario normalizado.

Dada la escasa probabilidad de que la mayoría de los usuarios de Internet modifiquen los parámetros preconfigurados de su navegador, la posición "por defecto" sobre las preferencias de privacidad de un usuario tendrá una enorme incidencia en el nivel general de protección de la intimidad en línea. La P3P y las OPS deben integrarse en la tecnología de navegación con posiciones por defecto que reflejen el interés del usuario por disfrutar de un nivel elevado de protección de su intimidad (incluida la capacidad de navegar por los sitios de la Red de forma anónima) sin verse bloqueado o sufrir molestias por su intento de acceder a los sitios. Cuando un operador exija que se le facilite un perfil de datos identificables como condición para acceder a su sitio Internet, habrá que pedir cada vez el consentimiento del usuario para proporcionar dicha información al sitio en cuestión. Cuando el sitio no requiera tal información, el acceso puede efectuarse sin solución de continuidad. Los principales fabricantes de *software* de navegación tienen la responsabilidad de aplicar la P3P y las OPS de forma que aumenten en lugar de disminuir los niveles de protección de la intimidad.

Dada la importancia del proceso de aplicación de la P3P y de la OPS, así como los diferentes asuntos que actualmente está examinando el Grupo de Trabajo en relación con la funcionalidad de los protocolos de web (HTTP), el Grupo de Trabajo anima a que se desarrolle un *software* de Internet que se ajuste a las normas en materia de protección de datos aplicables en la Unión Europea, y considera que sería apropiado poner a punto los mecanismos que permitan verificar la conformidad del *software* de Internet a este respecto.

Hecho en Bruselas, el 16 de junio de
1998
Por el Grupo de Trabajo
El Presidente
P.J. HUSTINX

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV

Mercado Interior y Servicios Financieros
Libre Circulación de la Información, Derecho de Sociedades e Información Financiera
Libre Circulación de la Información, protección de datos y sus aspectos internacionales

DG XV D/5025/98 WP 12
Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales
Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. Aprobado por el Grupo de Trabajo el 24 de julio de 1998 [versión española corregida]

Índice

Introducción p. 3
Capítulo 1 ¿Qué debe entenderse por "protección adecuada"? p. 5
Capítulo 2 Aplicación del enfoque a los países que han ratificado el Convenio 108 p. 9
Capítulo 3 Aplicación del enfoque a la autorregulación industrial p. 11
Capítulo 4 La función de las disposiciones contractuales p. 16
Capítulo 5 Excepciones al requisito de adecuación p. 26
Capítulo 6 Cuestiones de procedimiento p. 28
Anexo 1
Anexo 2
Ejemplos
Artículos 25 y 26

Introducción

El objetivo de este documento consiste en reunir el trabajo previamente realizado por el Grupo de Trabajo de los Comisarios para la Protección de Datos de la UE, creado al amparo del artículo 29 de la Directiva sobre protección de datos, en un conjunto de reflexiones más exhaustivo sobre todas las cuestiones centrales planteadas en las transferencias de datos personales a terceros países en el contexto de la aplicación de la Directiva sobre protección de datos

de la UE (95/46/CE). La estructura de este documento se ajusta al sistema utilizado en las transferencias internacionales de datos personales expuesto en los artículos 25 y 26 de la directiva. (Se ha incluido el texto de estos artículos en el Anexo 2).

El apartado 1 del artículo 25 establece el principio por el cual los Estados miembros sólo podrán permitir una transferencia si los terceros países en cuestión aseguran un nivel adecuado de protección. El apartado 2 declara que el "carácter adecuado" deberá evaluarse caso por caso "atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos". El apartado 6 dispone que la Comisión podrá declarar que ciertos países ofrecen una protección adecuada. El capítulo uno de este documento trata la cuestión central de la protección adecuada. Su objetivo es explicar lo que se entiende por "adecuada" y esboza un marco de cómo debe evaluarse el carácter adecuado de la protección en un caso concreto. La aplicación de este enfoque se trata más detalladamente en los capítulos dos y tres.

El capítulo dos se ocupa de las transferencias a países que han ratificado el Convenio 108 del Consejo de Europa, mientras que **el capítulo tres** evalúa las cuestiones que rodean las transferencias en las cuales la protección de datos personales se facilita principal o completamente mediante mecanismos de autorregulación y no por normas de Derecho.

A falta de una protección adecuada entendida según el artículo 25.2, la Directiva también contempla en el artículo 26.2 la posibilidad de medidas ad hoc, sobre todo de tipo contractual, que podrían dar lugar al establecimiento de garantías adecuadas sobre cuya base podrían realizarse las transferencias en cuestión. En **el capítulo cuatro** de este documento se examina en qué circunstancias las soluciones contractuales ad hoc pueden ser apropiadas y se mencionan algunas recomendaciones sobre la forma y el contenido posibles de dichas soluciones.

El capítulo cinco se ocupa de la tercera y última situación contemplada en la directiva: los grupos limitados de casos contenidos en el artículo 26.1 que incluyen efectivamente una excepción al requisito de "protección adecuada". Se examina el alcance exacto de estas excepciones, con ejemplos ilustrativos de los tipos de casos abarcables, junto con los que no parecen serlo.

Por último, **el capítulo seis** contiene algunos comentarios sobre cuestiones de procedimiento que surgen al juzgar el carácter adecuado (o inadecuado) de la protección y sobre la consecución de un enfoque coherente de estas cuestiones a escala comunitaria.

El anexo 1 comprende una serie de estudios ilustrativos que pretenden demostrar cómo puede aplicarse en la práctica el enfoque expuesto en este documento.

CAPÍTULO UNO: EVALUAR SI LA PROTECCIÓN ES ADECUADA

1) ¿Qué debe entenderse por "protección adecuada"?

El objetivo de la protección de datos es ofrecer protección a las personas cuyos datos son objeto de tratamiento. Normalmente, dicho objetivo se logra combinando los derechos del interesado y las obligaciones de quienes tratan los datos o controlan dicho tratamiento. Las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980) o en las directrices de la ONU (1990). Por eso, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince estados de la Comunidad.

Sin embargo, las normas de protección de datos sólo contribuyen a la protección de las personas físicas si efectivamente se cumplen en la práctica. Por ello es necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de dichas normas. En Europa, históricamente ha habido una tendencia a plasmar en el Derecho las normas de protección de datos, lo que ha permitido sancionar el incumplimiento y conceder a las personas físicas un derecho de reparación. Además, estas legislaciones han incluido en general otras normas de procedimiento como el establecimiento de autoridades de control con funciones de seguimiento e investigación de denuncias. Estos aspectos relativos al procedimiento están plasmados en la Directiva 95/46/CE, con sus disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones. Fuera del ámbito comunitario es menos común encontrar estos medios de procedimiento para asegurar el cumplimiento de las normas de protección de datos. Los signatarios del Convenio 108 deben incorporar los principios de la protección de datos en su legislación, pero no se requieren mecanismos complementarios tales como una autoridad de control. Las directrices de la OCDE sólo exigen que "se tengan en cuenta" en la legislación nacional y no prevén procedimientos para garantizar que las directrices resulten en una protección efectiva de las personas físicas. Por otro lado, las últimas directrices de la ONU sí incluyen disposiciones de control y sanciones, lo que refleja una creciente sensibilización a nivel mundial sobre la necesidad de aplicar debidamente las normas de protección de datos.

En este contexto, es evidente que todo análisis significativo de la protección adecuada debe comprender los dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz. Tomando la Directiva 95/46/CE como punto de partida, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección. Esta lista mínima no debería ser inamovible. En algunos casos será necesario ampliar la lista,

mientras que en otros incluso sea posible reducirla. El grado de riesgo que la transferencia supone para el 6 interesado será un factor importante para determinar los requisitos concretos de un caso determinado. A pesar de esta condición, la compilación de una lista básica de condiciones mínimas es un punto de partida útil para cualquier análisis.

i) **Principios de contenido:**Se sugiere la inclusión de los siguientes principios básicos:

1) **Principio de limitación de objetivos:** los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.

2) **Principio de proporcionalidad y de calidad de los datos:** los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) **Principio de transparencia:** debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2 y 13 de la Directiva.

4) **Principio de seguridad:** el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

5) **Derechos de acceso, rectificación y oposición:** el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

6) **Restricciones respecto a transferencias sucesivas a otros terceros países:** únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la directiva (estas excepciones se examinan en el capítulo cinco.) A continuación figuran ejemplos de principios adicionales que deben aplicarse a tipos específicos de tratamiento:

1) **Datos sensibles:** cuando se trate de categorías de datos "sensibles" (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.
2) **Mercadotecnia directa:** en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.
3) **Decisión individual automatizada:** cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

ii) Mecanismos del procedimiento/de aplicación:

En Europa existe un amplio consenso sobre la necesidad de plasmar los principios de la protección de datos en la legislación. También es amplio el consenso en que un sistema de "supervisión externa" en forma de una autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos. Sin embargo, en otras partes del mundo no siempre se encuentran estas características.

Con el fin de sentar las bases para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimientos judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o

arbitral y, en su caso, indemnizaciones y sanciones.

CAPÍTULO DOS: APLICACIÓN DEL ENFOQUE A LOS PAÍSES QUE HAN RATIFICADO EL CONVENIO 108 DEL CONSEJO DE EUROPA

El Convenio 108 es el único instrumento internacional existente con poder vinculante en el área de la protección de datos, aparte de la Directiva. La mayoría de los signatarios del Convenio también son Estados miembros de la Unión Europea (actualmente cuenta con la ratificación de los 15) o países, como Noruega e Islandia, donde en cualquier caso la Directiva es vinculante en virtud del acuerdo del Espacio Económico Europeo. Sin embargo, Eslovenia, Hungría y Suiza también han ratificado el Convenio, y es posible que otros terceros países lo hagan en el futuro, en particular porque el Convenio también está abierto a países no pertenecientes al Consejo de Europa. Por tanto, examinar si es posible considerar que los países que han ratificado el Convenio ofrecen un nivel adecuado de protección en el sentido del artículo 25 de la Directiva, es interesante no sólo por motivos académicos.

Como punto de partida, es útil examinar el propio texto del Convenio a la luz del esbozo teórico de la "protección adecuada" expuesta en el capítulo uno de este documento. Respecto al contenido de los principios básicos, puede decirse que el Convenio incluye las cinco primeras de las seis "condiciones mínimas". El Convenio también incluye el requisito de una protección adecuada para los datos sensibles, la cual será requisito de adecuación cuando se trate de tales datos.

Un elemento ausente en el Convenio, desde el punto de vista del contenido de sus normas sustantivas, son las restricciones a las transferencias a países no signatarios del Convenio. Esta carencia supone el riesgo de que un país signatario del Convenio 108 pueda utilizarse como "escala" en una transferencia de datos de la Comunidad a otro tercer país con niveles de protección absolutamente insuficientes.

El segundo aspecto de la "protección adecuada" se refiere a los mecanismos de procedimiento instaurados para asegurar que los principios básicos resulten eficaces. El Convenio exige que sus principios se plasmen en legislaciones nacionales y que se establezcan sanciones y remedios apropiados en caso de violación de estos principios. Estas medidas deberían bastar para garantizar un nivel razonable de cumplimiento de las normas y una reparación adecuada para los interesados en caso de incumplimiento de las normas (objetivos 1) y 3) de un sistema de cumplimiento de la protección de datos). No obstante, el Convenio no obliga a las partes contratantes a establecer mecanismos institucionales que permitan la investigación independiente de las quejas, aunque en general los países que lo han ratificado así lo han hecho en la práctica. Esto es un punto flaco porque, sin estos mecanismos institucionales, no se garantiza el apoyo y la asistencia prestados a las personas cuyos datos son objeto de tratamiento en el ejercicio de sus derechos (objetivo 2).

Este breve análisis parece indicar que es posible permitir la mayoría de las transferencias de datos personales a países que han ratificado el Convenio 108 al amparo del artículo 25.1 de la Directiva a condición de que - el país en cuestión también disponga de mecanismos adecuados para garantizar el cumplimiento, ayudar a las personas físicas y facilitar la reparación (como, por ejemplo, una autoridad de control independiente dotada de las competencias apropiadas); y - el país en cuestión sea el destino final de la transferencia y no un país intermediario a través del cual transitan los datos, excepto cuando las transferencias sucesivas se dirigen de nuevo a la UE o a otro destino que ofrezca una protección adecuada. Evidentemente, este es un examen bastante simplificado y superficial del Convenio. Los casos específicos de las transferencias de datos a los países signatarios del Convenio pueden plantear nuevos problemas que no se han tratado en este documento.

CAPÍTULO TRES: APLICACIÓN DEL ENFOQUE A LA AUTORREGULACIÓN INDUSTRIAL

Introducción

El artículo 25.2 de la Directiva sobre protección de datos (95/46/CE) establece que el nivel de protección que ofrece un tercer país se evaluará atendiendo a *todas las circunstancias* que concurran en una transferencia o en una categoría de transferencias de datos. Se hace referencia específica no sólo a las normas de Derecho, sino también a "las normas profesionales y las medidas de seguridad en vigor en dichos países." El texto de la Directiva exige por lo tanto que se tengan en cuenta las normas no jurídicas que puedan existir en el tercer país en cuestión, siempre que estas normas *se cumplan*. En este contexto debe evaluarse la función de la autorregulación industrial.

¿Qué es la autorregulación?

El término "autorregulación" puede significar cosas distintas para diferentes personas. A efectos del presente documento, deberá entenderse por código de autorregulación (u otro instrumento) cualquier conjunto de normas de protección de datos aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por los miembros del sector industrial o profesión en cuestión.

Esta es una definición amplia que abarcaría desde un código de protección de datos voluntario elaborado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos y banqueros, que a menudo tienen una fuerza cuasi judicial.

¿Es el organismo responsable del código representativo del sector?

Tal como sostendrá este capítulo, un importante criterio para juzgar el valor de un código es su fuerza ejecutiva. En este contexto, la cuestión de si la asociación u organismo responsable del código representa a todos los operadores del sector o únicamente a un pequeño porcentaje de éstos tiene probablemente menos importancia que la fuerza de la asociación en cuanto a su capacidad para imponer sanciones a sus miembros por incumplimiento del código, por ejemplo. No obstante, existen diversas razones secundarias que hacen que los códigos aplicables a todo un sector industrial o a toda una profesión sean instrumentos de protección más útiles que los elaborados por pequeñas agrupaciones de empresas dentro de un sector industrial. En primer lugar figura el hecho de que un sector industrial fragmentado y caracterizado por diversas asociaciones rivales, cada una con su propio código de protección de datos, resulta confuso para el consumidor. La coexistencia de varios códigos diferentes crea un panorama opaco para las personas cuyos datos son objeto de tratamiento. En segundo lugar, especialmente en sectores tales como la mercadotecnia directa, donde es práctica corriente transferir los datos personales entre diferentes empresas del mismo sector, pueden surgir situaciones en que la empresa que transmita datos personales no esté sujeta al mismo código de protección de datos que la empresa receptora. Esto supone una gran fuente de ambigüedad en cuanto a la naturaleza de las normas aplicables, y también puede dificultar en gran medida la investigación y resolución de las denuncias de los interesados.

Evaluación de la autorregulación - el enfoque más adecuado

Dada la gran variedad de instrumentos que entran dentro del concepto de autorregulación, está claro que existe una necesidad de diferenciar entre las diversas formas de autorregulación por su impacto real en el nivel de la protección de datos aplicable cuando se transfieran datos personales a un tercer país.

El punto de partida para la evaluación de cualquier conjunto específico de normas sobre protección de datos (tengan éstas categoría de autorregulación o de norma legal) debe ser el enfoque general establecido en el capítulo uno de este documento. La piedra angular de este enfoque es el examen no sólo del contenido del instrumento (deberá contener una serie de principios básicos) sino también de su eficacia para lograr:
- un buen nivel de cumplimiento general,
- apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento,
- una reparación adecuada (incluida la compensación, cuando corresponda).

Evaluación del contenido de un instrumento de autorregulación

Esta es una tarea relativamente sencilla. Se trata de garantizar que estén presentes los "principios de contenido" expuestos en el capítulo uno. Es una evaluación objetiva. Se trata de ver cuál es el contenido del código, y no de cómo se elaboró. El hecho de que un sector industrial o profesión haya desempeñado una función primordial en el desarrollo del contenido de un código no es relevante por sí mismo, aunque evidentemente, si en su desarrollo se han tenido en cuenta las opiniones de las personas cuyos datos son objeto de tratamiento y de las organizaciones de consumidores, es más probable que el código refleje fielmente los principios básicos necesarios para la protección de datos.

La transparencia del código es un elemento crucial; en particular, el código debería
redactarse en lenguaje sencillo y ofrecer ejemplos concretos que ilustren sus disposiciones.

Además, el código debería prohibir la transferencia de datos a empresas que no pertenezcan al sector y que no se rijan por el código, a menos que se prevean otras protecciones adecuadas.

Evaluación de la eficacia de un instrumento de autorregulación

La evaluación de la eficacia de un código o instrumento concreto de autorregulación es un ejercicio más difícil, que exige la comprensión de los métodos y formas para garantizar la adhesión al código y para resolver los problemas de incumplimiento. Es necesario que se cumplan los tres criterios funcionales de eficacia de la protección para considerar que un código de autorregulación proporciona una protección adecuada.

Un buen nivel de cumplimiento general:

Típicamente, un código profesional o industrial será desarrollado por un organismo representativo del sector industrial o profesión en cuestión, y se aplicará a los miembros de dicho organismo representativo específico. El nivel de cumplimiento del código dependerá del grado de conocimiento de la existencia del código y su contenido por parte de sus miembros, de las medidas que se adopten para garantizar la transparencia del código a los consumidores con el fin de permitir a las fuerzas del mercado realizar una contribución eficaz, de la existencia de un sistema de control externo (tal como la exigencia de una auditoría de su cumplimiento a intervalos periódicos) y, quizá lo más importante, de la naturaleza y la aplicación de las sanciones en caso de incumplimiento.
Por tanto, son importantes las siguientes preguntas:

- ¿Qué medidas adopta el organismo representativo para asegurarse de que sus miembros conocen el código?
- ¿Exige el organismo representativo a sus miembros pruebas de que aplican las disposiciones del código? ¿Con qué frecuencia?
- ¿Presentan dichas pruebas las propias empresas o proceden de una fuente exterior (tal como un auditor acreditado)?
- ¿Investiga el organismo representativo las supuestas o presuntas violaciones del código?
- ¿Es el cumplimiento del código una condición para formar parte del organismo representativo o es dicho cumplimiento meramente "voluntario"?
- En caso de que un miembro viole el código, ¿con qué tipos de sanciones disciplinarias cuenta el organismo representativo (expulsión u otras)?

- ¿Es posible para una persona o empresa continuar trabajando en la profesión o sector industrial concreto después de haber sido expulsado del organismo representativo?
- ¿Puede hacerse cumplir el código de otras maneras, por ejemplo en los tribunales o en un tribunal especializado? Los códigos profesionales tienen fuerza legal en algunos países. En algunas circunstancias, también puede ser posible recurrir a las leyes generales relativas a prácticas comerciales correctas o incluso de competencia para conseguir el cumplimiento de los códigos de conducta de los sectores industriales.

Al examinar los tipos de sanciones existentes, es importante distinguir entre una sanción "reparadora" que, en caso de incumplimiento, únicamente exige al responsable del tratamiento la modificación de sus prácticas con el fin de adecuarlas a lo establecido en el código, y una sanción que vaya más lejos, castigando al responsable por su incumplimiento. Sólo esta segunda categoría de sanción "punitiva" tiene repercusión en el comportamiento futuro de los responsables del tratamiento al proporcionar un incentivo para que se cumpla sistemáticamente el código.

La falta de sanciones auténticamente disuasorias y punitivas es, por lo tanto, una carencia importante en un código. Sin dichas sanciones, es difícil entender cómo puede lograrse un nivel satisfactorio de cumplimiento general, a no ser que se establezca un sistema riguroso de control exterior (como una autoridad pública o privada competente para intervenir en caso de incumplimiento del código, o una exigencia obligatoria de realizar auditorías externas a intervalos periódicos).

Apoyo y ayuda a las personas cuyos datos sean objeto de tratamiento:

Un requisito esencial para un sistema de protección de datos adecuado y eficaz es que no se abandone a las personas que se enfrentan a un problema relativo a sus datos personales, sino que se les proporcione un apoyo institucional que permita resolver sus dificultades. Este apoyo institucional debería, idealmente, ser imparcial, independiente y poseer los poderes necesarios para investigar cualquier denuncia de un interesado. A este respecto, las preguntas que deben formularse respecto de la autorregulación son las siguientes:

- ¿Existe un sistema que permita la investigación de las denuncias de los interesados?
- ¿Cómo se da a conocer a los interesados este sistema y las decisiones adoptadas en cada caso concreto?
- ¿Supone el sistema costes para el interesado?
- ¿Quién realiza la investigación? ¿Tiene los poderes necesarios?
- ¿Quién juzga sobre una supuesta violación del código? ¿Es independiente e imparcial?

La imparcialidad del árbitro o juez sobre una supuesta violación de un código es un punto clave. Claramente, dicha persona u organismo deberá ser independiente respecto al responsable del tratamiento. No obstante, esto por sí mismo no basta para garantizar la imparcialidad. Idealmente, el árbitro debería asimismo ser ajeno a la profesión o sector en cuestión, dado que los miembros de una misma profesión o sector tienen una clara comunidad de intereses con el responsable del tratamiento que supuestamente haya infringido el código. A falta de esto, la neutralidad del órgano de decisión podría garantizarse incluyendo a representantes de los consumidores (en igual número) junto a los representantes del sector.

Reparación adecuada

Probada la infracción del código de autorregulación, deberá existir un recurso para el interesado. Este recurso deberá solucionar el problema (por ejemplo, corregir o suprimir datos incorrectos, o garantizar que cese el tratamiento con objetivos incompatibles) y, si se ha producido un perjuicio al interesado, prever el pago de una compensación adecuada. Hay que tener en cuenta que "perjuicio" en el sentido de la Directiva sobre protección de datos incluye no sólo el daño físico y la pérdida financiera, sino también cualquier daño psicológico o moral que se cause (llamado "distress" en el Derecho del Reino Unido y de EEUU).

Muchas de las cuestiones relativas a las sanciones que se han enumerado en la sección "Un buen nivel de cumplimiento general" son pertinentes aquí. Tal y como se ha explicado anteriormente, las sanciones tienen una doble función: castigar al infractor (y fomentar así el cumplimiento de las normas por parte del infractor y de los demás), y remediar una violación de las normas. Nos ocuparemos ahora de la segunda función. Por lo tanto, podrían plantearse también las siguientes preguntas:

- ¿Es posible comprobar si un miembro que haya violado el código, ha modificado después sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación en virtud del código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una ruptura de contrato, o es susceptible de sanción en virtud del Derecho público (por ejemplo, protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

Conclusiones

La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el capítulo uno.
Para que un instrumento de autorregulación pueda considerarse un elemento válido de "protección adecuada", debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
El instrumento debe ser transparente e incluir el contenido básico de los principios
esenciales de la protección de datos.

El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograrlo es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada.

- ¿Es posible comprobar si un miembro que haya violado el código, ha modificado después sus prácticas y solucionado el problema?
- ¿Pueden los interesados obtener compensación en virtud del código, y en caso afirmativo, de qué manera?
- ¿Equivale la violación del código a una ruptura de contrato, o es susceptible de sanción en virtud del Derecho público (por ejemplo, protección de los consumidores, competencia desleal), y puede la jurisdicción competente conceder indemnización por daños y perjuicios sobre dicha base?

Conclusiones

La autorregulación debería evaluarse utilizando el enfoque funcional y objetivo establecido en el capítulo uno.
Para que un instrumento de autorregulación pueda considerarse un elemento válido de "protección adecuada", debe ser vinculante para todos los miembros a quienes se transfieran los datos personales y proporcionar una protección adecuada si los datos se transfieren a terceros.
El instrumento debe ser transparente e incluir el contenido básico de los principios
esenciales de la protección de datos.
El instrumento debe tener mecanismos que garanticen de forma eficaz un nivel satisfactorio de cumplimiento general. Una forma de lograrlo es el establecimiento de un sistema de sanciones disuasorias y punitivas. Otro sistema son las auditorías externas obligatorias.
El instrumento debe proporcionar apoyo y ayuda a los interesados que se enfrenten a un problema relativo al tratamiento de sus datos personales. Por ello, debe existir un órgano independiente, imparcial y de fácil acceso que acoja las denuncias de los interesados y resuelva sobre las violaciones del código.
El instrumento deberá garantizar una reparación adecuada en caso de incumplimiento. Los interesados deberán poder obtener una reparación de su problema y una compensación adecuada para definir y regular el reparto de responsabilidades en materia de protección de datos, cuando en el tratamiento de los datos en cuestión interviene más de una entidad.
De acuerdo con la Directiva, una entidad, el "responsable del tratamiento", debe asumir la responsabilidad principal del cumplimiento de los principios sustantivos de protección de datos. La segunda entidad, el "encargado del tratamiento", sólo es responsable de la seguridad de los datos. Una entidad se considera responsable del tratamiento si está capacitada para decidir sobre la finalidad y los medios del mismo, en tanto que el encargado del tratamiento es simplemente el organismo que presta materialmente el correspondiente servicio. La relación entre ambos se rige por lo dispuesto en el artículo 17.3 de la Directiva, en el que se establece lo siguiente:

La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:
- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento
- que las obligaciones del apartado 1 (las normas sustantivas sobre seguridad de los datos), tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

Se desarrolla así el principio general enunciado en el artículo 16, con arreglo al cual toda persona que esté bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, deberá abstenerse de procesar datos personales salvo cuando reciba instrucciones del responsable (o cuando lo exija la ley).

En caso de transferencia de datos a terceros países, también intervendrá, en general, más de una entidad. En este caso, se establece una relación entre la entidad que transfiere los datos (el "remitente") y la que los recibe en el otro país (el "receptor").

En tal contexto, una de las finalidades del contrato debe seguir siendo la de determinar el reparto de responsabilidades entre ambas partes en lo que atañe a la protección de datos. No obstante, el contrato no debe limitarse a ello: ha de ofrecer garantías adicionales para los interesados, por el hecho de que el receptor del país no comunitario no está sujeto a una serie de normas obligatorias de protección de datos que proporcionen garantías adecuadas.

3. Objetivo de una solución contractual

En el contexto de las transferencias a terceros países el contrato es, por consiguiente, un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Comunidad (y, por tanto, fuera del ámbito de aplicación de la Directiva y, de hecho, del marco general del Derecho comunitario 9), a un país en el que el nivel general de protección no sea suficiente. Para que una cláusula contractual pueda cumplir esta función, debe compensar de manera satisfactoria la ausencia de una protección general adecuada mediante inclusión de los elementos esenciales de la misma que no existen en una situación determinada.

4. Requisitos específicos de una solución contractual

El punto de partida para analizar el significado de la expresión "garantías suficientes" utilizada en el artículo 26.2 es el concepto de "protección adecuada", que ya se desarrolló con cierto detenimiento en el capítulo uno. Éste consiste en una serie de principios básicos para la protección de datos, junto con ciertas condiciones necesarias para asegurar su eficacia.

i) *Normas sustantivas de protección de datos*

El primer requisito de una solución contractual es, pues, que obligue a las partes de la transferencia a garantizar que se aplique íntegramente el conjunto de principios básicos de protección de datos, desarrollado en el capítulo uno, al tratamiento de los datos transferidos al país no comunitario. Dichos principios básicos son los siguientes:

- principio de limitación de objetivos
- principio de proporcionalidad y de calidad de los datos
- principio de transparencia
- principio de seguridad
- derecho de acceso, rectificación y oposición
- restricciones respecto a transferencias sucesivas a personas ajenas al contrato. Además, en determinados casos deben aplicarse los principios complementarios relativos a los datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas.

El contrato debe estipular minuciosamente la forma en que el receptor de los datos transferidos ha de aplicar los anteriores principios (es decir, deben especificarse los fines de la transferencia, las categorías de los datos, el plazo límite de conservación, las medidas de seguridad, etc.). En circunstancias distintas, por ejemplo cuando exista en el tercer país considerado una ley general de protección de datos similar a la Directiva, es probable que existan otros mecanismos por los que se precise la forma en la que se aplican, en la práctica, las normas sobre protección de datos (códigos de conducta, notificación, función consultiva de la autoridad supervisora). En el caso de un contrato esto no es así. Por tanto, en el supuesto de que la transferencia se base en un contrato, los detalles son imprescindibles.

ii) *Efectividad de las normas sustantivas*

El capítulo uno fija tres criterios para evaluar la efectividad de un sistema de protección de datos. Estos criterios son la capacidad del sistema para:

- ofrecer un **nivel satisfactorio de cumplimiento**de las normas
- facilitar **apoyo y asistencia a los interesados** en el ejercicio de sus derechos
- y, como elemento clave, proporcionar **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas.

Al evaluar la efectividad de una solución contractual, deben aplicarse los mismos criterios. Esto, como es natural, resulta complicado, pero no imposible. Para ello es necesario hallar medios que permitan suplir la falta de mecanismos de supervisión y aplicación, y ofrecer a los interesados, que pueden no ser partes del contrato, apoyo y asistencia y, en última instancia, vías de recurso.

Cada uno de estos aspectos debe examinarse detenidamente. Para facilitar el análisis, se han tomado invirtiendo el orden de los mismos.

Vías de recurso a disposición de los interesados

Ofrecer a una persona un recurso legal (es decir, el derecho a exigir que un árbitro independiente se pronuncie sobre su denuncia y a recibir, si procede, una indemnización), por medio de un contrato entre el "remitente" de los datos y su "receptor", no es cosa fácil. Será, en gran parte, determinante el tipo de normativa contractual elegida como legislación nacional aplicable al contrato. Cabe suponer que, en general, la legislación aplicable será la del Estado miembro en el que esté establecido el remitente. La normativa contractual de algunos Estados miembros permite reconocer derechos a terceros, en tanto que, en otros Estados miembros, esto no es posible.

Como regla general, cuanto más limitadas sean las posibilidades del receptor de elegir los fines, los medios y las condiciones con los cuales puede procesar los datos, mayor será la seguridad jurídica para los interesados. Teniendo en cuenta que nos estamos refiriendo a casos en los que la protección general es inadecuada, la solución óptima consistiría en que el contrato impidiera que el receptor disponga de una autonomía de decisión con respecto a los datos transferidos o a la manera en que se procesarán posteriormente. El receptor vendrá obligado a seguir exclusivamente las instrucciones del remitente y, aun cuando los datos se hayan transferido materialmente fuera de la UE, la capacidad para tomar decisiones con respecto a los mismos seguirá correspondiendo a la entidad establecida en la Comunidad que haya efectuado la transferencia. El remitente seguirá siendo así el responsable del tratamiento, en tanto que el receptor será un simple subcontratista del tratamiento. En tales circunstancias, dado que los datos estarán bajo el control de una entidad establecida en un Estado miembro de la UE, el tratamiento realizado en el tercer país seguirá estando sujeto a la normativa de dicho Estado miembro, y además el responsable del tratamiento continuará respondiendo, en virtud de la legislación de ese Estado, de los daños causados como consecuencia de un tratamiento ilegal de los datos. Este tipo de solución no dista mucho de la adoptada en el "Acuerdo Interterritorial", por el que se resolvió el caso "Bahncard" de Citibank mencionado con anterioridad. En este caso, el acuerdo contractual fijó pormenorizadamente las condiciones de tratamiento de los datos, en particular las relacionadas con la seguridad de los mismos, excluyendo cualquier otro uso por el receptor. De esta forma, el tratamiento de datos efectuado en el tercer país quedó

sujeto a la legislación alemana y se garantizó a los interesados un recurso legal. Como es lógico, habrá casos en los que esta solución no será válida.
Es posible que el receptor de los datos no preste simplemente un servicio de tratamiento al responsable radicado en la UE. De hecho, puede, por ejemplo, haber alquilado o comprado los datos para utilizarlos en su propio beneficio y con fines propios. En tales circunstancias, el receptor necesitará libertad para procesar los datos como desee y se convertirá así de pleno derecho en "responsable del tratamiento".

Ante una situación semejante, no es posible confiar en la aplicabilidad automática y continua de la legislación de un Estado miembro y en la permanente responsabilidad por daños del remitente de los datos. Deben idearse otros mecanismos más complejos para ofrecer al interesado un recurso legal adecuado. Como ya se ha mencionado antes, algunos ordenamientos jurídicos permiten conferir derechos a terceros en un contrato, lo cual podría servir para establecer derechos en favor de los interesados en un contrato abierto y público entre el remitente y el receptor. La situación del interesado mejoraría aún más si, dentro del contrato, las partes se comprometieran a someterse a un arbitraje vinculante en el supuesto de que el interesado impugnara su observancia de las disposiciones. Algunos códigos sectoriales autorreguladores incluyen tales mecanismos de arbitraje, por lo que cabe pensar en utilizar los contratos en conjunción con dichos códigos.

Otra posibilidad es que el remitente, por ejemplo en el momento en que obtenga inicialmente los datos del interesado, celebre un contrato independiente con éste en el que se estipule que el remitente responderá de cualesquiera daños y perjuicios que se deriven del incumplimiento, por parte del receptor de los datos, del conjunto de principios básicos acordados para la protección de los datos. De esta forma, el interesado dispondrá de una vía de recurso frente al remitente por las faltas cometidas por el receptor. Correspondería entonces al remitente iniciar una acción contra el receptor por ruptura de contrato, para recuperar las posibles indemnizaciones por daños y perjuicios que se hubiera visto obligado a pagar al interesado.

Esta compleja solución tridireccional es posiblemente más factible de lo que pueda parecer. El contrato con el interesado podría formar parte de las condiciones generales con arreglo a las cuales un banco o una agencia de viajes, por ejemplo, presta sus servicios a la clientela. Además, tiene la ventaja de ser transparente: el interesado puede así tener pleno conocimiento de los derechos de que disfruta.

Por último, como alternativa al contrato con el interesado, cabría también pensar en la posibilidad de que los Estados miembros adoptasen disposiciones legales por las que se atribuyera a los responsables del tratamiento que transfirieran datos fuera de la Comunidad la responsabilidad continuada por los perjuicios causados como consecuencia de los actos del receptor de la transferencia.

Apoyo y asistencia a los interesados

Una de las mayores dificultades a las que se enfrentan las personas cuyos datos son transferidos a un país extranjero radica en su incapacidad para determinar la raíz de su problema concreto, y, por tanto, en su imposibilidad de juzgar si se han aplicado correctamente las normas sobre protección de datos o si existen motivos para entablar una acción judicial.14 Por ello, una protección adecuada supone la existencia de algún tipo de mecanismo institucional que haga posible un examen independiente de las denuncias.

Los poderes de control e investigación de la autoridad supervisora de un Estado miembro se limitan al tratamiento de datos efectuado en el territorio de este último. Si los datos se transfieren a otro Estado miembro, el sistema de asistencia mutua entre autoridades de supervisión garantizará que se estudie debidamente la denuncia presentada por una persona en el Estado miembro. Si se transfieren a un tercer país, en la mayor parte de los casos no habrá tal garantía. La pregunta que debemos plantearnos es, pues, qué tipo de mecanismos compensatorios cabría idear en el supuesto de que la transferencia de datos se basara en un contrato.

Una posibilidad sería exigir sencillamente una cláusula contractual que confiriera a la autoridad supervisora del Estado miembro en el que estuviera establecido el remitente de los datos el derecho de inspeccionar el tratamiento realizado por el encargado del mismo en el tercer país. En la práctica, y siempre que se considere oportuno, esta inspección podría efectuarla un agente (por ejemplo, una empresa de auditoría especializada) designado por dicha autoridad. Ahora bien, uno de los problemas que entraña este planteamiento es que la autoridad supervisora no suele ser parte en el contrato, por lo que, en algunos países, le resultaría imposible invocar tal cláusula para tener acceso al tratamiento. Otra posibilidad es que el receptor de los datos en el tercer país se comprometa jurídica y directamente con la autoridad supervisora del Estado miembro afectado a autorizar el acceso de la misma o de un agente designado cuando existan sospechas de que se han incumplido los principios de la protección de datos.

Dentro de esta cláusula, podría exigirse también que las partes en la transferencia informaran a la autoridad supervisora de cualesquiera quejas recibidas de los interesados. De seguirse este planteamiento, la existencia del citado compromiso sería una condición previa para que pudiera autorizarse la transferencia de los datos. Sea cual sea la solución elegida, es difícil determinar con certeza si resulta oportuno, práctico, o incluso viable desde el punto de vista de los recursos disponibles, que una autoridad supervisora de un Estado miembro de la UE asuma la responsabilidad de examinar e inspeccionar el tratamiento de los datos efectuado en un tercer país.

Nivel satisfactorio de cumplimiento

Aun cuando el interesado no presente una queja concreta ni tope con dificultades particulares, es necesario poder confiar en que las partes del contrato se atienen realmente a sus cláusulas. El inconveniente de la solución contractual

radica en la dificultad de imponer sanciones por incumplimiento suficientemente serias como para producir el efecto disuasorio necesario para crear tal clima de confianza. Incluso en aquellos casos en que siga ejerciéndose un control efectivo sobre los datos desde dentro de la Comunidad, el receptor de la transferencia puede no estar sujeto directamente a ninguna penalización si procesa los datos sin atenerse a lo dispuesto en el contrato. Por el contrario, la responsabilidad recaería en el remitente de los datos establecido en la Comunidad, el cual tendría entonces que entablar una acción legal independiente contra el receptor, para resarcirse de sus posibles pérdidas. Esta forma de responsabilidad indirecta podría no ser suficiente para inducir al receptor a cumplir el contrato al pie de la letra.

En tales circunstancias, es probable que, en la mayor parte de los casos, la solución contractual deba completarse, al menos, con la posibilidad de llevar a cabo de algún modo una verificación externa de las actividades de tratamiento del receptor, como por ejemplo una auditoría efectuada por un organismo de normalización o una empresa especializada.

5. El problema de la legislación aplicable

Una de las dificultades específicas que plantea el enfoque contractual es la posibilidad de que las normas jurídicas generales del tercer país de que se trate obliguen al receptor de la transferencia, en determinadas circunstancias, a comunicar los datos personales a las autoridades (policiales, judiciales o fiscales, por ejemplo) y de que tales requisitos legales prevalezcan sobre todo contrato firmado por el encargado del tratamiento. En lo que respecta a los encargados del tratamiento en la Comunidad, esta posibilidad se contempla en el artículo 16 de la Directiva, con arreglo al cual éstos únicamente pueden procesar datos siguiendo las instrucciones del responsable del tratamiento, *salvo en virtud de un imperativo legal*. No obstante, de acuerdo con la Directiva, estas notificaciones de datos (que, por su naturaleza, persiguen fines incompatibles con los previstos al recabar los datos) deben limitarse a lo imprescindible para atender a los imperativos de orden público de las sociedades democráticas, enunciados en el artículo 13.1 de la Directiva. El artículo 6 del Tratado de Amsterdam garantiza también la salvaguarda de los derechos fundamentales establecidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. En terceros países, es posible que no siempre existan tales restricciones sobre la capacidad de los poderes públicos para exigir de las empresas y otros organismos que operen en su territorio la comunicación de datos personales. Esta dificultad no es fácil de superar. Demuestra sencillamente las limitaciones de la solución contractual. En algunos casos, un contrato es un instrumento demasiado frágil como para ofrecer garantías suficientes en relación con la protección de datos, y no deberían autorizarse las transferencias de datos a determinados países.

6. Consideraciones de carácter práctico de cara a la utilización de contratos.

El anterior análisis demuestra la necesidad de que los contratos contengan cláusulas pormenorizadas y debidamente adaptadas a la transferencia de datos de que se trate. Esta necesidad de fijar minuciosamente la finalidad y las condiciones concretas del tratamiento al que se someterán los datos transferidos no excluye la posibilidad de desarrollar un modelo de contrato tipo, pero supone que todo contrato basado en el mismo se adecue a las circunstancias particulares del caso. El análisis realizado indica también que existen serias dificultades de orden práctico para llevar a cabo investigaciones en relación con el incumplimiento de un contrato cuando el tratamiento se efectúa fuera de la UE y cuando el país en cuestión no dispone de ningún tipo de organismo de supervisión. Si se unen ambas consideraciones, podemos concluir que habrá situaciones en las que una solución contractual resulte adecuada, y otras en las que quizá un contrato no pueda ofrecer "garantías suficientes".

Dada la necesidad de que el contrato se adapte rigurosamente a las particularidades de la transferencia, esta solución resultará especialmente adecuada en el caso de transferencias de datos similares y repetitivas. Los problemas relacionados con la supervisión suponen que la solución contractual será más eficaz cuando las partes del contrato sean grandes operadores que estén ya sometidos a inspección y regulación públicas. Las grandes redes internacionales, como las utilizadas para las transacciones con tarjetas de crédito y las reservas en líneas aéreas, presentan ambas características, por lo que, en este caso, los contratos pueden resultar de la máxima eficacia. En tales circunstancias podrían, incluso, completarse con convenios multilaterales que ofrezcan una mayor seguridad jurídica.

Del mismo modo, cuando las partes de la transferencia sean filiales o miembros del mismo grupo de empresas, es probable que aumenten considerablemente las posibilidades de investigar un incumplimiento de contrato, dada la fuerte vinculación existente entre el receptor en el tercer país y la entidad establecida en la Comunidad. Otro caso en el que convendría claramente desarrollar soluciones contractuales es, por tanto, el de las transferencias efectuadas dentro de una misma empresa.

Principales conclusiones y recomendaciones

En la Comunidad se utilizan contratos para determinar el reparto de responsabilidades en materia de protección de datos entre el responsable del tratamiento y el subcontratista encargado de llevarlo a cabo. Cuando se utilice un contrato en relación con transferencias de datos a terceros países, éste debe abarcar mucho más: ha de ofrecer a la persona a la que se refieran los datos salvaguardas adicionales, puesto que el receptor establecido en el tercer país no está sujeto a una serie de normas obligatorias para garantizar un nivel de protección adecuado.

Para evaluar la idoneidad de las salvaguardas ofrecidas por una solución contractual debe partirse de la misma base que para evaluar el nivel general de protección en un tercer país. Una solución contractual debe contener todos los principios básicos para la protección de datos y ofrecer los medios necesarios para que pueda velarse por su observancia.

El contrato debe fijar minuciosamente la finalidad, los medios y las condiciones del tratamiento de los datos transferidos, así como la forma en que se aplicarán los principios básicos de protección de datos. Los contratos que limitan la posibilidad de que el receptor de los datos los procese por cuenta propia de forma autónoma ofrecen una mayor seguridad jurídica. Por consiguiente, en la medida de lo posible, el contrato debería servir para atribuir al remitente de los datos el

poder decisorio sobre el tratamiento efectuado en el tercer país.
Si el receptor disfruta de cierta autonomía en relación con el tratamiento de los datos transferidos, la situación es más compleja y es posible que un simple contrato entre las partes de la transferencia no siempre permita a las personas a las que se refieren los datos ejercer sus derechos. Puede resultar necesario un mecanismo por el cual el remitente establecido en la Comunidad conserve la responsabilidad por los daños que pudieran derivarse del tratamiento llevado a cabo en el tercer país.
El contrato debería excluir expresamente la posibilidad de que los datos sean transmitidos posteriormente por el receptor a organismos u organizaciones no vinculados por el contrato, a menos que pueda obligarse a terceros, mediante disposiciones contractuales, a respetar los mismos principios de protección de datos.
La confianza en el respeto de tales principios, una vez efectuada la transferencia, mejoraría si el cumplimiento de los mismos por parte del receptor quedase sujeto a una verificación externa, de la que podría encargarse, por ejemplo, una empresa de auditoría especializada o un organismo de normalización o certificación.
En el supuesto de que la persona a la que se refieren los datos se encuentre con algún problema, como consecuencia, en su caso, del incumplimiento de las cláusulas sobre protección de datos contenidas en el contrato, resulta, en general, difícil asegurarse de que la queja del interesado se investiga convenientemente. Las autoridades supervisoras de los Estados miembros experimentarán dificultades de orden práctico a la hora de llevar a cabo tales indagaciones.
Las soluciones contractuales resultan probablemente más adecuadas para las grandes redes internacionales (tarjetas de crédito, reservas de billetes de avión), que se caracterizan por un elevado volumen de transferencias de datos similares y repetitivas, y por la existencia de un número relativamente reducido de grandes empresas que operan en sectores ya sujetos a supervisión y regulación públicas. Otro caso en el que la utilización de contratos presenta un potencial considerable es el de las transferencias de datos entre distintas sucursales o empresas del mismo grupo.
Los países en los que las prerrogativas con las que cuentan los poderes públicos para acceder a la información son más amplias de lo que autorizan las normas sobre protección de los derechos humanos aceptadas en el ámbito internacional, no constituyen un destino seguro para las transferencias basadas en cláusulas contractuales.

CAPÍTULO CINCO: EXCEPCIONES AL REQUISITO DE ADECUACIÓN

El artículo 26.1 de la Directiva enuncia un número limitado de situaciones en las que se puede aplicar una excepción al requisito de "adecuación" de las transferencias a terceros países. Estas excepciones, muy circunscritas, se refieren en su mayoría a casos en los que los riesgos para el interesado son relativamente escasos o en los que otros intereses (intereses públicos o del propio interesado) prevalecen sobre los derechos de intimidad del interesado. Como excepciones a un principio general, deben interpretarse restrictivamente. Además, los Estados miembros pueden estipular en la legislación nacional que las excepciones no se apliquen en determinados casos. Este puede ser el caso, por ejemplo, cuando sea necesario proteger a grupos de personas especialmente vulnerables, como los trabajadores o los pacientes.

La primera de estas excepciones abarca casos en los que el interesado ha dado su consentimiento *inequívocamente* a la transferencia prevista. Es importante tener en cuenta que el consentimiento, de acuerdo con la definición del artículo 2.h de la Directiva, debe ser libre, específico e informado. El requisito de información es especialmente relevante porque exige que el interesado esté debidamente informado del riesgo concreto que supone el hecho de que sus datos se transfieran a un país que carece de la protección adecuada. Si no se facilita esta información, dicha excepción no será aplicable. Puesto que el consentimiento debe ser inequívoco, cualquier duda sobre su obtención anularía la aplicabilidad de la excepción. Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto), la excepción no resultaría aplicable. Sin embargo, la excepción será útil cuando el remitente esté en contacto directo con el interesado y sea posible facilitar sin problemas la información necesaria y obtener un consentimiento inequívoco. Normalmente, éste será el caso en transferencias emprendidas en el contexto de, por ejemplo, la suscripción de seguros.

Las excepciones segunda y tercera abarcan transferencias *necesarias* para la ejecución de un contrato entre el interesado y el responsable del tratamiento (o para la ejecución de medidas precontractuales adoptadas a petición del interesado) o para la celebración o ejecución de un contrato celebrado *en interés del interesado* entre el responsable del tratamiento y un tercero. Aparentemente, estas excepciones son potencialmente bastante amplias, pero, al igual que las excepciones cuarta y quinta comentadas a continuación, es probable que su aplicación en la práctica se vea limitada por la "prueba de necesidad": todos los datos transferidos deben ser necesarios para la ejecución del contrato. Así, si se transfieren datos complementarios que no son esenciales o si el objetivo de la transferencia no es la ejecución del contrato sino otro (mercadotecnia de seguimiento, por ejemplo) se invalidará la excepción. Respecto de las situaciones precontractuales, esta excepción sólo abarca situaciones iniciadas por el interesado (como una solicitud de información sobre un servicio particular) y no las que derivan de propuestas de mercadotecnia planteadas por el responsable del tratamiento.

A pesar de estas salvedades, las excepciones segunda y tercera tienen bastante peso. Es probable que sean aplicables con frecuencia, por ejemplo, en las transferencias necesarias para reservar un billete de avión de un pasajero, o en transferencias de datos personales necesarios para la transacción de un banco internacional o de un pago con tarjeta de crédito. De hecho, la excepción de contratos "en interés del interesado" (artículo 26.1.c) abarca específicamente la transferencia de datos relativos a los beneficiarios de los pagos bancarios, quienes, aunque sean interesados, es posible que a menudo no sean parte de un contrato celebrado con el responsable del tratamiento que realiza la transferencia.

La cuarta excepción tiene dos vertientes. La primera engloba las transferencias necesarias o legalmente exigidas por

un interés público importante. Este aspecto puede abarcar ciertas transferencias limitadas entre administraciones públicas, aunque hay que tener cuidado de no interpretar esta disposición en sentido muy amplio. Para justificar una transferencia no basta con alegar un interés público, debe ser un interés público *importante*. El considerando 58 declara que, normalmente, se incluirán los datos transferidos entre administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social. Es posible que también las transferencias entre organismos supervisores de los servicios financieros se beneficien de la excepción. La segunda vertiente se refiere a las transferencias que tienen lugar en el contexto de litigios o procedimientos judiciales internacionales, concretamente transferencias necesarias para el reconocimiento, ejercicio o defensa de derechos legales. La quinta excepción se refiere a las transferencias necesarias para proteger los intereses vitales del interesado. Un ejemplo evidente sería la transferencia urgente de datos médicos a un tercer país, en el caso de un turista que, habiendo recibido anteriormente tratamiento médico en la UE, haya sufrido un accidente o haya enfermado gravemente. Sin embargo, es preciso tener en cuenta que el considerando 31 de la Directiva interpreta con bastante concreción el "interés vital" como un interés "esencial para la vida del interesado". Esta interpretación normalmente excluye, por ejemplo, los intereses financieros, de propiedades o familiares.

La excepción sexta y última se refiere a las transferencias realizadas desde registros que por la ley se han destinado a la consulta pública, si se cumplen las condiciones de consulta en cada caso particular. La intención de esta excepción es que cuando un registro de un Estado miembro esté disponible para consulta pública o por personas que demuestren un interés legítimo, el hecho de que la persona con derecho a consultar el registro se encuentre en un tercer país y que la consulta conlleve el hecho de una transferencia de datos, no impida que se le transmita la información. El considerando 58 especifica que es preciso no permitir la transferencia de la totalidad de los datos o categorías de datos contenidos en el mencionado registro en virtud de esta excepción. Dadas estas restricciones, no hay que considerarla una excepción general relativa a la transferencia de datos de registros públicos. Por ejemplo, es evidente que las transferencias masivas de datos de registros públicos con fines comerciales o la búsqueda de datos a disposición del público con el fin de realizar perfiles de personas físicas específicas no se beneficiarían de la excepción.

CAPÍTULO SEIS: CUESTIONES DE PROCEDIMIENTO

El artículo 25 contempla un planteamiento individualizado en el que la evaluación de la adecuación se efectúa en relación con transferencias particulares o con categorías de transferencias particulares. Sin embargo, es evidente que, dado el elevado número de transferencias diarias de datos personales desde la Comunidad y la multitud de agentes que participan en estas transferencias, ningún Estado miembro, sea cual sea el sistema que elija para aplicar el artículo 25 19 , podrá asegurar que cada caso se examine en detalle. Evidentemente, ello no implica que no se vaya a examinar ningún caso en detalle, sino que será preciso idear mecanismos que racionalicen el proceso decisorio para un elevado número de casos, permitiendo tomar decisiones, o al menos decisiones provisionales, sin una demora injustificada o sin implicar recursos excesivos.

Esta racionalización es necesaria independientemente de quién toma la decisión, ya sea el responsable del tratamiento, la autoridad supervisora o algún otro organismo creado por el procedimiento del Estado miembro.

i) Uso del artículo 25.6 de la Directiva

Una forma evidente de contribuir a esta racionalización, prevista en la Directiva misma, sería la determinación de que ciertos terceros países aseguran un nivel adecuado de protección. Estas determinaciones serían "sólo orientativas" y, por tanto, sin perjuicio de los casos que pudieran presentar dificultades concretas. No obstante, constituiría una respuesta práctica al problema.

En particular, estas determinaciones proporcionarían cierta seguridad a los agentes económicos en lo referente a los países que podrían considerarse, en general, garantes de un nivel "adecuado" de protección. También ofrecerían un incentivo claro y público a los terceros países que aún siguen organizando y mejorando sus sistemas de protección. Además, una serie de estas determinaciones a escala comunitaria contribuiría al establecimiento de un enfoque coherente de esta cuestión e impediría la publicación "listas blancas" divergentes, y quizás contradictorias, por parte de los gobiernos o autoridades de protección de datos de los diferentes Estados miembros. Sin mbargo, este enfoque no carece de dificultades. La principal es que muchos terceros países no disponen de una protección uniforme en todos los sectores económicos. Por ejemplo, muchos países disponen de legislación de protección de datos en el sector público pero no en el privado. Algunos países, por ejemplo Estados Unidos, tienen leyes específicas para aspectos concretos (informes comerciales y registros de alquiler de vídeos), pero no para otros. Otra de las dificultades se da en países con constituciones federales como EEUU, Canadá y Australia, donde a menudo hay diferencias entre los distintos estados que conforman la federación. Por ello, actualmente parece improbable que muchos terceros países puedan ser considerados garantes de una protección adecuada de una manera general. Cuanto menor sea el número de países sobre los cuales puedan hacerse determinaciones positivas, menos útil será este ejercicio, evidentemente, para proporcionar más seguridad a los responsables del tratamiento. Otro riesgo es que algunos terceros países puedan considerar políticamente provocativa o cuando menos dicriminatoria la ausencia de determinación positiva porque esta ausencia podría obedecer tanto al no examen de su caso como a un juicio negativo sobre su sistema de protección de datos.

Una vez sopesados estos diferentes argumentos con detenimiento, el Grupo de Trabajo opina que iniciar el trabajo para llegar a una serie determinaciones con arreglo al artículo 25.6 es, a pesar de todo, una medida útil. Se trataría de un proceso continuo, no de un proceso que dé lugar a una lista definitiva, sino a una lista ampliada y revisada constantemente a la luz de las nuevas situaciones. En principio, una determinación positiva no debería limitarse a países con una legislación de protección de datos horizontal, sino que también debe abarcar sectores específicos donde la

protección de datos sea adecuada dentro de un país que en otros sectores ofrezca una protección insuficiente.

Es necesario advertir que el grupo del artículo 29 no desempeña un papel explícito en la toma de decisiones sobre transferencias de datos particulares o en las determinaciones de la "adecuación" previstas en el artículo 25.6. Estas decisiones y determinaciones están sujetas al procedimiento de comitología establecido en el artículo 31. Sin embargo, hay que recordar que uno de los deberes específicos del grupo del artículo 29 es expresar a la Comisión su opinión sobre el nivel de protección en terceros países (véase el artículo 30.i.b). Por tanto, examinar la situación en terceros países particulares y alcanzar una conclusión provisional sobre el carácter adecuado de la protección es algo que entra en el mandato del grupo del artículo 29. Para que las determinaciones positivas resulten de utilidad, es preciso que se promulguen ampliamente una vez confirmadas con arreglo al artículo 25.6. Por otro lado, la determinación de que un país no dispone de la protección adecuada no implica necesariamente que el país esté en la "lista negra" implícita o explícitamente. El mensaje público más bien sería que todavía no se dispone de orientación general relativa al país en cuestión.

ii) Análisis de riesgos de transferencias específicas

Aunque el uso del artículo 25.6 descrito anteriormente sea una valiosa ayuda para el proceso de toma de decisiones en relación con un elevado número de transferencias de datos, habrá muchos casos en los que el tercer país en cuestión no será objeto (total o parcialmente) de una determinación positiva. El modo en que los Estados miembros se ocupen de estos casos puede variar de acuerdo con el modo en que el artículo 25 se incorpore en la legislación nacional (véase la nota a pie de página nº 19). Si se otorga a la autoridad de control la función específica de autorizar las transferencias de datos antes de que ocurran o para realizar una revisión *ex post facto*, el enorme volumen de transferencias evidenciará la necesidad de contemplar un sistema para fijar las prioridades en los esfuerzos de la autoridad de control. Este sistema podría adoptar la forma de un conjunto de criterios aceptados que permitan considerar con prioridad una transferencia concreta o una categoría de transferencias porque supone una amenaza particular para la vida privada.

Evidentemente, el efecto de este sistema no alteraría la obligación de todos los Estados miembros de garantizar que únicamente puedan realizarse transferencias cuando los terceros países aseguren un nivel de protección adecuado. Supondría una orientación para determinar qué casos de transferencia de datos requieren prioritariamente un examen o incluso una investigación y, de ese modo, permitiría que se destinen los recursos disponibles a las transferencias que generen mayor preocupación en cuanto a la protección de los interesados.

El Grupo de Trabajo considera que entre las categorías de transferencias que conllevan un riesgo particular para la vida privada y, por tanto, merecen atención especial, figuran las siguientes:

- las transferencias de ciertas categorías sensibles de datos definidas en el artículo 8 de la directiva;
- las transferencias que comportan el riesgo de pérdida financiera (por ejemplo, pagos con tarjeta de crédito a través de Internet);
- las transferencias que comportan un riesgo para la seguridad personal; - las transferencias cuyo objetivo sea tomar una decisión que afecta significativamente a la persona (como, por ejemplo, decisiones de contratación o promoción, la concesión de créditos, etc.);
- las transferencias que comportan el riesgo de poner a la persona en una situación embarazosa o de empañar su reputación;
- las transferencias que pueden dar lugar a acciones específicas que constituyan una intrusión significativa en la vida privada de una persona, como las llamadas de teléfono no solicitadas;
- las transferencias repetitivas de volúmenes masivos de datos (por ejemplo, datos transaccionales tratados en redes de telecomunicaciones, Internet, etc.);
- las transferencias que incluyen la recopilación de datos mediante nuevas tecnologías que, por ejemplo, podrían realizarse de forma particularmente encubierta o clandestina (por ejemplo, "cookies" de Internet).

iii) Cláusulas contractuales tipo

Como se ha especificado en el capítulo cuatro, la Directiva contempla la posibilidad de que, incluso cuando el nivel de protección no sea adecuado, un responsable del tratamiento pueda alegar que una transferencia de datos reúne garantías adecuadas gracias a un contrato. El artículo 26.2 de la Directiva permite a los Estados miembros autorizar transferencias en virtud de tales disposiciones contractuales, decisión que después debe notificarse a la Comisión. En caso de oposición a la autorización, la Comisión puede anular o confirmar la decisión, de acuerdo con el procedimiento de comitología establecido en el artículo 31. Además de las autorizaciones de los Estados miembros, el artículo 26.4 de la Directiva permite a la Comisión, también de acuerdo con el procedimiento de comitología establecido en el artículo 31, juzgar si ciertas cláusulas contractuales tipo ofrecen las garantías suficientes. Estos juicios son vinculantes para los Estados miembros.

Dada la manifiesta complejidad y dificultad de estas soluciones contractuales, es evidente que los responsables del tratamiento que contemplen este uso de los contratos precisan una orientación consensuada. En los Estados miembros, es posible que las autoridades nacionales competentes asuman una mayor responsabilidad en la facilitación de esta orientación, en particular al preparar autorizaciones en el contexto del artículo 26.2. Las autoridades de los Estados miembros y la Comisión deberían cooperar e intercambiar opiniones sobre las cláusulas contractuales que se les sometan. Cuando se presentan propuestas de cláusulas tipo a las autoridades de los Estados miembros o directamente a la Comisión, sería preciso desarrollar un procedimiento para garantizar que también el Grupo de Trabajo examine estas cláusulas, para evitar diferencias en las prácticas nacionales y para garantizar que la Comisión pueda asesorarse debidamente antes de adoptar ninguna decisión en virtud del artículo 26.4.

ANEXO 1

QUÉ IMPLICACIONES PUEDEN TENER EN LA PRÁCTICA LOS ARTÍCULOS 25 Y 26 DE LA DIRECTIVA EN LA TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES

Introducción

La parte principal de este documento presenta un enfoque global de la cuestión de las transferencias a terceros países que incluye:

- qué debe entenderse por protección adecuada en el sentido del artículo 25 de la directiva sobre protección de datos;
- una evaluación de los medios alternativos para justificar garantías suficientes a través de soluciones contractuales, como se contempla en el artículo 26.2;
- una evaluación de las excepciones al requisito de protección adecuada previstas en el artículo 26.1.

Sin embargo, un conocimiento de estas cuestiones no sería completo sin un ejemplo del modo en que este enfoque global puede repercutir en las transferencias reales de datos personales. Por tanto, en este anexo se examinan una serie de casos realistas (aunque ficticios) de transferencias de datos en la forma en que, previsiblemente, se examinarán cuando entren en vigor las legislaciones nacionales que aplican la Directiva. Se exponen tres casos diferentes. En cada caso el primer paso consiste en evaluar si la protección en el país de destino es adecuada en virtud de las legislaciones pertinentes o de la autorregulación efectiva del sector privado. Si no es así, entonces el segundo paso es buscar una solución al problema entre las posibilidades enumeradas en el artículo 26, apartados 1 (excepciones) y 2 (soluciones contractuales). Sólo entonces, si ninguna solución es apropiada, el tercer paso sería bloquear la transferencia.

CASO (1): una transferencia de datos relativos a la solvencia crediticia

Un ciudadano comunitario desea comprar una residencia secundaria en el país A, fuera de la CE, y solicita un crédito a una institución financiera en este país. La institución financiera solicita un informe comercial a una agencia de informes comerciales. La agencia no tiene ningún fichero sobre dicha persona, pero solicita la transferencia del historial crediticio completo de esta persona a su agencia "hermana", la Agencia de Referencia Crediticia del Reino Unido. El país A es un país industrializado y desarrollado, con instituciones democráticas antiguas y estables. El sistema judicial está bien dotado de recursos y funciona eficazmente. Tiene una estructura constitucional federal.

PRIMER PASO: EVALUAR EL CARÁCTER ADECUADO DE LA PROTECCIÓN

Normas aplicables

El responsable del tratamiento receptor está sujeto a una legislación federal que establece normas relativas a la información personal empleada para evaluar riesgos crediticios. Además, el responsable del tratamiento afirma que cumple la política de protección de la intimidad que ha instaurado en su entidad y que ha hecho pública. No hay ninguna ley nacional aplicable ni ningún código de autorregulación industrial.

Evaluación del contenido de las normas aplicables

En primer lugar, es preciso indicar que la comunicación de la agencia de referencia crediticia ubicada en el Reino Unido estaría, como cualquier comunicación dirigida a un responsable del tratamiento establecido en otro lugar distinto del Reino Unido u otro Estado miembro, sujeta a los requisitos normales de la legislación nacional que aplica todos los artículos de la Directiva, excepto los artículos 25 y 26. Esto es importante porque elimina la necesidad de examinar la legalidad de la propia comunicación. Se prestará más atención a la protección ofrecida a los datos una vez transferidos al país A. Lógicamente, la evaluación del contenido de las normas empezará con la legislación federal. Si se encuentran lagunas, puede estudiarse la norma menos vinculante que es la política de protección de la intimidad para ver si suple esta carencia. A continuación, se ofrece una lista del contenido necesario y un juicio sobre la presencia de este contenido necesario en la legislación o en la política de protección de la intimidad.

En este contexto, el principio de limitación de objetivos puede centrarse únicamente en el requisito de que todo uso y divulgación secundarios de los datos transferidos no ean incompatibles con el objetivo de su transferencia. La inclusión de los datos en una lista de correo que se vende o alquila en el mercado abierto podría considerarse incompatible, al igual que la divulgación de datos a posibles empleadores o socios comerciales interesados en la solvencia de la persona física afectada. Sin embargo, es posible que la divulgación de los datos a otros otorgantes de crédito (bancos, empresas de tarjetas de crédito) se considere compatible.

En este caso, la legislación nacional establece un número limitado de objetivos para los cuales la información personal crediticia puede revelarse legítimamente. No obstante, estos objetivos incluyen el "empleo" y la "necesidad comercial legítima relativa a una transacción comercial que implica a la persona física". Este último concepto incluye ciertos usos comerciales de los datos que podrían llevar aparejada la mercadotecnia de productos o servicios, excepto créditos, por parte de terceros. Por tanto, parece que el objetivo no está suficientemente limitado por la legislación federal y que, en este punto, la protección no es adecuada. La política de protección de la intimidad de la empresa no mejora la situación.

El principio de transparencia debería permitir al interesado conocer la identidad de la agencia de informes comerciales del país A, así como cualquier nuevo objetivo del tratamiento de los datos. El método para lograrlo debe ser equiparable al previsto en el artículo 11 de la Directiva.

En este caso, la legislación federal no contiene disposiciones específicas sobre la transparencia que obliguen directamente a la agencia de informes comerciales. Sin embargo, el otorgante de crédito del país A deberá informar a la persona de que se solicitará un informe comercial a la Agencia de Informes Comerciales, aunque no es preciso indicar el nombre y la dirección de la agencia. Por tanto, la persona no disfruta de garantía jurídica de que se le vaya a informar sobre el hecho de que la Agencia de Informes Comerciales en cuestión está tratando sus datos. Sin embargo, dado que la agencia no tiene contacto directo con la persona, obligar a la agencia a entrar en contacto con la persona especialmente para informarle parece ser un "esfuerzo desproporcionado", en el sentido del artículo 11 de la Directiva. Por tanto, el nivel de protección en cuanto a la transparencia parece adecuado.

El principio de proporcionalidad y de calidad incluye varios elementos diferentes. No existe ninguna restricción a la recopilación y tratamiento de datos innecesarios en la legislación federal. Respecto de la duración de almacenaje, hay normas que evitan la divulgación de la información obsoleta (decisiones judiciales de insolvencia con más de 10 años de antigüedad), y que permiten eficazmente la eliminación de esta información. No existen requisitos jurídicos generales para conservar fielmente los datos, aunque cuando una persona que ha solicitado acceder a sus informes comerciales impugne parte de la información, los datos que no puedan verificarse deben borrarse. De nuevo, la protección no parece del todo adecuada, y la política de intimidad de la empresa no supera a la legislación federal.

El principio de seguridad se refleja en la legislación federal mediante un requisito 35 de adopción de medidas justificadas para evitar la divulgación ilegal. La política de intimidad de la empresa evidencia que se han establecido controles estrictos para evitar el acceso no autorizado a información crediticia y la manipulación de la misma. Estos controles adoptan la forma de dispositivos técnicos (contraseñas, etc.) e instrucciones a empleados cuyo incumplimiento puede dar lugar a expedientes disciplinarios. Todo ello parece garantizar un nivel adecuado de seguridad.

Los derechos de acceso y rectificación se incluyen en la legislación federal y son equiparables a los encontrados en la Directiva. Cuando se ha denegado el crédito a una persona, el acceso al informe comercial es gratuito. Sin embargo, no hay derecho de oposición aunque una persona puede quejarse ante un organismo federal especializado o ir a los tribunales (véase más adelante), cuando sus derechos jurídicos establecidos en la legislación federal han sido violados.

Los datos sensibles sobre la salud de la persona física forman parte de los datos transferidos. La legislación federal incluye disposiciones más estrictas para el tratamiento de la información relativa a antecedentes penales, sexo, raza, origen étnico, edad y estado civil, pero no para la información sobre la salud. Sin embargo, en su política de intimidad, la agencia de informes comerciales establece que los datos sobre la salud no se utilizarán para la evaluación crediticia, sino únicamente para revisiones médicas a efectos de empleo o de seguros. En estas dos situaciones, el uso de dichos datos deberá autorizarlo la persona en un impreso de solicitud de empleo o de seguros. Por tanto, parece que la protección de los datos sobre la salud de este ejemplo se ha reforzado sustancialmente, aunque no se prevé jurídicamente.

El uso de los datos para la mercadotecnia directa por parte de la agencia de informes comerciales (y la divulgación de los datos a terceros con el mismo fin) es una cuestión importante en este caso. No existen verdaderos impedimentos jurídicos a este uso, y tampoco requisitos jurídicos que ofrezcan la exclusión voluntaria. Esto es claramente inadecuada, sobre todo porque en este caso la agencia no sólo utilizará los datos (para realizar envíos publicitarios por cuenta de instituciones financieras de concesión de crédito), sino que también se divulgarán a terceros para la mercadotecnia de productos afines y no afines a los servicios financieros, como cortacéspedes o vacaciones.

Parece que el objetivo de la transferencia sea permitir la adopción de una decisión automatizada sobre la concesión de un crédito al interesado. Por tanto, es preciso que el interesado se beneficie de las garantías complementarias a este respecto. Aunque la legislación federal incluye disposiciones que permiten a la persona afectada impugnar la información contenida en un informe financiero y adjuntar explicaciones al informe si es necesario, no hay disposiciones que permitan recusar y revisar una decisión tomada sobre la base de información errónea o incompleta y modificarla si la recusación está justificada. Este mecanismo permite alterar un informe comercial para evitar problemas futuros, pero no resuelve necesariamente el problema de una decisión crediticia ya adoptada. Esta no retroactividad de la protección jurídica supone una insuficiencia.

Restricciones a transferencias posteriores de los datos a otro tercer país o a organizaciones de otros sectores dentro del país A no sujetas a las normas establecidas en la legislación federal. No existen estas disposiciones ni en la legislación federal ni en la política de protección de la intimidad de la empresa.

Ámbito de aplicación de la legislación federal y de la política de protección de la intimidad. Es necesario realizar otra comprobación para garantizar que tanto la legislación como la política de intimidad se aplican a los datos de todas las personas, y no sólo a los datos sobre residentes o nacionales del país A. En este caso, no existen restricciones al ámbito de aplicación.

Evaluación de la eficacia de la protección

La legislación federal en cuestión tiene fuerza de ley y también establece una autoridad pública con ciertas competencias de control externo. Las personas también pueden iniciar procesos judiciales privados al amparo de la legislación

para ejercer sus derechos. Sin embargo, la autoridad pública no está claramente obligada a investigar cada una de las quejas, y según algunos analistas no siempre ha sido particularmente activa en la aplicación de la ley. Para las personas, los procesos judiciales privados constituyen medios caros, y a menudo lentos, de asegurar una vía de recurso, en particular cuando el interesado vive en un país diferente al país en el que tiene lugar el procedimiento judicial.

La política de intimidad de la empresa no comprende ningún mecanismo independiente que permita a la persona afectada ejercer sus derechos, pero sí contiene algunas sanciones disciplinarias para empleados que infringen la política. De hecho, varios empleados ya han sido sancionados en relación con infracciones en el pasado. La combinación de legislación y código interno de protección de la intimidad debe evaluarse en función de los "objetivos" establecidos para los mecanismos de procedimiento. En este caso, las cuestiones clave podrían incluir:

Nivel satisfactorio de cumplimiento general

El estímulo principal de la empresa para cumplir su política de intimidad es el riesgo de la publicidad dañina en la prensa si se descubre el incumplimiento de sus promesas. Además, las personas que trabajan en la empresa pueden estar sujetas a medidas disciplinarias si desobedecen las normas de seguridad.

Sin embargo, estos mecanismos no parecen suficientes para garantizar que en la práctica se cumple la política de protección de la intimidad. Esta conclusión podría haber sido diferente si:

1) la política de intimidad de la empresa se hubiera plasmado en un código industrial de conducta establecido por la asociación gremial del sector, en virtud del cual toda empresa que violara el código sería expulsada inmediatamente de la 37 asociación; o

2) un principio general de la legislación permitiera a un organismo público demandar a una empresa que hubiera violado su código de intimidad hecho público por prácticas "desleales y engañosas".

Respecto de la legislación federal, la posibilidad de emprender procesos judiciales privados en el caso de incumplimiento induce al cumplimiento. La perspectiva de ser llevado a los tribunales ejercería cierta influencia disuasoria sobre el responsable del tratamiento. Sin embargo, esta influencia es muy escasa en el método de la verificación directa y externa de los procedimientos de tratamiento de los datos, pues la autoridad pública sólo reacciona cuando se llama su atención sobre un problema a través de una queja o de la prensa, por ejemplo.

Apoyo y ayuda a los interesados

Está claro que existe un organismo público que centraliza las quejas de personas en relación con sus informes comerciales. La investigación de quejas no supone ningún coste para estas personas.

Reparación adecuada

En caso de incumplimiento de las estrictas obligaciones judiciales de la legislación federal, la persona afectada puede obtener reparación de un tribunal. Sin embargo, es un proceso relativamente caro, y el interesado no suele recibir apoyo del organismo público en estos procedimientos judiciales. El tribunal puede ordenar al responsable del tratamiento el pago de una indemnización por daños y perjuicios a dicha persona (si se demuestra que éstos se han producido) y la modificación de sus procedimientos de tratamiento de datos y el contenido del fichero crediticio en cuestión. En cuanto al incumplimiento de los principios de protección de datos englobados únicamente en la política de intimidad, esta reparación no es posible.

Veredicto

1) Algunos principios de protección de datos, establecidos como "principios básicos" en el documento de debate, pueden encontrarse en cierto modo en la legislación federal aplicable al fichero crediticio. Otros principios se encuentran en la política de intimidad. Incluso aunque se reúnan todos, no puede decirse que esté presente el conjunto completo de los "principios básicos", y la presencia de algunos (por ejemplo, el p rincipio de limitación de objetivos) es bastante precaria.

2) Se plantea el problema más general de si la política de intimidad de la empresa es, en cualquier caso, un mecanismo suficientemente eficaz como para tenerlo en cuenta. A menos que la política cuente con un mayor sostén y con una mayor fuerza ejecutiva a través de poderes de control externo conferidos a una asociación industrial o a un órgano público, sus disposiciones son, en gran parte, inejecutables y, por tanto, pueden dejarse de lado.

3) Aunque el organismo público creado para hacer cumplir la legislación federal no disfruta de los mismos poderes que la típica autoridad de protección de datos europea, la legislación proporciona cierta seguridad jurídica, especialmente en el contexto de un sistema judicial que funciona debidamente y de la "cultura de litigio" del país A. La legislación contiene disposiciones claras relativas a los principios de protección de datos que quizá sean los más importantes: el derecho de acceso y rectificación, y algunas limitaciones del objetivo con el que se pueden utilizar los datos.

Conclusión

La protección no es adecuada porque la legislación no abarca suficientes "principios básicos" y porque la política de intimidad, por sí misma, no es un medio eficaz para proporcionar protección. Podría llegarse a un veredicto de "ade-

cuado" si el desarrollo de la legislación incluyera principios como la transparencia y la protección de datos sobre la salud, o si uno de los métodos antes sugeridos (es decir, hacer del cumplimiento una condición para ser miembro de una asociación industrial o facultar a un organismo público para procesar a la empresa por prácticas engañosas si ha incumplido su propia política) dotara de mayor eficacia a la política de intimidad.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

De las excepciones posibles expuestas en el Artículo 26.1, únicamente la a), el consentimiento del interesado, parece adecuada. La excepción b) referente a las transferencias necesarias por motivos contractuales, no es aplicable porque la parte remitente, la agencia de referencia crediticia ubicada en el Reino Unido, no tiene ninguna relación contractual con el interesado. También es difícil defender el argumento de la necesidad de la transferencia en razón de un contrato "en interés del interesado", como dispone la excepción c).

No obstante, el consentimiento del interesado parece ser una solución relativamente sencilla al problema. El consentimiento podría obtenerlo directamente la agencia de referencia de crédito con sede en el Reino Unido o, en su nombre, la institución financiera radicada en el país A, que podría recabarlo en el impreso de solicitud de préstamo. Independientemente del método elegido, sería preciso informar al interesado del riesgo concreto que supone la transferencia de sus datos a un país que carece de protección adecuada.

Dado que este tipo de transferencia todavía es relativamente raro, la obtención del consentimiento con carácter puntual probablemente sea la solución más práctica. Si las agencias de referencia de crédito y de informes comerciales de todo el mundo empiezan a intercambiar datos de forma más sistemática, podrían ponerse a punto otros acuerdos como las soluciones contractuales o un código de conducta internacional.

CASO (2): transferencia de datos sensibles en el sector aeronáutico

Un ciudadano portugués reserva un billete en una agencia de viajes de Lisboa para volar con una compañía aérea con sede en el país B. Los datos recabados incluyen información sobre la discapacidad del ciudadano y sobre el hecho de que utiliza una silla de ruedas. Los datos se introducen en un sistema informático internacional de reservas y, desde allí, la compañía aérea los descarga en su base de datos sobre pasajeros, ubicada en el país B, donde se conservan indefinidamente. La compañía aérea decide utilizar los datos para prestar un mejor servicio al pasajero en caso de que viaje con ellos en el futuro, así como para la planificación de la gestión interna.

PRIMER PASO: EVALUAR EL CARÁCTER ADECUADO DE LA
PROTECCIÓN

Normas pertinentes aplicables

Aunque existe un código de conducta internacional que se aplica a los datos contenidos en un sistema informático de reservas, no hay normas vigentes de protección de los datos contenidos en la base de datos de la compañía aérea con sede en el país B.

Evaluación del contenido de las normas aplicables

No existen normas aplicables.

Evaluación de la eficacia de la protección

No es pertinente.

Veredicto

Los niveles de protección en el país B no son adecuados, particularmente dada la sensibilidad de los datos en cuestión.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

La transferencia de datos al sistema informático de reservas y su uso por parte de la compañía aérea para prestar el servicio apropiado al pasajero discapacitado en el vuelo en cuestión, es una transferencia necesaria para la ejecución del contrato entre el pasajero y la compañía aérea (artículo 26.1.b). No obstante, la conservación permanente de los datos (que incluyen datos sensibles sobre la salud del interesado) en la base de datos de la compañía aérea no puede justificarse por estos motivos. Por tanto, es preciso que la transferencia de datos a la compañía aérea sea cubierta por una excepción diferente.

Como con el caso 1), el consentimiento del interesado parecería la mejor solución. El agente de viajes de Lisboa podría obtener el consentimiento en nombre de la compañía aérea. Es recomendable comunicar al interesado los riesgos que pueden derivarse de conservar los datos en el país B, y que la transferencia y la conservación de los datos en la base de datos de la compañía aérea no son necesarias para la reserva del vuelo en cuestión.

CASO (3): transferencia de datos de una lista de direcciones

Una empresa de los Países Bajos está especializada en la elaboración de listas de direcciones. Empleando muchas fuentes distintas de información pública disponibles en los Países Bajos, junto con listas de clientes alquiladas de otras empresas holandesas, las listas resultantes pretenden incluir a personas que se ajusten a un perfil socioeconómico particular. Después, la empresa holandesa vende estas listas a clientes no sólo de los Países Bajos y de la UE, sino también de muchos otros países.

Las empresas clientes receptoras utilizan las listas (que incluyen direcciones postales de correo electrónico, números de teléfono y, a menudo, direcciones de correo electrónico) para entrar en contacto con las personas relacionadas con vistas a vender una desconcertante selección de diferentes productos y servicios. Un elevado número de personas incluidas en las listas se han quejado a la autoridad de protección de datos holandesa en relación con las proposiciones comerciales de que han sido objeto.

Normas pertinentes aplicables

Algunas de las empresas que compran las listas de direcciones ofertadas por la empresa holandesa se ubican en países con una legislación general de protección de datos que incluye el derecho de las personas a optar por no ser objeto de estas proposiciones comerciales. Otras se encuentran en países que no disponen de tal legislación, pero son miembros de asociaciones de autorregulación que han elaborado códigos de protección de datos. Otras no están sujetas a ninguna norma de protección de datos.

Evaluación del contenido de las normas aplicables

Este caso por sí solo exigiría la evaluación de un elevado número de diferentes leyes y códigos. Si la empresa ubicada en los Países Bajos tiene la intención de mantener la actividad de venta o alquiler de sus listas a empresas ubicadas en cualquier país del mundo, entonces necesariamente habrá situaciones donde el nivel de protección no sea adecuado.

SEGUNDO PASO: BÚSQUEDA DE UNA SOLUCIÓN

En este ejemplo, debido a que los datos se recaban de fuentes públicas y sin establecer ningún contacto directo con el interesado, sería muy problemático para la empresa de los Países Bajos recabar el consentimiento de cada uno de los interesados para incluirlo en las listas de direcciones. Por ello, es improbable que alguna de las excepciones del artículo 26.1 sea de utilidad.

La empresa holandesa tiene dos posibilidades, que podrían utilizarse como alternativas o juntas. En primer lugar, limitar su actividad comercial con las listas de direcciones a empresas ubicadas en países que aseguren inequívocamente la protección adecuada en virtud la ley o de instrumentos de autorregulación eficaces. A la hora de adoptar esta 42 decisión, la empresa puede obtener orientación en cualquier "lista blanca" disponible. La segunda posibilidad consiste en solicitar compromisos contractuales de todos los clientes (o al menos de los radicados en países "no adecuados") en relación con la protección de los datos transferidos. Estos acuerdos contractuales deberían seguir el consejo expuesto en el capítulo cuatro del documento principal. En particular, es preciso que su objetivo sea la creación de una situación en la cual la empresa de los Países Bajos se responsabilice, con arreglo a la legislación holandesa, de toda violación de los principios de protección de datos causada por las acciones del cliente al cual se transfirió la lista de direcciones.

Esta solución contractual, si se aplica debidamente, permitiría superar la efectiva barrera a la actividad comercial que la falta de protección adecuada de datos crea en determinados terceros países.

Bruselas, 24 de julio de 1998
Por el Grupo de Trabajo
El Presidente
P.J. HUSTINX

MEMORIA DE 1998 - ANEXO X

COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre circulación de la información, Derecho de sociedades e información financiera
Libre circulación de la información, protección de datos y sus aspectos internacionales

DG XV D/5004/98
WP 13

Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales.

Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo.

Aprobado el 10 de septiembre de 1998

Labor futura sobre los códigos de conducta: procedimiento de admisión y examen de los códigos de conducta comunitarios por el Grupo de Trabajo

Introducción:

El presente documento de trabajo pretende aclarar el procedimiento que deben seguir los interesados con vistas a la presentación de códigos de conducta comunitarios y a su posterior evaluación por el Grupo de Trabajo de conformidad con lo previsto en los artículos 27 y 29 de la Directiva 95/49/CE.

En primer lugar se resumen en el presente documento las etapas básicas del procedimiento, definiéndose a continuación una serie de normas específicas en relación con cada una de ellas. Estas normas se revisarán, en su caso, a la luz de la experiencia adquirida.

Etapas básicas del procedimiento

El procedimiento de admisión y examen de los códigos de conducta por el Grupo de Trabajo consta de las siguientes etapas:

I) Presentación y admisión.
II) Elaboración del dictamen del Grupo de Trabajo.
III) Aprobación del dictamen del Grupo de Trabajo y notificación del mismo a los interesados.

Artículo 1 - Definiciones

A efectos de las presentes normas se entenderá por:

1.1 "Directivas": la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y 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.

1.2 "Grupo de Trabajo": el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales a que se refiere el artículo 29 de la Directiva 95/46/CE.

1.3 "Código de conducta": los códigos de conducta comunitarios contemplados en el apartado 3 del artículo 27 de la Directiva 95/46/CE, incluidas las modificaciones o prórrogas de códigos comunitarios existentes.

Artículo 2 - Normas relativas a la presentación y admisión de códigos de conducta para su examen por el Grupo de Trabajo.

2.1 Toda organización representativa del sector considerado que esté establecida u opere en un número significativo de Estados miembros podrá presentar un proyecto de código de conducta para su examen por el Grupo de Trabajo.

2.2 Dicho proyecto de código deberá elaborarse cuidadosamente, y de preferencia previa consulta a las personas a las que se refieran los datos procesados o sus representantes, y definir claramente la organización o el sector al que el código está destinado a aplicarse.

2.3 Los proyectos de códigos se redactarán en una lengua comunitaria y se enviarán, junto con su traducción inglesa y francesa, al Presidente del Grupo de Trabajo, a través de la secretaría (Comisión Europea, DG XV-D1), adjuntando, asimismo, una exposición de motivos.

2.4 Los proyectos prematuros y los proyectos de códigos que no se ajusten a los requisitos previstos en los apartados 2. 1 a 2.3 no serán admitidos para examen por el Grupo de Trabajo.

2.5 La secretaría acusará recibo de los proyectos de códigos a sus remitentes.

2.6 En concertación con el Presidente, la secretaría elaborará un informe en el que se determine si el proyecto de código presentado cumple o no los requisitos de admisión previstos en los apartados 2.1 a 2.3.

2.7 El Presidente decidirá si el proyecto de código presentado cumple los requisitos de admisión. Si el Presidente considera que no los cumple, informará a los miembros del Grupo de Trabajo y fijará un plazo de respuesta. Salvo que dos o más miembros del Grupo soliciten que el caso se someta a debate en la siguiente reunión del Grupo de Trabajo, la decisión del Presidente será notificada a los remitentes, junto con los motivos por los que se rechaza el proyecto.

Artículo 3 - Normas relativas a la elaboración del dictamen del Grupo de Trabajo.

3.1 Los proyectos de códigos presentados que cumplan los requisitos de admisión serán enviados a todos los miembros del Grupo de Trabajo.

3.2 En concertación con el Presidente, la secretaría formulará propuestas con vistas a la elaboración del dictamen, que serán debatidas por el Grupo de Trabajo. Dichas propuestas podrán preconizar la creación de grupos operativos o de trabajo específicos integrados por uno o más miembros del Grupo de Trabajo y asistidos por la secretaría podrán preconizar la aplicación de un procedimiento simplificado de examen a un código presentado, en particular cuando se trate de modificaciones o prórrogas de códigos existentes; y asesorarán al Grupo de Trabajo sobre la conveniencia de recabar la opinión de las personas a las que se refieran los datos procesados o sus representantes, y de otros interesados.

3.3 Con ocasión de un primer debate sobre el código presentado, el Grupo de Trabajo determinará, basándose en las propuestas contempladas en el apartado 3.2, el procedimiento que se seguirá para la elaboración y emisión del dictamen.

3.4 Durante la elaboración del dictamen podrá contactarse con los remitentes del proyecto de código u otros interesados, para obtener mayor información o aclaraciones o para debatir de las mejoras que requiere el código presentado, con vistas a la posterior presentación, en su caso, de un proyecto de código revisado.

3.5 El Grupo de Trabajo podrá dar otras pautas o instrucciones para la elaboración de un dictamen en relación con el código presentado.

Artículo 4 - Normas relativas al dictamen del Grupo de Trabajo y la notificación del mismo a los interesados.

4.1 El Grupo de Trabajo determinará si los códigos de conducta presentados se atienen o no a lo dispuesto en las Directivas y, en su caso, a las disposiciones nacionales adoptadas en cumplimiento de las mismas, reúnen las oportunas condiciones de calidad y coherencia interna y ofrecen un valor añadido suficiente con respecto a las Directivas y otras normas sobre protección de datos aplicables, evaluando, en particular, si el proyecto de código se centra suficientemente en los problemas específicos de protección de datos de la organización o el sector al que está destinado a aplicarse, y si aporta soluciones suficientemente claras a dichos problemas.

4.2 El Grupo de Trabajo notificará su dictamen a los remitentes del proyecto de código y otros interesados. Cuando el dictamen no sea favorable, se indicarán los motivos en los que se fundamentan sus conclusiones.

4.3 La Comisión podrá hacer público el dictamen del Grupo de Trabajo por los medios adecuados.

Hecho en Bruselas, el 10 de septiembre de 1998

Por el Grupo de Trabajo
El Presidente
P.J. HUSTINX

MEMORIA DE 1998 - ANEXO XI - POSICIONES COMUNES DEL GRUPO DE BERLÍN

Posición Común sobre la
Protección de Datos y los motores de búsqueda en Internet.
(Adoptada en la 23 Reunión del IWG en Hong Kong SAR, China el 15 de abril de 1998)

En la actualidad, Internet alberga una gran cantidad de información sobre las más diversas disciplinas que uno pueda imaginar. Por esta razón y durante los últimos años, los motores de búsqueda de información en Internet se están convirtiendo en los mecanismos más populares para encontrar la información concreta que nos interesa de entre toda la que se encuentra disponible en la red.

Además de para lo anterior, los motores de búsqueda pueden ser también utilizados para la búsqueda de datos personales. En este caso, el resultado de la búsqueda podría facilitar el perfil de comportamiento de un persona concreta en la red. Los motores de búsqueda podrían también ser susceptibles de ser utilizados como herramientas de explotación masiva de datos ("data mining"). A medida que Internet se populariza cada vez más como el mecanismo para el intercambio de información y el desarrollo de otras actividades (ej. comercio electrónico), se incrementan los riesgos para sus usuarios desde el punto de vista de la privacidad.

Además, los proveedores de motores de búsqueda tiene la capacidad de establecer perfiles detallados sobre lo que interesa a sus usuarios.

Las Autoridades de Privacidad y Protección de Datos han seguido con especial interés en el pasado las posibilidades de establecer perfiles de ciudadanos. En la actualidad, las tecnologías disponibles en Internet hacen que estas posibilidades sean, hasta cierto punto, técnicamente posible sobre una base global. Incluso, la implantación prevista de programas filtro con fines de privacidad pueden llevar asociado un riesgo adicional, si las preferencias definidas por el usuario en dichos programas son registradas por los motores de búsqueda. El Grupo de Trabajo recomienda que cualquier sistema de filtrado se diseñe de manera que las preferencias de privacidad especificadas por los usuarios no puedan ser accesibles a los administradores de las ubicaciones Web ni a terceros.

Finalmente, con respecto a la divulgación o publicación de datos personales, el Grupo de Trabajo quiere recordar dos principios sobre los que se sustenta esta posición común:

Los datos personales hechos públicos voluntariamente por el usuario permanecen bajo la protección asociada a su naturaleza;
Cualquier individuo debería tener el derecho, en cualquier momento y en cualquier caso, a objetar acerca de la divulgación de datos sobre su persona en una Web, y debería tener el derecho a requerir que la finalidad, para la cual divulga sus datos, sea respetada.

Recomendaciones:

El Grupo de Trabajo ya se ha preocupado en el pasado por los problemas de protección de datos y privacidad relacionados con el uso de Internet y ha elaborado recomendaciones para resolver estos problemas. Los organismos reguladores pueden restringir que los motores de búsqueda realicen búsquedas de nombres así como prohibir la recopilación masiva de perfiles de búsqueda. Sin embargo, dada la estructura internacional de Internet, no es posible regular por completo Internet utilizando mecanismos jurídicos.

Los usuarios de Internet pueden a la vez ser proveedores de información. Por este motivo, deben ser conscientes de que cada bit de información personal que publican en la red (ej. cuando crean su propia página en la Web, servicio ofrecido por la mayoría de los proveedores de acceso) puede ser utilizado por terceros con el fin de establecer perfiles. Los usuarios deberían tener la opción de poder limitar la utilización de sus datos para determinados propósitos.

Mas aún, los mensajes en los grupos de noticias pueden ser indexados y trazados por los motores de búsqueda, incorporando información a perfiles del tipo *"quien expresó una determinada opinión sobre una materia concreta"*. Una manera de reducir esta amenaza a la privacidad podría pasar por la utilización de seudónimos cuando se participa en servicios de noticias (*news*). Los proveedores de servicios de Internet y los fabricantes de *software* deberían de ofrecer servicios de seudónimo a sus clientes. La utilización de estos servicios podría minimizar la amenaza a la privacidad de los usuarios cuando se utiliza un motor de búsqueda. Al mismo tiempo, los usuarios deben ser conscientes de los riesgos que conlleva el participar en servicios de noticias utilizando direcciones de correo electrónico reales e incluso la identidad real.

Los usuarios deberían tener también la posibilidad de poder limitar que los datos personales sean recogidos por los motores de búsqueda. Ello puede conseguirse definiendo opciones del tipo *"no-robots"* en el *software* de la Web. Sin embargo, esta funcionalidad depende de que los proveedores de servicios de motores de búsqueda la faciliten.

Se hace necesario, por lo tanto, establecer la conformidad de los motores de búsqueda con los principios básicos de protección de datos mediante un procedimiento de verificación. Para establecer el procedimiento adecuado (ej. auditoria, evaluación, certificación) se debería realizar un estudio específico en el que se tengan en cuenta las diferentes situaciones.

El contrato o acuerdo establecido entre el usuario del motor de búsqueda y el proveedor del servicio de búsqueda

debería recoger la obligación para el proveedor de cumplir con la Directiva Europea de Protección de Datos. Se deberían incorporar a dichos contratos cláusulas del tipo: *"El proveedor del motor de búsqueda no registrará ninguna información relativa a la búsqueda ni sobre el usuario del motor de búsqueda. No se mantendrán datos sobre la búsqueda una vez ésta haya concluido".*

Se deberían adoptar también tecnologías avanzadas de privacidad con el fin de proteger la privacidad del individuo. Siempre que un usuario lo requiera se debería facilitar un *Protector de Identidad* que facilite el anonimato del usuario durante la sesión. El intercambio de datos debe técnicamente mantenerse de acuerdo al principio de proporcionalidad adoptado en las Guías de la OCDE de 1980 y en la Directiva EC de 1995.

Con el fin de imposibilitar el análisis de flujo de tráfico, se deberían adoptar medidas de seguridad en la comunicación entre extremos (*end-to-end*) como por ejemplo rellenar los tiempos vacíos con cadenas aleatorias de bits.

Posición común sobre la Responsabilidad Pública en relación
con la interceptación de comunicaciones privadas.
(Adoptada en la 23 Reunión del IWG en Hong Kong SAR, China el 15 de abril de 1998)

1. Si bien el individuo tiene la expectativa razonable de disponer de comunicaciones privadas, el interés público puede, en determinadas ocasiones, justificar la interceptación de dichas comunicaciones por las autoridades competentes.

2. La interceptación de comunicaciones debería únicamente ser autorizada en circunstancias excepcionales, en casos justificados y siempre sujetas a las correspondientes garantías - tales como autorización judicial, notificación a los individuos, limites de uso, y requerimientos para la destrucción de las cintas y las transcripciones. (Este documento no se opone a las interceptaciones mencionadas, ni a las que se requieran por razones de operaciones técnicas en la red o para las finalidades propias de los organismos reguladores.)

3. Las interceptaciones de comunicaciones que se realizan de acuerdo a la ley se hacen sin conocimiento de los interesados como es obvio. Sin embargo, y de acuerdo a los principios de transparencia, y responsabilidad, deben establecerse mecanismos que aseguren al público que dichas interceptaciones son llevadas a cabo dentro de la ley.

4. Estos mecanismos deberían incluir los siguientes aspectos:
* *Registro de las grabaciones.*
* *Mecanismos de monitorización y auditoria:*
* *Informes públicos y periódicos.*

5. Registro de las grabaciones: Las agencias encargadas de efectuar las interceptaciones deberán mantener un registro de las grabaciones que efectúen así como su justificación. Esto se aplicará también al proveedor de telecomunicaciones que se vea afectado.

6. Mecanismos de monitorización y auditoria: Un órgano independiente de la agencia que efectúe las interceptaciones desempeñará el papel de comprobar que las mismas se efectúan de acuerdo a la ley, para ello deberá disponer de las competencias necesarias y de los recursos necesarios para poder realizar las oportunas inspecciones.

7. Informes públicos y periódicos: Periódicamente se publicarán informes que a nivel general pondrán de manifiesto el grado de intrusión en la privacidad. Entre las estadísticas a incluir en estos informes deberán figurar:
* El número de interceptaciones autorizadas realizadas y su duración.
* El número de solicitudes de interceptación denegadas por la autoridad.
* Autorizaciones con condiciones o características especiales (ej. autorizaciones para entrar en lugares privados).
* El número de interceptaciones realizadas y las personas identificadas.
* Los diferentes métodos de interceptación (teléfono, fax, e-mail, mensajería, mensajes vocales, etc.).
* Las clases generales o lugares donde se han realizado las interceptaciones (oficinas, domicilios, coches, etc.).
* La naturaleza de los delitos que se investigaban.
* Los resultados y el grado de efectividad que las interceptaciones han tenido en el esclarecimiento de los delitos perseguidos.
* El coste asociado a las interceptaciones.

El informe deberá presentar la información de forma clara y legible y deberá incluir las tendencias y las características significativas de la actividad de interceptación durante el periodo cubierto por el informe.

Posición Común
relacionada con las búsquedas inversas en directorios.
(Adoptada en la 23 Reunión del IWG en Hong Kong SAR, China el 15 de abril de 1998)

Se entiende por búsqueda inversa el obtener la identidad y/o dirección de una persona a partir de su número de teléfono, fax o dirección de correo electrónico. Este servicio puede tener importantes efectos negativos para la privacidad y debería estar sujeto a reglas específicas de protección de los derechos de las personas.

Sin embargo, algunos estados tienen regulaciones que prohiben a los proveedores de servicios de telecomunicaciones, que operan en su territorio, prestar este tipo de servicios. En este contexto, el IWG desea hacer las siguientes observa-

ciones:

- En el marco de las relaciones privadas entre las personas, la existencia de este tipo de servicios, sin reglas específicas de protección, puede representar una amenaza para la privacidad.

- La utilización comercial de este servicio puede tener consecuencias para personas que específicamente ante una oferta comercial únicamente proporcionan su número de teléfono.

- La finalidad de un repertorio con búsqueda inversa es diferente que un repertorio tradicional de abonados. Un directorio telefónico permite obtener el número de teléfono de una persona conocida, a partir de su nombre y un criterio geográfico, mientras que la finalidad de una búsqueda inversa es la obtención de la identidad y la dirección de un abonado del que únicamente es necesario conocer su número de teléfono.

- De hecho, un abonado podría solicitar no aparecer en un repertorio tradicional de abonados o apareciendo, impedir la utilización de esos datos para fines comerciales y al mismo tiempo querer figurar en un directorio inverso.

- Aunque el recurso de los directorios inversos puede servir a los intereses legítimos en algunos casos especiales de emergencia y seguridad pública, el proporcionar los datos de un usuario a partir de su número de teléfono, sin disponer del consentimiento del afectado constituye un tratamiento desleal de la información.

- Los tratamientos relacionados con la facturación detallada y la presentación del número de teléfono llamante, deben ser contemplados, a partir de ahora, desde la óptica de la existencia de los directorios inversos.

En este contexto, si los directorios inversos no se prohiben por las legislaciones nacionales se acuerda:

- Existen servicios que requieren el consentimiento expreso y previo del afectado. Al menos, se debe garantizar el derecho a objetar y el derecho de acceso, generalmente reconocidos por las legislaciones nacionales e internacionales en materia de protección de datos.

- En todo caso es necesario dotar a los usuarios del derecho a ser informados por el que preste los servicios de telefonía o de correo electrónico, de la existencia del servicio de búsquedas inversas y, si el consentimiento expreso no es requerido, reconocer el derecho del usuario a no prestarse a tal servicio (derecho de objeción) libre de coste.

Posición común
sobre
Tecnologías Avanzadas de Privacidad (PET) (ej. P3P1) en WWW.
(Adoptada en la 23 Reunión del IWG en Hong Kong SAR, China el 15 de abril de 1998)

El IWG recoge favorablemente cualquier iniciativa que desarrolle tecnologías que ayuden a mejorar la privacidad de los usuarios en la WWW.

En este sentido, el IWG sigue con interés el proyecto *Platform for Privacy Preferences Project* (P3P) promovido por el WWWC.

No obstante, se considera que en dicho proyecto todavía existen aspectos que han de ser clarificados en relación con la seguridad, calidad de datos, periodos de retención de la información así como los derechos de acceso y rectificación que han de ser contemplados. En este contexto se presentan las condiciones esenciales que deberían ser tenidas en cuenta por cualquier plataforma tecnológica para la protección de la privacidad en la WWW con el objetivo de evitar la recolección sistemática de datos personales:

1. La tecnología por si misma nunca podrá ser la solución para garantizar la privacidad en la Web. Se necesita además un marco regulatorio (legislación, códigos de conducta, contratos, auditorias independientes y recursos legales para el individuo).

2. Cualquier usuario debería tener la opción de visitar una Web de forma anónima. Este precepto debería aplicarse incluso en las descargas de información de dominio público. En este último caso, la información personal únicamente podría ser procesada mientras el usuario se encuentre leyendo información de la Web, excepto para las conexiones de datos que será el necesario para los propósitos de seguridad.

3. Se requerirá el consentimiento previo e informado del afectado como paso previo al tratamiento de sus datos personales. Mas aún, los datos personales no deberán transmitirse de forma automática hacia una Web sin una previa notificación al afectado, quien deberá tener siempre la opción de bloquear dicha transmisión.

4. Se considera de vital importancia realizar un seguimiento del desarrollo del proyecto P3P.

1 P3P es una iniciativa del W3C cuyo objetivo es elaborar un protocolo mediante el cual, usuario y Web negocian las preferencias relativas a la privacidad, pudiendo el usuario decidir si acepta los términos de la Web antes de navegar a través de ella. (ver http://www.w3.org/P3/Overview.html).