AGENCIA
DE
PROTECCION DE DATOS

MEMORIA
1994

MEMORIA DE 1994 - PRESENTACIÓN

El año 1994 ha supuesto un avance significativo desde el punto de vista de la aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Durante el mismo se ha hecho realidad la presencia de la Agencia de Protección de Datos como tal, se la ha dotado de la necesaria infraestructura tanto presupuestaria como de edificio y personal, se ha llevado a cabo el desarrollo de los programas informáticos necesarios para lograr un correcto funcionamiento del Registro General de Protección de Datos y un mejor servicio de información al ciudadano. Igualmente se han diseñados los servicios de la Inspección de la Agencia y de la Secretaría General de la misma que atiende y cubre las necesidades del resto de los órganos que componen su estructura orgánica.

A lo largo de dicho año se ha llevado a término el desarrollo reglamentario de la Ley Orgánica, a excepción de lo establecido en los artículos 4.5 y 9, puntos 2 y 3, de la misma, mediante la aprobación del Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, se ha realizado la campaña de publicidad necesaria y previa para la inscripción de los ficheros de titularidad privada y pública en el Registro de la Agencia con un resultado que ha superado las doscientas mil inscripciones de ficheros afectando a más de cien mil empresas privadas, y ello tan sólo en 6 meses de campaña.

Se han iniciado, por otro lado, la tramitación de los correspondientes expedientes sancionadores, los informes preceptivos de disposiciones legales y reglamentarias que desarrollan la Ley Orgánica o inciden en materias propias de la misma. Igualmente se ha procedido a la inscripción del primer código tipo.

En el plano internacional, aparte de asistir a la Conferencia Internacional de Agencias de Protección de Datos celebrada en Septiembre de 1994, así como a las reuniones precisas para la implantación del Sistema de Información Schengen o la discusión del Proyecto de Directiva Europea en materia de protección de datos, se logró que se celebrara en Madrid, en Mayo de 1994, la reunión de Agencias de Protección de Datos europeas, dando a conocer a las mismas el nacimiento y presencia de la Agencia española.

No quisiera dejar de resaltar la inestimable colaboración que en todas las tareas de la Agencia ha venido prestando el Consejo Consultivo de la misma. Las reuniones periódicas efectuadas con carácter mensual y la dedicación de cada uno de sus miembros a las tareas de la protección de datos personales han sido, son y serán imprescindibles para la defensa de la intimidad dentro de nuestra sociedad.

La presente Memoria, que se remite a las Cortes Generales a través del Ministro de Justicia e Interior, recoge y amplía cada uno de los hechos anteriormente expuestos respetando el contenido fijado en el artículo 8 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

EL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

MEMORIA DE 1994 - FUNCIONAMIENTO DE LA AGENCIA

1. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

Dentro del ejercicio de las funciones a las que se refiere el artículo 36 de la Ley Orgánica, debe resaltarse por su interés el número en principio amplio, (14), de proyectos de disposiciones legales que han sido remitidas a la Agencia de Protección de Datos hasta el 31 de diciembre de 1994 a fin de dar cumplimiento a lo dispuesto en el citado precepto y en los apartados a) y b) del artículo 5 del Estatuto de la misma.

El contenido y categoría de los proyectos de disposiciones legales es muy variado abarcando desde una Ley Orgánica, la del Poder Judicial, a proyectos de ley, como el de reforma parcial de la Ley General Tributaria, el de Incompatibilidades del Gobierno de la Nación y de los Altos Cargos de la Administración del Estado, el de Medidas Fiscales, Administrativas y de Orden Social; o proyectos de Reales Decretos y Ordenes Ministeriales y proyecto de Orden de la Consejería de Sanidad de la Junta de Comunidades de Castilla-La Mancha.

Dentro de la categoría de informes preceptivos de los proyectos de disposiciones generales de desarrollo de la Ley Orgánica, debe citarse el informe emitido respecto del Real Decreto por el que se desarrollaban reglamentariamente determinados preceptos de aquélla y que se convirtió en el Real Decreto 1332/1994, de 20 de junio.

Como ya se examina en otro lugar de esta Memoria, se ha producido cierto grado de incumplimiento en cuanto a la remisión de proyectos a fin de dar por cumplido el trámite del informe preceptivo. Ello determinó que la Agencia remitiera a los órganos de la Administración Central y a los correspondientes autonómicos una comunicación tendente a poner de manifiesto la existencia de aquella obligación.

Dentro de los incumplimientos producidos merece destacarse, por afectar de manera muy directa a la Ley Orgánica, el Proyecto de Ley de Regulación del Uso de la Informática en el tratamiento de datos personales por la Comunidad de Madrid, que con fecha 7 de diciembre de 1994 se ha publicado en el Boletín Oficial de la Asamblea de Madrid.

Se acompaña como anexo número 1 relación de los proyectos de disposiciones generales informados por la Agencia de Protección de Datos a 31 de diciembre de 1994.

2. CONSEJO CONSULTIVO

El Consejo Consultivo, previsto en el artículo 37 de la Ley Orgánica, y en los artículos 18 a 22 del Real Decreto 428/1993, de 26 de marzo, 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 integrado por los siguientes miembros:

Presidente:
***** D. Juan José Martín-Casallo López, **Director de la Agencia de Protección de Datos.**
Vocales:
***** D. Carlos Navarrete Merino, **Diputado propuesto por el Congreso de los Diputados.**
***** D. José Antonio India Gotor, **Vocal de la Administración Local propuesto por la Federación Española de Municipios y Provincias.**
***** D. Eloy Benito Ruano, **Vocal propuesto por la Real Academia de Historia.**
***** D. Eduardo Vilariño Pintos, **Vocal propuesto por el Consejo de Universidades.**
***** D. Adolfo Varela Cea, **Vocal propuesto por el Consejo de Consumidores y Usuarios.**
***** Dª. Elena Gómez del Pozuelo, **Vocal del sector de ficheros privados propuesta por el Consejo Superior de 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 Senador**, propuesto por la Cámara correspondiente.
* **Un Representante de la Administración Central**, designado por el Gobierno.
* **Un representante de las Comunidades Autónomas**, propuesto mediante acuerdo adoptado por mayoría simple de éstas.

Al tratarse de un órgano consultivo se ha pretendido articular su funcionamiento mediante reuniones mensuales, de forma que pudiera participar en el ámbito del funcionamiento regular de la Agencia. De este modo, a lo largo de 1994, ha sido convocado y se ha reunido en diez ocasiones en las que ha tenido conocimiento preciso de los problemas de todo tipo que iban surgiendo como consecuencia de la puesta en marcha de aquélla.

Ha colaborado de forma activa y valiosa en la redacción del informe preceptivo que sobre el desarrollo reglamentario de la Ley Orgánica se efectuó durante los primeros meses del año, igualmente en el proceso masivo de inscripción de ficheros que se llevó a cabo a lo largo del verano pasado y en la definición del contenido mínimo que ha de exigirse a los proyectos de códigos tipo presentados en la Agencia para su debida aprobación.

3. EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

OBJETIVOS Y LÍNEAS DE ACCIÓN

El artículo 38 de la Ley Orgánica y el artículo 23 del Estatuto de la Agencia configuran al Registro General como un órgano dependiente jerárquicamente del Director de la misma **al que le corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 13 a 15, de la Ley Orgánica.**

Entre sus funciones figuran:

* Instruir los expedientes de inscripción de los ficheros automatizados de titularidad pública o privada, así como los de modificación y cancelación del contenido de los asientos del Registro General de Protección de Datos.
* Instruir los expedientes de inscripción de códigos tipo.
* Instruir los expedientes de autorización de las transferencias internacionales de datos.
* Rectificar y suprimir de oficio los errores materiales de los asientos
* Expedir certificaciones de los asientos.
* Publicar una relación anual de los ficheros notificados e inscritos.

La Ley Orgánica, en su Disposición Adicional Segunda, reguló la obligación de notificar los ficheros existentes con anterioridad a su entrada en vigor habilitando un plazo legal de un año a partir de la misma. Este concluía el 31 de Enero de 1994, siendo posteriormente ampliado por Real Decreto Ley 20/1993, de 22 de Diciembre, hasta el 31 de Julio de 1994.

El Registro General se encontraba en su punto de partida. El Reglamento que desarrollaba determinados aspectos de la inscripción de ficheros estaba en fase avanzada de elaboración, pero no se publicaría hasta el 21 de Junio de 1994. Además de la proximidad de la fecha límite para que los responsables de ficheros notificasen su inscripción, quedaban aspectos muy importantes por definir e implementar:

* Organización funcional del Registro.
* Definición de puestos de trabajo y asignación de funciones.
* Definición de procedimientos administrativos de gestión interna y externa.
* Infraestructura de sistemas de información, comunicaciones y seguridad.

En esas circunstancias la Agencia hizo frente a importantes compromisos a corto plazo. La fase previa de implantación del Registro, tenía una importancia estratégica, era imprescindible ofrecer la imagen adecuada para obtener una respuesta eficaz y rigurosa en sus primeras actividades públicas.

Se hacía necesario cumplir previamente los siguientes requisitos:

* Adoptar las acciones encaminadas a garantizar el máximo nivel de respuesta tanto de entidades privadas como públicas.
* Informar a los responsables de ficheros de la obligación de inscribirlos en el Registro, en el plazo determinado por la Ley.
* Definir los procedimientos de inscripción y notificación.

ACTIVIDADES DE DIFUSIÓN DE LAS OBLIGACIONES DERIVADAS DE LA LEY

La ejecución del mandato legislativo sobre Protección de Datos llevaba consigo la tarea de informar a los ciudadanos de los derechos que les garantizaba la Ley Orgánica. Teniendo en cuenta la escasa divulgación que había tenido la misma, uno de los puntos críticos con los que se encontraba la Agencia, era la necesidad de informar en primer lugar, a los responsables de ficheros de datos personales, de cuáles eran las obligaciones que se derivaban de la Ley de Protección de Datos y los plazos establecidos para la inscripción de ficheros existentes con anterioridad a su entrada en vigor.

Uno de los requisitos imprescindibles para garantizar a los ciudadanos los derechos que la Ley les reconoce, era lograr el máximo nivel de respuesta de los responsables, creando para ello un catálogo con todos los ficheros notificados para su inscripción en el Registro.

Con este fin se diseñó una estrategia de información que se realizó a través de los siguientes medios y actividades.

Asesoramiento e Información

Para asegurar la adecuada difusión de los aspectos relevantes relacionados con los procesos de inscripción inicial, se mantuvieron reuniones, presentaciones y jornadas informativas con numerosas organizaciones públicas y privadas, entre las que cabe destacar:

Instituciones y Organismos Públicos

-Agencia Estatal de Administración Tributaria.
-Dirección General de Organización, Puestos de Trabajo e Informática (Ministerio para las Administraciones Públicas).
-Comisiones y grupos de trabajo del Consejo Superior de Informática.
-Ministerios con peculiaridades relevantes en materia de inscripción de ficheros:
  * Sanidad y Consumo (Hospitales y Centros de Salud)
  * Educación y Ciencia (Centros Públicos de Enseñanza)
  * Asuntos Exteriores (Oficinas Consulares)
  * Interior (Fuerzas y Cuerpos de Seguridad del Estado)
  * Defensa
-Comunidades Autónomas.
-Diputaciones Provinciales.
-Federación Española de Municipios y Provincias.
-Consejo Superior de Cámaras de Comercio, Industria y Navegación.
-Universidades.
-Banco de España.

Entidades y Organizaciones Privadas

-Asociación Española de Marketing Directo.
-Grandes empresas de distribución.
-Asociación Española de Banca.
-Entidad de Investigación Cooperativa entre Entidades Aseguradoras (ICEA)
-Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA)
-Asociación Nacional de Seguridad en Entornos Informáticos (ANSEI)
-Organización de Auditoría Informática (OAI)
-Colegios Profesionales.
-Comité de Investigación en Tecnologías de la Información.(CITI-TENEO)
-Confederación Española de Cajas de Ahorros (CECA)

Organismos homólogos de la Agencia de Protección de Datos en otros países:

-Visitas a: The Data Protection Registrar (Reino Unido)

Campaña de información

En prensa, servicio de información telefónica e información postal.

DISEÑO Y DESARROLLO DE LOS MODELOS DE NOTIFICACIÓN

El procedimiento de inscripción de un fichero se inicia con la recepción de la correspondiente notificación en la Agencia. Esta notificación fue previamente normalizada en base a lo dispuesto en la Ley Orgánica y el Reglamento, estructurando la información requerida en los apartados siguientes:

* Identificación del responsable del fichero.
* Dirección de la oficina o dependencia ante la que se pueden ejercer los derechos de acceso, rectificación o cancelación.
* Estructura o tipología de los datos que se pretenda tratar.
* Ubicación del fichero y sistema de tratamiento del mismo (si éste es de titularidad privada)
* Origen y procedencia de los datos.
* Finalidad y usos previstos.
* Colectivo del que se recogen datos (si el fichero es de titularidad pública)

* Cesiones y transferencias internacionales previstas.
* Medidas de seguridad.

La elección del soporte físico de los modelos de inscripción determinó en gran medida el éxito de la inscripción masiva en su conjunto. Se analizaron tres opciones:

-Emplear únicamente el soporte papel: utilizando un formulario preimpreso.
-Emplear únicamente el soporte magnético: generando un disquete con los programas de introducción y validación.
-Emplear ambos soportes.

Cada una de las opciones presentaba características y requisitos que condicionaban los procesos de distribución, costes de producción, depuración, etc. Asegurar una recepción masiva en los plazos legales, facilitar a los responsables de ficheros la notificación de los mismos, minimizar los costes de recogida de información y conseguir el máximo control en todo el procedimiento, fueron los factores determinantes que decantaron la elección por la tercera opción.

El modelo de notificación en soporte magnético se distribuyó en un sobre que contenía:

-Díptico con instrucciones y solapa para colocar el disquete.
-Disquete 3.5" HD etiquetado y serializado con un número secuencial distinto para todos los disquetes en código de barras.
-Sobre burbuja autofranqueado para devolver el disquete con las notificaciones.
-Bolsa-sobre para meter el conjunto de elementos.

El proceso se completó en las siguientes fases:

-Diseño y desarrollo del programa.
-Diseño de imagen de los sobres, dípticos y etiquetas.
-Especificación del programa de automatización del proceso de recepción masiva y de generación de las notificaciones a los responsables.
-Realización del programa de acuerdo con las especificaciones de recogida, validación y pruebas.

Se realizaron 78.000 sobres conteniendo todos los elementos destinados al declarante pudiéndose adquirir en Estancos, en Cámaras de Comercio o en la propia Agencia.

Los trabajos que se realizaron fueron los siguientes:

* Generación de los fotolitos o artes finales de todos los elementos de papelería.
* Impresión de 100.000 etiquetas, 100.000 sobres burbuja, 78.000 sobres bolsa y 78.000 disquetes.
* Duplicación de 78.000 disquetes con las opciones de formateo, copia verificación y verificación bit-a-bit.
* Serialización de los códigos de barras en las 100.000 etiquetas externas.
* Serialización de la etiqueta interna y duplicados con lectura automática de los códigos de barras.
* Manipulado (colocación de los disquetes y demás elementos en el sobre)
* Control antivirus sobre conjuntos finalizados.
* Entrega de partidas en Tabacalera y en Cámaras de Comercio.

Todas estas actividades se contrataron con empresas externas y se realizaron en el plazo aproximado de cuatro semanas. Los recursos humanos y materiales utilizados están recogidos en la siguiente tabla:

ACTIVIDAD	RECURSOS	HORAS
Imprenta	Subcontratada	---------
Duplicación	1 Operario 14 Duplicadoras 2 Etiquetadoras	50
Serialización Etiquetas	1 Operario 1 Impresora T. Termic.	8
Serialización Disquetes	1 Operario 14 Duplicadoras automáticas	18
Manipulados	8 Empleados	1.000
Entragas	1 Operario 1Furgón	24

INSTRUMENTACIÓN INFORMÁTICA DE LOS PROCEDIMIENTOS

Aplicación informática para la notificación en soporte magnético.

Con objeto de facilitar el proceso, se pensó en desarrollar una aplicación informática que permitiese validar con antelación a su envío la información requerida. De esta forma, se conseguiría agilizar el procesamiento de la misma, pues se obtendría en soporte informático, pero además normalizada y con la garantía de ser suficiente para proceder a la inscripción (siempre que los tratamientos notificados sobre los ficheros cumpliesen los requisitos de legalidad), con lo cual se evitaba en gran parte de las notificaciones tener que realizar requerimientos adicionales a los declarantes, con vistas a completar la información suministrada.

En caso de utilizar los modelos de papel, las notificaciones llevarían un proceso adicional de grabación y validación, sin la garantía de ser suficientes en términos legales para la inscripción.

La aplicación informática que se distribuyó para ordenadores personales compatibles permitía grabar los datos de la notificación a través de pantallas que se correspondían con cada uno de los apartados en que se estructura la misma. Una vez introducidos los datos relativos a cada uno de los ficheros que se desea notificar, se generaba sobre disquete un fichero con formato DOS incluyendo toda la información grabada (hasta 5000 caracteres por notificación). Este disquete, junto con una hoja firmada que incluía los datos del declarante, se recibía en la Agencia para su procesamiento.

Antes de la duplicación de los disquetes que se distribuirían con la aplicación, fue necesario conseguir la máxima garantía de que el disquete original no incluía ninguno de los virus conocidos, para lo cual se solicitó a una empresa especializada un diagnóstico de infección y una certificación de su resultado negativo.

Infraestructura informática de la Agencia

Para dotar a la Agencia de una infraestructura tecnológica capaz de hacer frente a las necesidades a corto plazo del Registro se realizó también una previsión a medio plazo para el resto de unidades: la Inspección de Datos y la Secretaría General. Se buscó un servidor multiusuario suficientemente dimensionado y conforme a las recomendaciones del Consejo Superior de Informática, como plataforma para la instalación posterior de un sistema gestor de bases de datos relacional.

La adopción de una **estrategia cliente/servidor** para configurar la arquitectura informática de la Agencia se justificaba plenamente si se considera el carácter claramente transaccional del sistema de información del Registro, en el que los tratamientos se basan en la lectura y escritura en un almacén centralizado de datos (las inscripciones de ficheros). Esta estrategia permite así la especialización del servidor en la gestión de los datos, centralizándose en él las labores de acceso y mantenimiento de integridad, gestión de perfiles de usuario, auditoría y planificación eficiente del almacenamiento. Los clientes (ordenadores personales) se limitan de esta forma a ofrecer un entorno gráfico e intuitivo para la manipulación de los datos, y a realizar las validaciones básicas sobre los mismos, antes de su almacenamiento.

Además, durante el período de inscripción masiva se utilizó un subsistema adicional integrado con el sistema informático definitivo que permitió la lectura masiva y automática de los disquetes recibidos. Este subsistema estaba constituido por un número variable de estaciones de lectura (ordenadores personales con un dispositivo que permitía cargar hasta 50 disquetes simultáneamente, lo que facilitó su manipulación) y una estación principal en la que se unían los ficheros leídos y se enviaban al servidor para su validación y análisis de adecuación a los supuestos legales. Cada disquete se recibía con el número de serie grabado magnéticamente, lo que facilitaba las tareas de clasificación. Para ello, mediante un lector óptico se comprobaba previamente que el número interno coincidía con el código de barras, asignándose un nuevo número en caso contrario.

DISTRIBUCIÓN DE LOS MODELOS DE NOTIFICACIÓN.

Los modelos normalizados publicados por Resolución de la Agencia de Protección de Datos de fecha 22 de Junio de 1. 994, en el B.O.E. de 23 de Junio, permitían a los responsables notificar la inscripción de sus ficheros, utilizando para ello fotocopia de dichos formularios.

En cuanto a la distribución de los disquetes, la vía principal fue TABACALERA S.A., a través de las expendedurías de la red nacional, donde se realizaba la venta al público.

Las cifras de distribución y venta por grandes zonas geográficas de la red de Tabacalera, a fecha 19 de Agosto de 1994, se presenta en el siguiente cuadro:

ZONA	Nº. DISQUETES	%
Zona Centro	16.050	83,53
Zona Catalano/Balear	14.000	91,65
Zona Norte	9.900	89,55
Zona de Levante	7.441	86,02
Zona Noroeste	5.685	86,37
Zona Sur	8.530	76,31

Los porcentajes representan el % de ventas sobre el número de disquetes distribuidos en cada zona. Las cifras para esta fecha son muy significativas, ya que se refieren a 61.556 disquetes, cifra muy similar a los 62.388 que se habían distribuido a 30 de diciembre de 1994.

Otro canal importante de distribución de disquetes fueron las Cámaras de Comercio, Industria y Navegación coordinadas a través de su Consejo Superior.

También es destacable que determinadas Diputaciones Provinciales, distribuyesen disquetes para facilitar la inscripción de ficheros a los organismos públicos y entidades privadas que lo requiriesen.

La propia Agencia de Protección de Datos distribuyó también los disquetes, bien mediante compra directa en sus oficinas, o bien mediante envío a través de Postal Express con pago por transferencia bancaria.

INSCRIPCIÓN MASIVA

Recepción de notificaciones de inscripción

Una vez abierto el plazo de presentación de las notificaciones de inscripción, se instrumentaron los procedimientos siguientes:

- Recepción en apartados de correos abiertos al efecto
- Apertura y clasificación de los envíos
- Rechazo de envíos incompletos.

En el caso de **notificaciones en soporte magnético**, el proceso consistía en:

* Someter a cada disquete a una verificación óptica con el fin de asegurar que el código de barras se correspondía con el grabado magnéticamente en el soporte.
* Verificar la inexistencia de virus.
* Comprobar el contenido del disquete.
* Asignar automáticamente un número de Registro de entrada.
* Transferir el contenido del disquete al servidor para su tratamiento.

Para hacer frente al previsible volumen de notificaciones a recibir en **soporte de papel** se definieron unos procedimientos y reglas de grabación que permitieron obtener en un corto espacio de tiempo un resultado susceptible de ser tratado de forma análoga al recibido en disquete, con la salvedad de que en este caso no se tenía la garantía de que la información obtenida fuese suficiente para la inscripción. En todo caso, el tiempo empleado en el tratamiento de las notificaciones recibidas en este tipo de soporte fue significativamente superior al empleado para procesar los disquetes (7 minutos de media por notificación en papel frente a 20 segundos, por notificación en disquete). A esto hay que añadir el enorme coste en términos de recursos humanos que supuso su grabación de forma normalizada.

Notificación a los Responsables

Una vez inscrito cada fichero, se hacía necesario notificar al responsable del mismo cuál era el contenido de la inscripción efectuada por el Registro, con objeto de subsanar posibles errores cometidos en la transcripción. Además, era preciso informar de los casos en los que la inscripción no se hubiera producido, bien por defectos de forma en la información recibida, bien porque no se cumplían los requisitos de legalidad establecidos por la Ley Orgánica.

Dado el volumen de información incluido en una inscripción, se estimó una media de 3 hojas para cada contestación, lo

que hizo necesario el establecimiento de un conjunto de normas conducentes a la correcta clasificación y ensobrado de los documentos de salida.

Del total de ficheros notificados en soporte magnético, sólo en un 1,2% de los casos fue preciso recabar su subsanación. En su mayor parte fue debido al hecho de declarar un almacenamiento de datos sensibles no ajustado a la legalidad (sin el consentimiento previo de los afectados) o una realización de cesiones o transferencias internacionales de datos sin reunir todas las garantías o condiciones que establece la Ley.

En el caso de las notificaciones procesadas en soporte papel, el número de ellas en las que fue preciso solicitar una subsanación superó el 16% del total. Ello se debió fundamentalmente a la declaración incompleta de apartados que la Ley establece como obligatorios para proceder a la inscripción.

Tras el período masivo de notificación, se hacía necesario adaptar los procedimientos previamente establecidos para hacer frente a las nuevas necesidades que surgían durante el funcionamiento habitual del Registro.

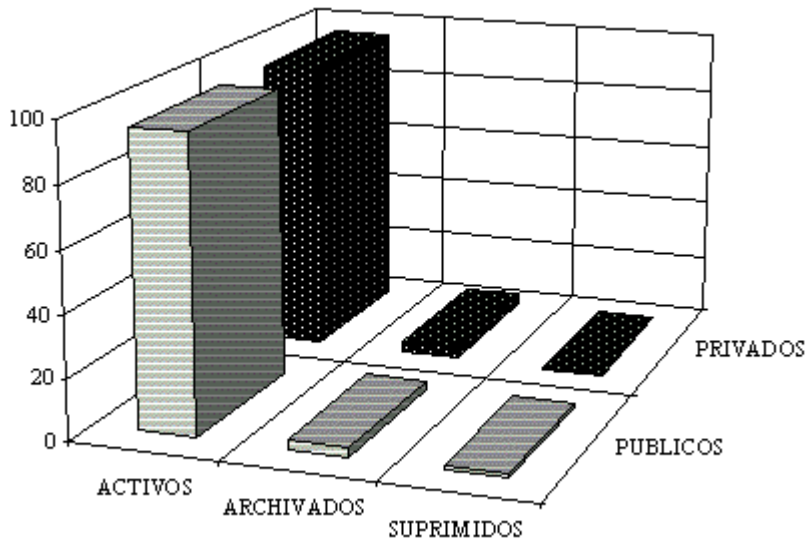
Para ello, se instrumentaron facilidades de consulta en función de distintos criterios (identificadores y encuadramiento administrativo del responsable, titularidad del fichero, tipología de datos, soporte de notificación,...), y se transformó el tratamiento por lotes de disquetes en la transmisión on line de su contenido al servidor, unificando dicho proceso con el Registro de entrada/salida, con vistas a su posterior integración.

RESUMEN DE LOS RESULTADOS OBTENIDOS DURANTE LA INSCRIPCIÓN

Ficheros inscritos según el estado en que se encuentran (Porcentajes sobre total de ficheros inscritos a 31 de Diciembre de 1.994)

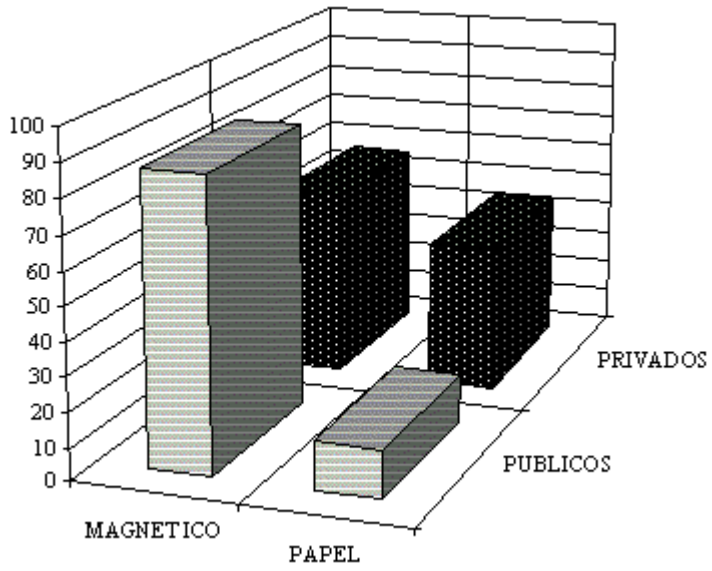
TITULARIDAD	ACTIV.	% TOTAL	ARCHIV.	% TOTAL	SUPRIM.	% TOTAL	TOTAL	% TOTAL
PRIVADA								
Soporte magnético	111.140	55,32	939	0,47	745	0,37	112.824	56,16
Soporte papel	80.957	40,30	6924	3,45	203	0,10	88.084	43,84
	192.097	**95,61**	**7.863**	**3,91**	**948**	**0,47**	**200.908**	**100,00**
PÚBLICA								
Soporte magnético	17.641	83,38	220	1,04	283	1,35	18.144	85,77
Soporte papel	2.557	12,09	437	2,07	16	0,08	3.010	14,23
	20.198	**95,47**	**657**	**3,11**	**299**	**1,43**	**21.154**	**100,00**
TOTAL								
	212.295		**8.520**		**1.247**		**222.062**	

Distribución de ficheros según TITULARIDAD y ESTADO en que se encuentran



(*) % sobre total de ficheros

Distribución de ficheros según TITULARIDAD y SOPORTE



(*) % sobre total de ficheros

El gráfico GR1 muestra el alto porcentaje de ficheros activos, en contraste con los archivados y suprimidos. A su vez, la evolución de las tres magnitudes es similar para ficheros públicos y privados.

El gráfico GR2 refleja un uso de soporte magnético superior al de soporte papel, tanto para la inscripción de ficheros públicos como privados. A su vez, el porcentaje de uso de soporte magnético en los ficheros de titularidad pública es sensiblemente superior al de los ficheros de titularidad privada.

Se consideran ACTIVOS los ficheros inscritos correctamente en el Registro General de Protección de Datos.

Se consideran ARCHIVADOS los ficheros cuya notificación no contiene la información preceptiva o no cumple las

exigencias legales, en uno o más apartados.

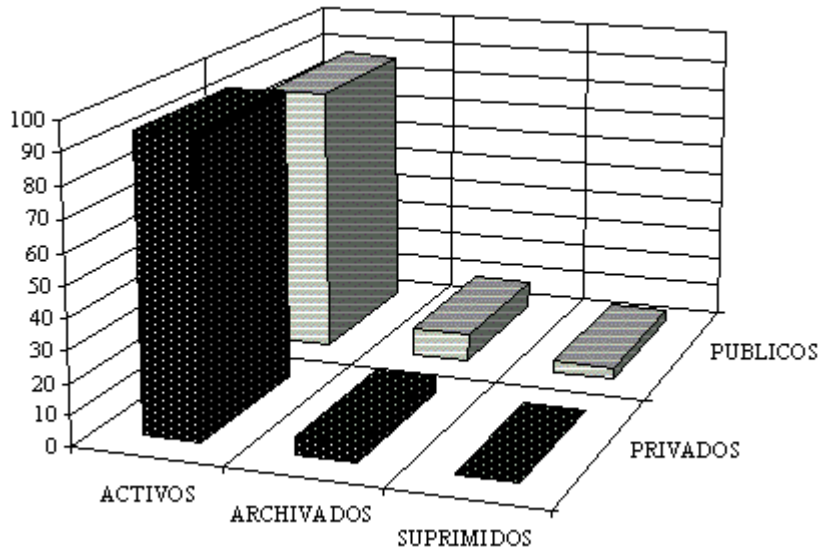
Se consideran SUPRIMIDOS, los ficheros que han causado baja en el Registro de Protección de Datos por diferentes causas, legales o formales.

Empresas y Organismos inscritos según el estado en que se encuentran sus ficheros (Porcentajes sobre total de empresas)

El número de Empresas Privadas y de Organismos Públicos inscritos está basado en el Código de Identificación Fiscal del Responsable.

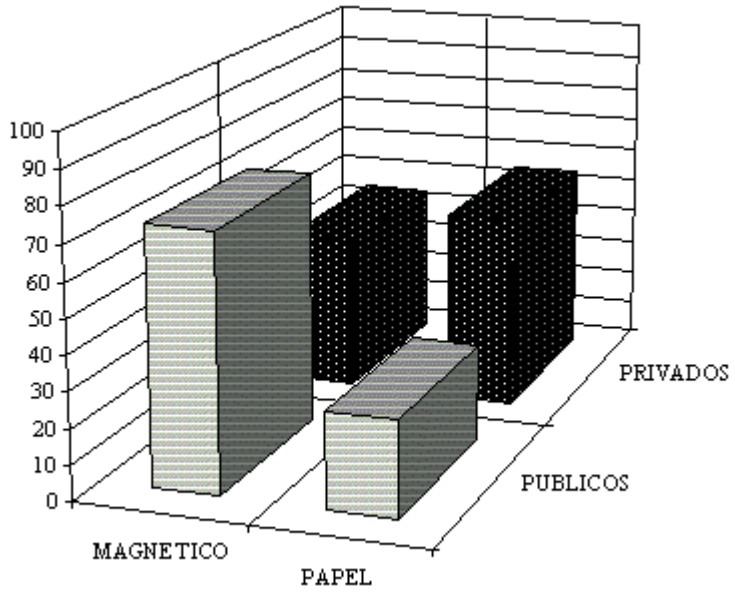
TITULARIDAD	ACTIV.	% TOTAL	ARCHIV.	% TOTAL	SUPRIM.	% TOTAL	TOTAL	% TOTAL
PRIVADA								
Soporte magnético	48.293	44,15	548	0,53	212	0,19	49.053	44,84
Soporte papel	54.676	49,97	5.528	5,05	148	0,14	60.352	55,16
	102.969	**94,12**	**6.076**	**5,55**	**360**	**0,33**	**109.405**	**100,00**
PÚBLICA								
Soporte magnético	2.267	66,04	115	3,35	111	3,23	2.493	72,62
Soporte papel	725	21,12	207	6,03	8	0,23	940	27,38
	2.992	**87,15**	**322**	**9,38**	**119**	**3,47**	**3.433**	**100,00**

Distribución de empresas y organismos según TITULARIDAD y el ESTADO de sus ficheros



(*) % sobre total de empresas y organismos

Distribución de empresas y organismos según TITULARIDAD y SOPORTE



(*) % sobre total de empresas y Organismos

El gráfico GR3 muestra cómo un elevado porcentaje de organismos públicos y empresas privadas han realizado correctamente la inscripción de sus ficheros, siendo ligeramente superiores las cifras de inscripción correcta para empresas privadas, lo que se traduce en un menor número de ficheros archivados y suprimidos para este sector.

El gráfico GR4 muestra que la mayoría de los organismos públicos han utilizado el soporte magnético para la inscrip - ción de sus ficheros, con una diferencia notable respecto del uso del soporte papel. En el caso del sector privado ocurre lo contrario, siendo menor la diferencia en el uso de ambos soportes que en caso de los organismos públicos.

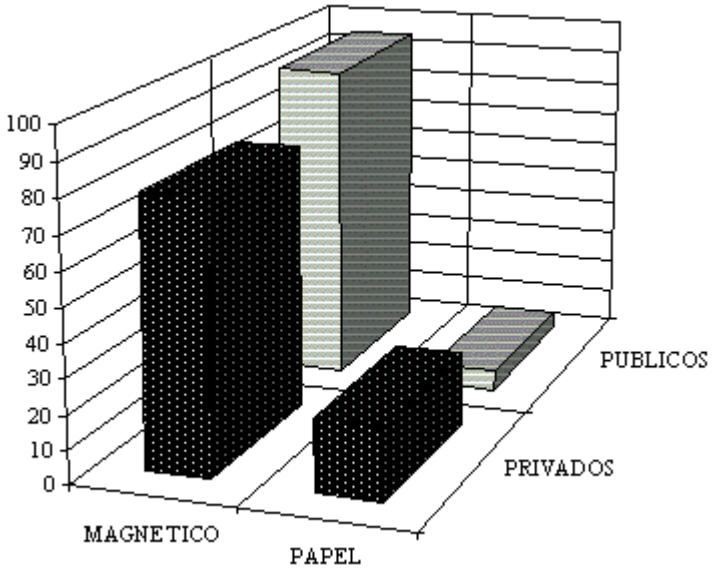
Ficheros inscritos según el estado en que se encuentran (porcentajes parciales en función del tipo de soporte utilizado)

TITULARIDAD	ACTIV.	% TOTAL	ARCHIV.	% TOTAL	SUPRIM.	% TOTAL	TOTAL	% TOTAL
PRIVADA								
Soporte magnético	111.140	57,86	939	11,94	745	78,79	112.824	56,16
Soporte papel	80.957	42,14	6924	88,06	203	21,41	88.084	43,85
	192.097	**100,00**	**7.863**	**100,00**	**948**	**100,00**	**200.908**	**100,00**
PÚBLICA								
Soporte magnético	17.641	87,34	220	33,49	283	94,70	18.144	85,77
Soporte papel	2.557	12,66	437	66,51	16	5,30	3.010	14,23
	20.198	**100,00**	**657**	**100,00**	**299**	**100,00**	**21.154**	**100,00**

Empresas y Organismos inscritos según el estado en que se encuentran sus ficheros (porcentajes parciales en función del tipo de soporte utilizado)

TITULARIDAD	ACTIV.	% TOTAL	ARCHIV.	% TOTAL	SUPRIM.	% TOTAL	TOTAL	% TOTAL
PRIVADA								
Soporte magnético	48.293	46,90	548	9,02	212	58,89	49.053	44,84
Soporte papel	54.676	53,10	5.528	90,98	148	41,11	60.352	55,16
	102.969	**100,00**	**6.076**	**100,00**	**360**	**100,00**	**109.405**	**100,00**
PÚBLICA								
Soporte magnético	2.267	75,77	115	35,71	111	93,28	2.493	72,62
Soporte papel	725	24,23	207	64,29	8	6,72	940	27,38
	2.992	**100,00**	**322**	**100,00**	**119**	**100,00**	**3.433**	**100,00**

Distribución ficheros ACTIVOS según TITULARIDAD y SOPORTE



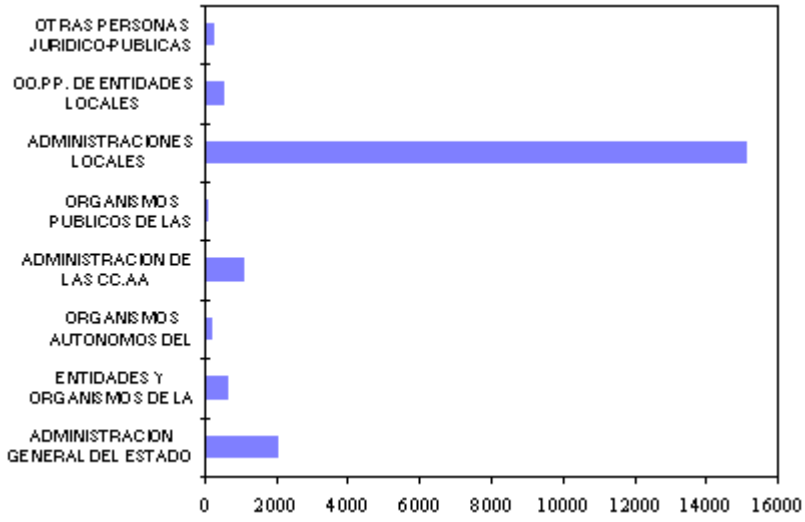
El gráfico GR5 muestra un mayor porcentaje de inscripción correcta realizada en soporte magnético, tanto para ficheros públicos como privados, siendo más acusada la diferencia en ficheros públicos. Esto se debe a que la aplicación informática relativa al soporte magnético realiza depuraciones y validaciones automáticamente.

Si se compara esta figura con la GR4, se deduce que la mayor fuente de errores en la inscripción proviene del soporte papel, tanto para ficheros públicos como para privados.

Distribución de ficheros públicos inscritos en 1994

Según tipo de Administración

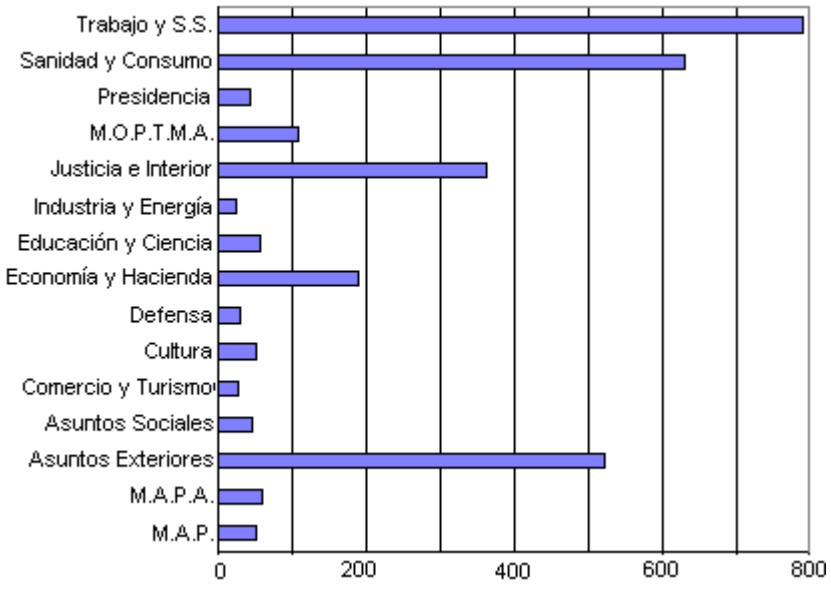
ADMINISTRACIÓN	FICHEROS	%
Administración General del Estado	2.034	10,06
Entidades y Organismos de la Seguridad Social	702	3,48
Organismos Autónomos del Estado	247	1,22
Administración de las Comunidades Autónomas	1.100	5,45
Organismos Públicos de la Comunidades Autónomas	116	0,57
Administraciones Locales	15.164	75,08
Organismos Públicos de Entidades Locales	535	2,65
Otras personas Jurídico-Públicas	300	1,49
TOTAL	**20.198**	**100,00**



El gráfico GR6 muestra que las tres cuartas partes de la inscripción pública corresponde a la Administración Local. Le sigue en importancia la Administración General del Estado, con un diez por ciento de la inscripción total. Del resto de la inscripción pública destacan la Administración de Comunidades Autónomas y las Entidades y Organismos de la Seguridad Social.

Administración General del Estado, Entidades y Organismos de la Seguridad Social y Organismos autónomos del Estado, distribuidos por Ministerios.

DEPARTAMENTO	FICHEROS	%
Ministerio de Agricultura, Pesca y Alimentación	59	1,98
Ministerio de Asuntos Exteriores	523	17,53
Ministerio de Asuntos Sociales	46	1,54
Ministerio de Comercio y Turismo	25	0,84
Ministerio de Cultura	51	1,71
Ministerio de Defensa	28	0,94
Ministerio de Economia y Hacienda	188	6,30
Ministerio de Educación y Ciencia	57	1,91
Ministerio de Industria y Energía	23	0,77
Ministerio de Justicia e Interior	363	12,17
Ministerio de la Presidencia	42	1,41
Ministerio de Obras Públicas, Transportes y Medio Ambiente	107	3,59
Ministerio de Sanidad y Consumo	630	21,12
Ministerio de Trabajo y Seguridad Social	790	26,48
Ministerio para las Administraciones Públicas	51	1,71
TOTAL	**2.983**	**100,00**

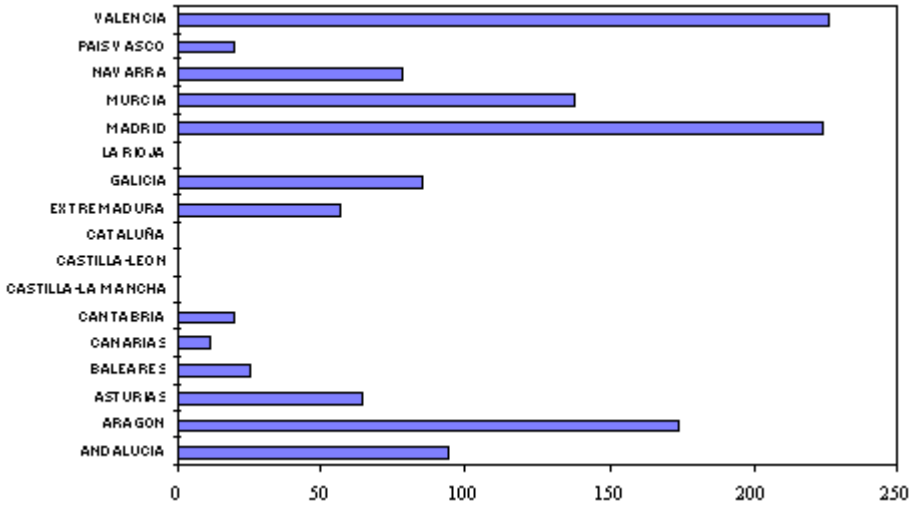


El gráfico GR7 muestra que los Ministerios con mayor número de ficheros inscritos son Trabajo y Seguridad Social , Sanidad y Consumo y Asuntos Exteriores. El número de ficheros inscritos por cada Departamento parece depender de dos variables:

- mayor o menor dispersión de sus centros directivos en el ámbito territorial.
- la centralización o distribución de sus sistemas de información.

Administración y organismos públicos de las Comunidades Autónomas

COMUNIDAD AUTÓNOMA	FICHEROS	%
Comunidad Autónoma de Andalucía	94	7,73
Comunidad Autónoma de Aragón	174	14,31
Comunidad Autónoma de Canarias	11	0,90
Comunidad Autónoma de Cantabria	20	1,64
Comunidad Autónoma de Extremadura	57	4,69
Comunidad Autónoma de Galicia	85	6,99
Comunidad Autónoma de la Región de Murcia	138	11,35
Comunidad Autónoma de las Islas Baleares	25	2,06
Comunidad Autónoma del País Vasco	20	1,64
Comunidad Autónoma del Principado de Asturias	64	5,26
Comunidad de Madrid	224	18,42
Comunidad Foral de Navarra	78	6,41
Comunidad Valenciana	226	18,59
TOTAL	**1.216**	**100,00**



En el gráfico GR8 se puede observar que las Comunidades que más ficheros han inscrito son la Comunidad Valenciana, Comunidad de Madrid y las Comunidades Autónomas de Aragón y Murcia.

Es destacable que a fecha de 31/12/94, las Comunidades de Cataluña, Castilla-La Mancha, Castilla-León y La Rioja no habían inscrito sus ficheros.

Administración Local y organismos públicos de entidades locales, distribuidos por provincia.

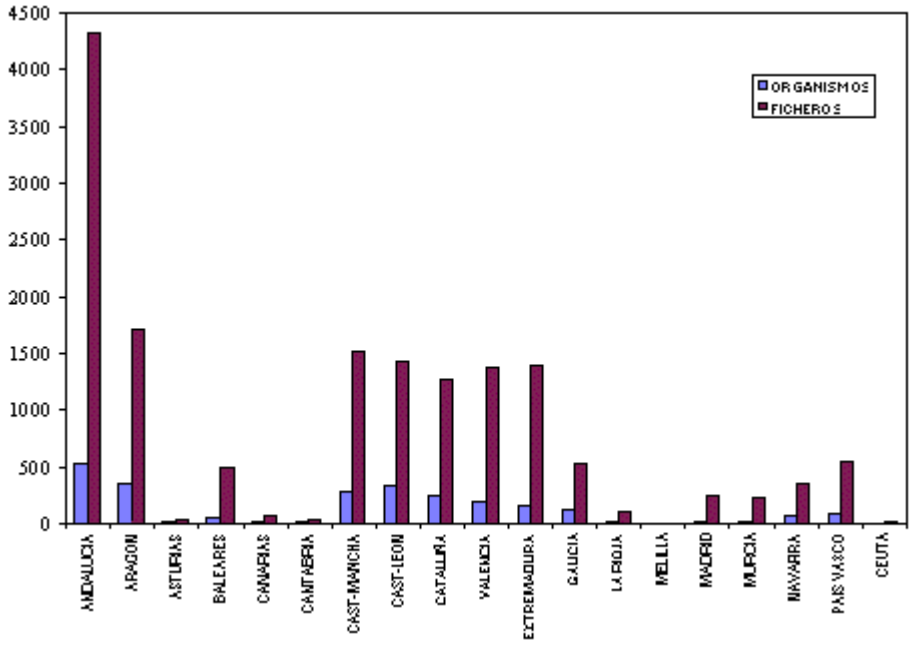
COMUNIDAD/PROVINCIA	ÓRGANOS	FICHEROS	%
ANDALUCÍA	**519**	**4.319**	**27,51**
ALMERÍA	103	939	
CÁDIZ	21	142	
CÓRDOBA	45	166	
GRANADA	159	1.111	
HUELVA	84	1.131	
JAÉN	9	60	
MÁLAGA	14	199	
SEVILLA	83	571	
ARAGÓN	**368**	**1.703**	**10,85**
HUESCA	131	434	
TERUEL	14	53	
ZARAGOZA	223	1.216	
ASTURIAS	**10**	**47**	**0,30**
BALEARES	**55**	**500**	**3,18**
CANARIAS	**16**	**78**	**0,50**
PALMAS,LAS	4	30	
SANTA CRUZ DE TENERIFE	12	48	
CANTABRIA	**14**	**38**	**0,24**
CASTILLA LA MANCHA	**288**	**1.514**	**9,64**
ALBACETE	65	334	
CIUDAD REAL	105	550	
CUENCA	65	387	
GUADALAJARA	8	49	
TOLEDO	45	194	
CASTILLA Y LEÓN	**338**	**1.423**	**9,06**
ÁVILA	3	6	
BURGOS	52	135	
LEÓN	162	771	
PALENCIA	8	36	
SALAMANCA	16	72	
SEGOVIA	6	65	
SORIA	6	25	
VALLADOLID	72	268	
ZAMORA	13	45	

COMUNIDAD/PROVINCIA	ÓRGANOS	FICHEROS	%
CATALUÑA	**253**	**1.270**	**8,09**
BARCELONA	100	528	
GIRONA	23	173	
LLEIDA	94	359	
TARRAGONA	36	210	
COMUNIDAD VALENCIANA	**199**	**1.377**	**8,77**
ALICANTE	123	923	
CASTELLÓN DE LA PLANA	24	182	
VALENCIA	52	272	
EXTREMADURA	**159**	**1.398**	**8,91**
BADAJOZ	152	1.361	
CÁCERES	7	37	
GALICIA	**131**	**523**	**3,33**
CORUÑA, LA	56	265	
LUGO	22	88	
ORENSE	10	49	
PONTEVEDRA	43	121	
RIOJA, LA	**24**	**100**	**0,64**
MADRID	**17**	**241**	**1,54**
MURCIA	**23**	**237**	**1,51**
NAVARRA	**69**	**359**	**2,29**
PAÍS VASCO	**81**	**549**	**3,50**
ÁLAVA	32	142	
GUIPÚZCOA	18	223	
VIZCAYA	31	184	
CEUTA	**1**	**23**	**0,14**
TOTAL	**2.561**	**15.699**	**100,00**

Otras Personas Jurídico-Públicas

	ÓRGANOS	FICHEROS
Cámaras de Comercio, Industria y Navegación	55	186
Universidades	18	88
Otros	5	26
TOTAL	**78**	**300**

Distribución de ficheros de la ADMINISTRACIÓN LOCAL por Comunidades Autónomas



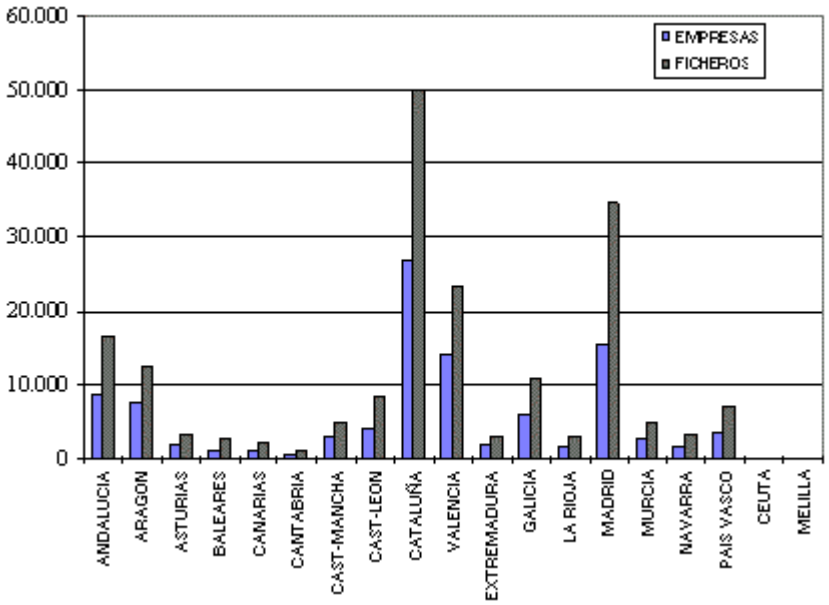
En el gráfico GR9 se observa que el mayor nivel de inscripción de ficheros de la Administración Local, corresponde a las Comunidades Autónomas de Andalucía, Aragón, Castilla-La Mancha, Castilla-León, Cataluña, Valencia y Extremadura. Ello es consecuencia del número de municipios existentes en sus ámbitos territoriales. También ha influido la coordinación que algunas Diputaciones Provinciales han realizado en la inscripción de los ficheros de los distintos Ayuntamientos de la Provincia. A su vez, se observa la relación directa entre el número de organismos y el número de ficheros inscritos.

Distribución de Empresas y ficheros por Comunidad Autónoma y Provincia. Ficheros de Titularidad Privada

	EMPRESAS	% TOTAL EMPRESAS	FICHEROS	% TOTAL FICHEROS
ANDALUCÍA	**8.838**	**8,58**	**16.624**	**8,65**
ALMERÍA	405	0,39	768	0,40
CÁDIZ	1.596	1,55	2.463	1,28
CÓRDOBA	1.057	1,03	2.335	1,22
GRANADA	719	0,70	1.364	0,71
HUELVA	689	0,67	1.112	0,58
JAÉN	817	0,79	1.717	0,89
MÁLAGA	1.895	1,84	3.219	1,68
SEVILLA	1.660	1,61	3.646	1,90
ARAGÓN	**7.698**	**7,48**	**12.567**	**6,54**
HUESCA	1.634	1,59	2.261	1,18
TERUEL	567	0,55	886	0,46
ZARAGOZA	5.497	5,34	9.420	4,90
ASTURIAS	**1.866**	**1,81**	**3.502**	**1,82**
BALEARES	**1.165**	**1,13**	**2.780**	**1,45**
CANARIAS	**1.144**	**1,11**	**2.104**	**1,10**
PALMAS, LAS	654	0,64	1.217	0,63
SANTA CRUZ DE TENERIFE	490	0,47	887	0,46
CANTABRIA	**543**	**0,53**	**1.189**	**0,62**
CASTILLA LA MANCHA	**3.023**	**2,93**	**5.218**	**2,72**
ALBACETE	992	0,97	1.511	0,79
CIUDAD REAL	602	0,58	1.070	0,56
CUENCA	519	0,50	867	0,45
GUADALAJARA	220	0,21	509	0,26
TOLEDO	690	0,67	1.261	0,66
CASTILLA Y LEÓN	**4.264**	**4,14**	**7.980**	**4,15**
ÁVILA	193	0,19	343	0,18
BURGOS	1.267	1,23	1.996	1,04
LEÓN	635	0,62	1.200	0,62
PALENCIA	231	0,22	444	0,23
SALAMANCA	519	0,50	1.301	0,68
SEGOVIA	276	0,27	475	0,25
SORIA	236	0,23	383	0,20
VALLADOLID	676	0,66	1.319	0,69
ZAMORA	231	0,22	519	0,27

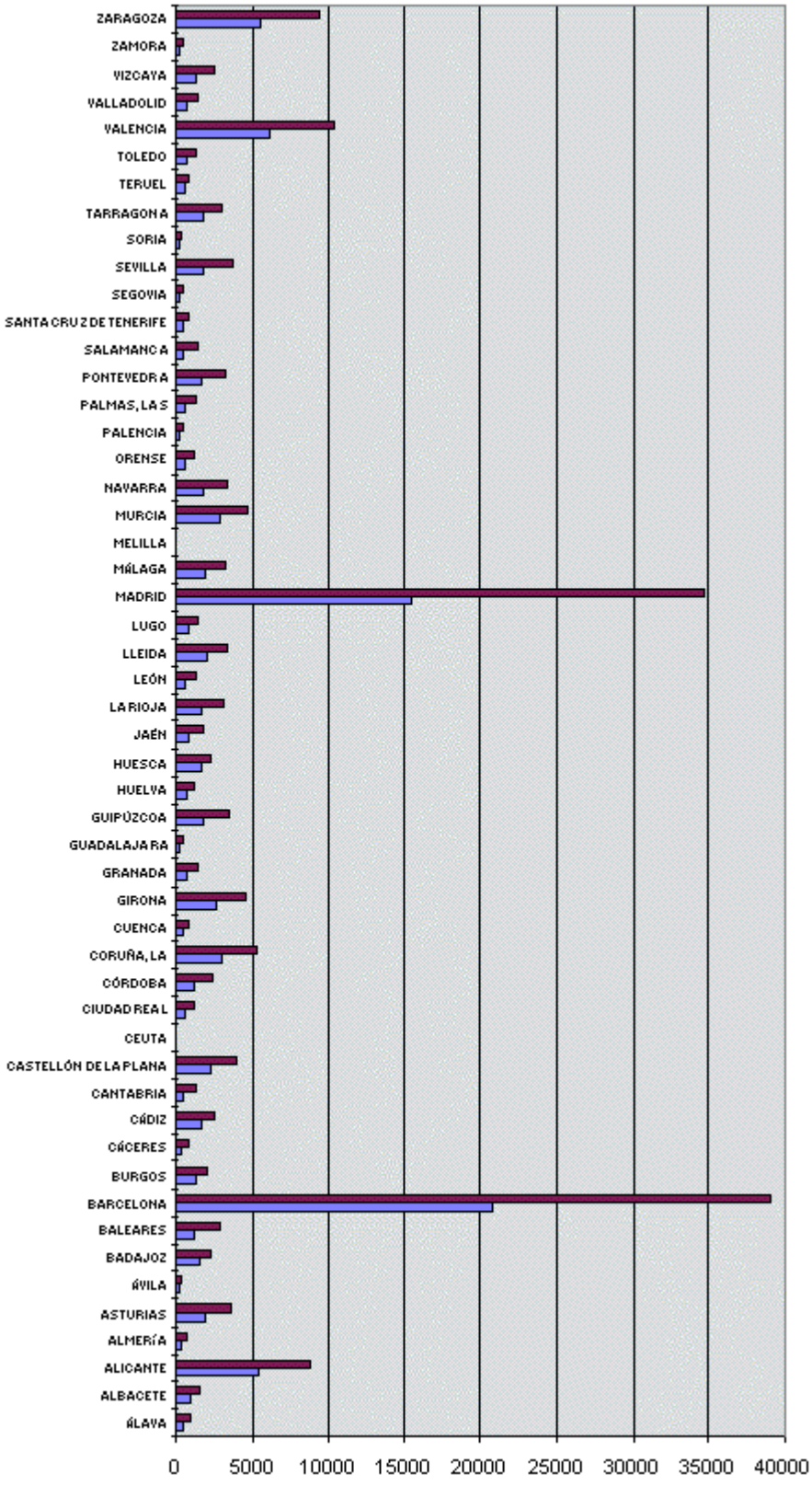
	EMPRESAS	% TOTAL EMPRESAS	FICHEROS	% TOTAL FICHEROS
CATALUÑA	**26.996**	**26,20**	**50.016**	**26,04**
BARCELONA	20.688	20,09	39.132	20,37
GIRONA	2.593	2,51	4.543	2,36
LLEIDA	2.018	1,95	3.357	1,75
TARRAGONA	1.697	1,65	2.984	1,55
EXTREMADURA	**1.857**	**1,80**	**3.159**	**1,64**
BADAJOZ	1.429	1,39	2.267	1,18
CÁCERES	428	0,41	892	0,46
GALICIA	**5.926**	**5,76**	**10.834**	**5,64**
CORUÑA, LA	2.941	2,86	5.304	2,76
LUGO	848	0,82	1.316	0,69
ORENSE	553	0,54	1.055	0,55
PONTEVEDRA	1.584	1,54	3.159	1,64
LA RIOJA	**1.654**	**1,61**	**3.070**	**1,60**
MADRID	**15.406**	**14,96**	**34.746**	**18,09**
MURCIA	**2.878**	**2,79**	**4.701**	**2,45**
NAVARRA	**1.724**	**1,67**	**3.267**	**1,70**
PAÍS VASCO	**3.514**	**3,42**	**6.902**	**3,59**
ÁLAVA	513	0,50	1.023	0,53
GUIPÚZCOA	1.777	1,73	3.422	1,78
VIZCAYA	1.224	1,19	2.457	1,28
COMUNIDAD VALECIANA	**13.725**	**13,38**	**23.246**	**12,10**
ALICANTE	5.425	5,27	8.804	4,58
CASTELLÓN DE LA PLANA	2.219	2,15	3.968	2,07
VALENCIA	6.081	5,96	10.474	5,45
CEUTA	**63**	**0,06**	**139**	**0,07**
MELILLA	**35**	**0,03**	**53**	**0,03**
TOTAL	**102.969**	**100,00**	**192.097**	**100,00**

Distribución de ficheros y empresas de TITULARIDAD PRIVADA por Comunidades Autónomas (Cifras Absolutas)

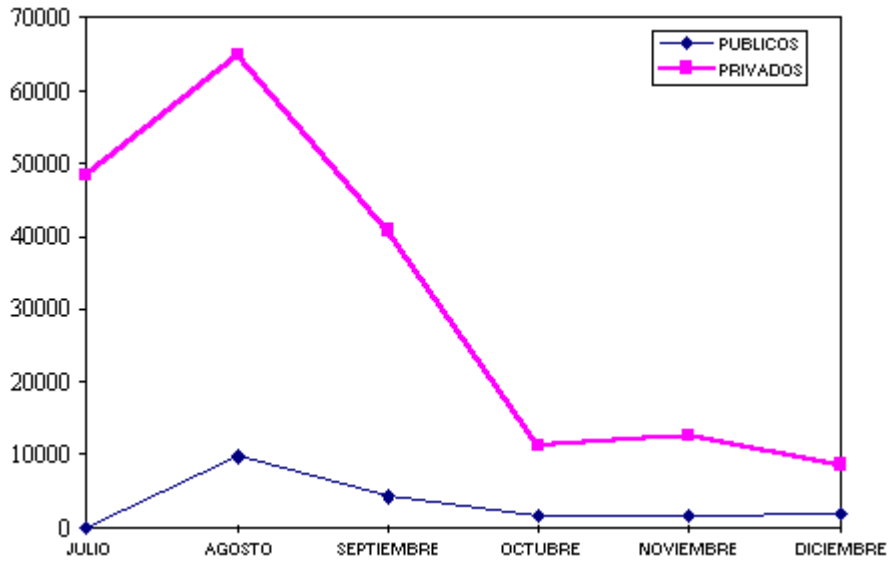


El gráfico GR10 muestra que las Comunidades Autónomas con mayor número de ficheros inscritos son Cataluña, Madrid y Valencia. Comunidades Autónomas con un gran número de provincias, como Andalucía, Castilla-La Mancha y Castilla-León presentan cifras de inscripción más bajas. El gráfico muestra que el número de ficheros inscritos por empresa es aproximadamente de dos para todo el territorio nacional.

Distribución de ficheros y empresas de TITULARIDAD PRIVADA por provincias
(Cifras Absolutas)



Evolución de ALTAS DE FICHEROS efectuadas en la base de datos del Registro a lo largo del año 1994



El gráfico GR12 muestra que el mayor número de inscripciones se realizó durante los meses de Agosto y Septiembre. A partir del mes de Octubre, se observa una suave tendencia decreciente en la inscripción. La tendencia en la inscripción es similar para ficheros públicos y privados. La incripción de ficheros públicos empezó a realizarse a partir del mes de Agosto.

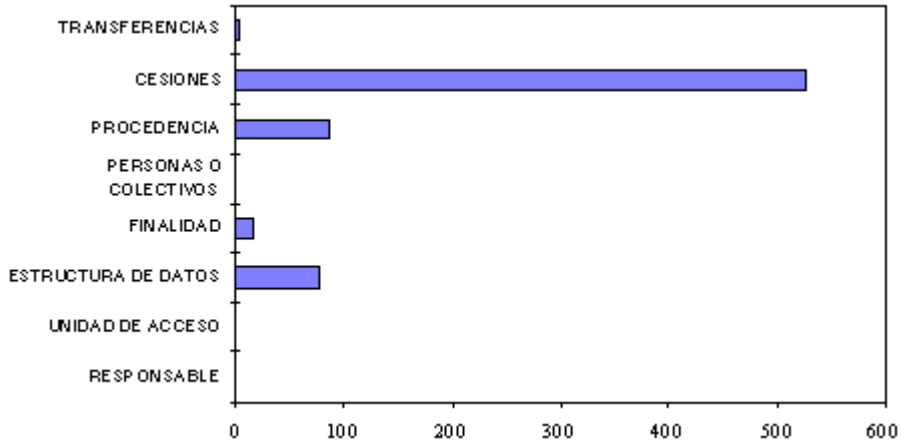
Ficheros notificados en 1994 cuya inscripción se ha archivado

Notificaciones de ficheros que no contenían la información preceptiva o no cumplían las exigencias legales. Porcentajes en función del número total de ficheros archivados.

Titularidad Pública

Apartado	Ficheros	%
Responsable	0	0
Unidad de Acceso	0	0
Estructura de Datos	77	11,72
Finalidad	15	2,28
Personas o Colectivos	0	0
Procedencia	85	12,94
Cesiones	526	80,06
Transferencias	4	0,61
Total Ficheros Archivados	**657**	

* Un fichero puede estar archivado por más de un apartado erróneo.

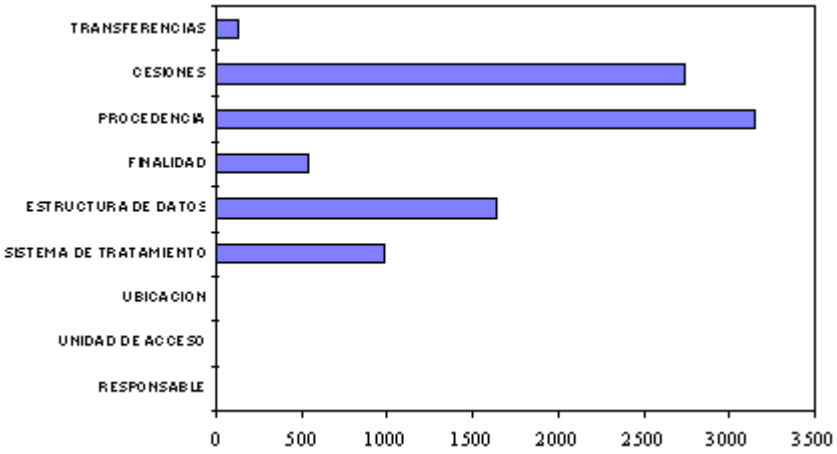


El gráfico GR13 muestra que el apartado de cesiones de datos ha sido la causa que ha producido mayor número de ficheros archivados. La procedencia de los datos y la estructura de los ficheros son los apartados que le siguen como causa de archivo más común.

Titularidad Privada

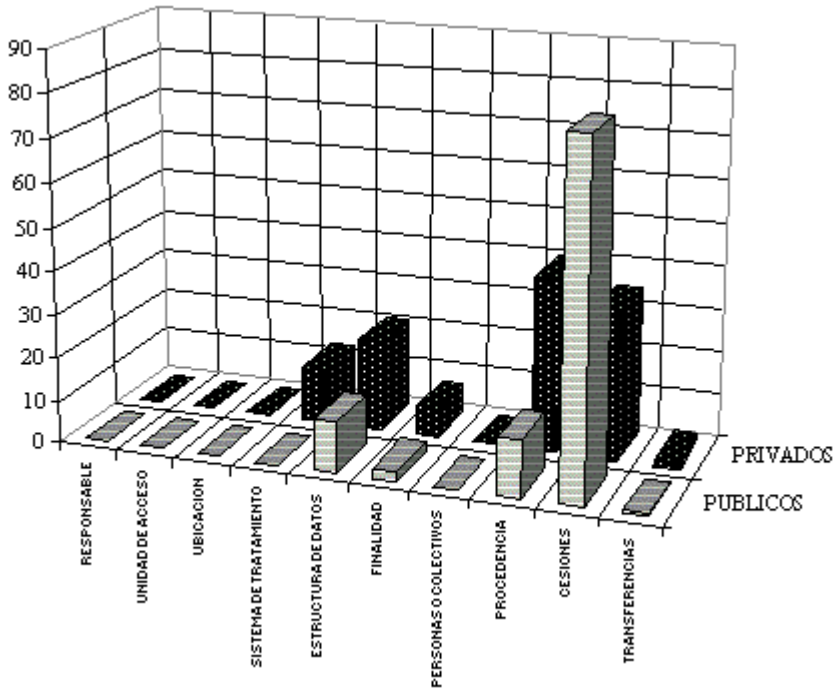
Apartado	Ficheros	%
Responsable	0	0
Unidad de Acceso	0	0
Ubicación	0	0
Sistema de Tratamiento	981	12,48
Estructura de Datos	1.640	20,86
Finalidad	537	6,83
Procedencia	3.157	40,15
Cesiones	2.738	34,82
Transferencias	131	1,67
Total Ficheros Archivados	**7.863**	

* Un fichero puede estar archivado por más de un apartado erróneo



En el gráfico GR14 se observa que la procedencia de los datos, las cesiones y la estructura de los ficheros son las principales causas de archivo de ficheros privados.

Ficheros notificados cuya inscripción se ha archivado, con indicación del apartado erróneo que ha producido el rechazo según TITULARIDAD



En el gráfico GR15 se observa que el apartado de cesiones es la causa más generalizada que ha producido el archivo de la notificación de ficheros en el sector público, mientras que los apartados de procedencia y estructura son causa más relevante de archivo para el sector privado.

El apartado de cesiones ha sido el que más dificultades de interpretación ha tenido para los responsables de ficheros públicos y privados. Asimismo, los apartados de procedencia de los datos, finalidad y sistema de tratamiento, que era de obligada cumplimentación, originaron como erróneas todas las notificaciones en las que no venían rellenos. También presentaron dificultad de cumplimentación los datos especialmente protegidos, produciendo un tanto por ciento muy elevado de errores en el apartado de estructura de datos.

Distribución de ficheros activos según la tipología de datos que contienen

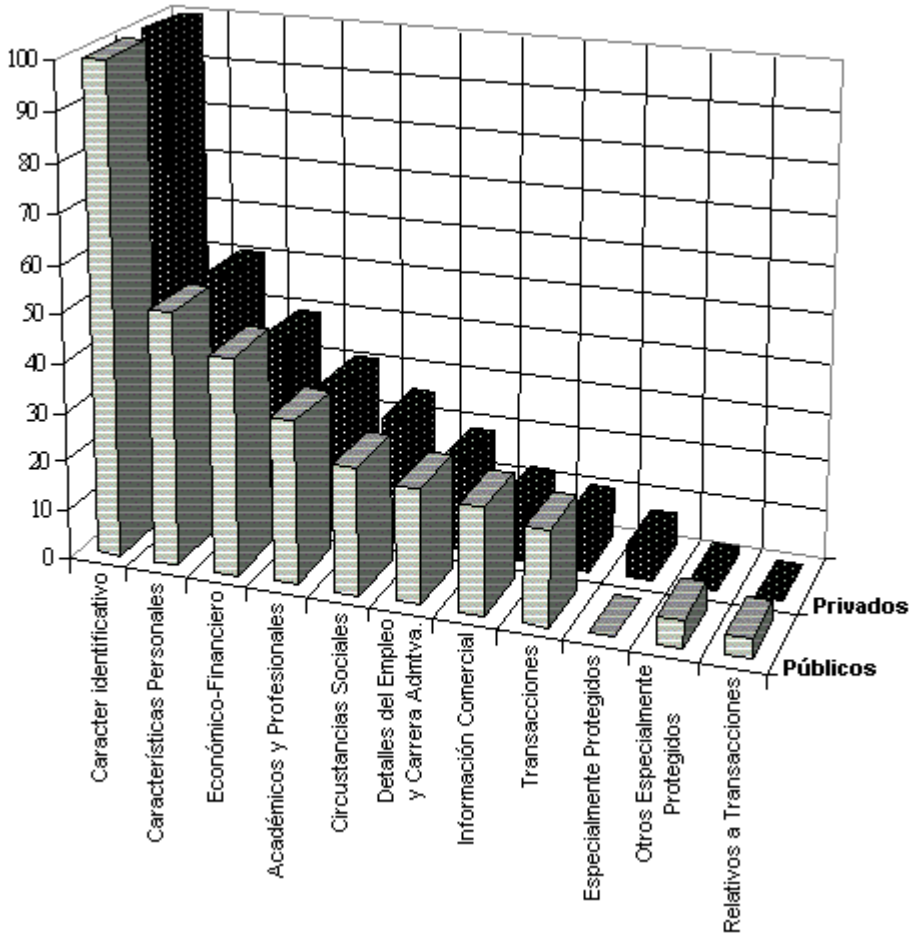
Ficheros de Titularidad Pública

TIPOLOGÍA DE DATOS	FICHEROS	% TOTAL
Datos de carácter identificativo	20.198	100,00
Datos de características personales	10.957	51,70
Datos económico-financieros	9.369	44,20
Datos académicos y profesionales	7.017	33,11
Datos de circunstancias sociales	5.476	25,84
Datos de detalles del empleo y carrera admtva.	4.961	23,41
Datos de información comercial	4.593	21,67
Datos de transacciones	3.992	18,83
Datos especialmente protegidos	2.081	9,81

Ficheros de Titularidad Privada

TIPOLOGÍA DE DATOS	FICHEROS	% TOTAL
Datos de carácter identificativo	192.097	100,00
Datos económico-financieros	97.747	50,88
Datos de características personales	75.489	39,30
Datos de detalles del empleo y carrera admtva.	59.769	31,11
Datos de transacciones	48.610	25,30
Datos de información comercial	36.540	19,02
Datos académicos y profesionales	23.554	12,26
Datos de circunstancias sociales	19.716	10,26
Datos especialmente protegidos	4.546	2,30

Distribución de ficheros ACTIVOS según la TIPOLOGÍA DE DATOS que contienen



Como se puede observar en el gráfico GR16, el cien por cien de los ficheros inscritos contienen datos de carácter identificativo, dada la obligatoriedad de este apartado. A continuación le siguen los datos de características personales, los económico-financieros y los académicos y profesionales. La evolución de la tipología de datos es similar para ficheros públicos y privados.

Distribución de ficheros inscritos por finalidad. Titularidad Pública

La tabla TR15 refleja la distribución de los ficheros de titularidad pública inscritos en el Registro en función de su finalidad y usos previstos. Se indica el número de ficheros asociados a cada uno de los fines indicados, así como su relación respecto del total de ficheros de esta titularidad.

Analizando esta tabla se observa que los fines denominados "PROCEDIMIENTOS ADMINISTRATIVOS", "GESTIÓN DE ESTADÍSTICAS INTERNAS", "GESTIÓN ECONÓMICA CON TERCEROS" y "GESTIÓN DE PERSONAL", claramente asociados a los ficheros propios de la gestión interna de las Administraciones Públicas, como son los Registros de entrada y salida de documentos, contabilidad y personal, ocupan la mayor parte de las inscripciones, con un porcentaje entre el 29,81 % y el 15,14%.

A continuación, se encuentran aquellos ficheros que sirven de base para el ejercicio propio de las funciones de cada uno de los Organismos Públicos que integran la Administración, existiendo una proporcionalidad directa entre la dispersión geográfica y de competencias y el número de ficheros. Así se puede observar que la finalidad de "GESTIÓN TRIBUTARIA Y DE RECAUDACIÓN" está incluida en el 20,71% de los ficheros, le siguen "PADRÓN" con un 14,08%, "ACTUACIONES POLICIALES" con un 8,97%, y "SERVICIO MILITAR" con un 8,18%.

Posteriormente, a medida que las competencias sobre determinadas materias están mas centralizadas, disminuye progresivamente el número de ficheros para su gestión.

FINALIDAD	FICHEROS	%
Procedimientos administrativos	6.020	29,81
Gestión de estadísticas internas	6.019	29,81
Gestión tributaria y de recaudación	4.201	20,80
Gestión económica con terceros	4.182	20,71
Función estadística pública	3.977	19,69
Gestión de personal	3.058	15,14
Padrón	2.843	14,08
Concesión y gestión de permisos y licencias	2.413	11,95
Gestión sancionadora	1.843	9,13
Gestión deuda pública y tesorería	1.811	8,97
Actuaciones policiales	1.760	8,72
Servicio militar	1.652	8,18
Pensiones, subsidios y otras prestaciones económicas	1.521	7,53
Protección civil	1.516	7,51
Seguridad y control interno	1.468	7,27
Actuaciones de fuerzas y cuerpos de seguridad	1.464	7,25
Gestión de catastros inmobiliarios rústicos y urbanos	1.303	6,45
Seguridad vial	1.174	5,81
Formación de personal	1.101	5,45
Prestaciones de asistencia social	1.066	5,28
Relaciones laborales y condiciones de trabajo	937	4,64
Formación profesional	867	4,29
Prestaciones a los desempleados	838	4,15
Ayudas acceso a vivienda	821	4,07
Gestión y control sanitario	809	4,01
Investigaciones científicas o médicas y actividades análogas	785	3,89

FINALIDAD	FICHEROS	%
Otros servicios sociales	738	3,65
Prestación social sustitutoria	723	3,58
Servicios sociales a la tercera edad	713	3,53
Nacionalidad	711	3,52
Otras enseñanzas, becas y ayudas a estudiantes	705	3,49
Procedimientos judiciales	682	3,38
Acción social en favor del personal de las Admones. Públicas	669	3,31
Deportes	657	3,25
Inspección y control de seguridad y protección social	573	2,84
Formación profesional y escuela oficial de idiomas	565	2,80
Educación infantil y primaria	553	2,74
Promoción y gestión de empleo	508	2,52
Educación secundaria	490	2,43
Control de incompatibilidades	488	2,42
Servicios sociales a minusválidos	462	2,29
Promoción servicios a la juventud	431	2,13
Historial clínico	420	2,08
Protección del menor	407	2,02
Publicaciones	404	2,00
Promoción y servicios a la mujer	403	2,00
Relaciones comerciales con el exterior	347	1,72
Gestión y control de centros e instituciones penitenciarias	299	1,48
Acción en favor de migrantes	298	1,48
Enseñanza universitaria	298	1,48
Educación especial	259	1,28
Trabajos penitenciarios	259	1,28
Indultos	253	1,25
Control de patrimonio de altos cargos públicos	173	0,86
Fomento y apoyo a actividades artísticas y culturales	164	0,81
Prestaciones de garantía salarial	140	0,69
Protección a los consumidores	125	0,62
Encuestas sociológicas y de opinión	89	0,44
Protección patrimonio histórico artístico	69	0,34
Regulación de mercados financieros	16	0,08
Defensa de la competencia	14	0,07

Procedencia de los datos y procedimiento de recogida. Titularidad pública

La tabla TR16 indica el número de ficheros asociados a cada una de las modalidades de procedencia de los datos, así

como el porcentaje que representa este número sobre el total de ficheros inscritos.

Es significativo el número de ficheros cuyos datos pueden proceder directamente del PROPIO INTERESADO O SU REPRESENTANTE LEGAL, (94,09 %), también hay que tener en cuenta el elevado porcentaje en que los datos proceden de las propias Administraciones Públicas (40,12%).

La distribución de los procedimientos de recogida de los datos de los ficheros de titularidad pública inscritos en el Registro se refleja en la tabla TR17. Se indica el número de ficheros asociados a cada uno de los posibles procedimientos de recogida de la información empleados, así como el porcentaje que representa este número sobre el total de ficheros inscritos.

Se observa que el procedimiento de recogida mas empleado es el de DECLARACIONES O FORMULARIOS para un 86,37% de los ficheros, lo cual también es lógico pues por ahora continúa siendo el papel la forma más habitual de dirigirse a la Administración.

En la tabla TR18 se puede observar la relación de los diferentes soportes utilizados en la obtención de los datos de los ficheros de titularidad pública. Se indica el número de ficheros asociados a cada uno de los soportes empleados, así como el porcentaje que representa este número sobre el total de ficheros inscritos.

Destaca el porcentaje del 44,40%, de utilización del soporte informático/magnético para obtener los datos en los ficheros de titularidad pública, del que se deduce, el alto grado de informatización de las Administraciones Públicas, más alto aún si se compara con el del sector privado.

PROCEDENCIA	FICHEROS	%
El propio interesado o su representante legal	19.005	94,09
Administraciones públicas	8.104	40,12
Entidad privada	2.352	11,64
Fuentes accesibles al público	2.253	11,15
Otras personas distintas del afectado o su representante	3.236	16,02

PROCEDIMIENTO DE RECOGIDA	FICHEROS	%
Declaraciones o formularios	17.446	86,37
Registros públicos	5.077	25,14
Transmisión electrónica de datos	4.045	20,03
Encuestas o entrevistas	2.952	14,62
Directorios telefónicos, comerciales, catálogos, memorias	1.656	8,20
Otros procedimientos de recogida	1.743	8,63

SOPORTE UTILIZADO PARA LA OBTENCIÓN	FICHEROS	%
Soporte papel	19.232	95,22
Soporte informático/magnético	8.968	44,40
Vía telemática	2.850	14,11
Otros soportes (oral, telefónica)	2.875	14,23

Cesiones.

La cesión de datos entre ficheros de titularidad pública es bastante frecuente como puede observarse en la tabla TR19, alcanzando a un 60,64% de los ficheros inscritos. Esta cifra llama más la atención si se compara con las cesiones que se realizan en el sector privado.

Cesiones de datos. Ficheros inscritos en el Registro

TITULARIDAD	CON CESIONES	INSCRITOS	%
Pública	12.249	20.198	60,64
Privada	36.797	192.097	19,15
TOTAL	**49.046**	**212.295**	**23,10**

Cesiones de datos. Titularidad Pública

Este fenómeno encuentra su explicación en la propia naturaleza de la Administración, que con el fin de agilizar su funcionamiento y facilitar la comunicación al ciudadano pone a su disposición la ventanilla única.

En la tabla TR20 se refleja la distribución de las cesiones antes mencionadas en relación con los supuestos legales que establece la propia Ley Orgánica. Esta es bastante uniforme, alcanzando la cota más alta al tratarse de competencias idénticas ejercidas por otras administraciones, o bien ser datos obtenidos o elaborados con destino a otra Administración Pública.

SUPUESTOS LEGALES EN VIRTUD DE LOS CUALES SE REALIZA LA CESIÓN	FICHEROS
Existe consentimiento de los afectados	5.065
Existe una norma reguladora que las autoriza	5.618
Existe una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros	2.719
Corresponden a competencias idénticas o que versan sobre las mismas materias, ejercidas por otras Administraciones Públicas	7.607
Son datos obtenidos o elaborados con destino a otra Administración Pública	7.107
Se trata de datos recogidos de fuentes accesibles al público	3.947

Transferencias internacionales.

Los ficheros sobre los que se realizan transferencias internacionales de datos no alcanzan el 1% de los inscritos, como se refleja en la tabla TR21, siendo mucho menor si analizamos el porcentaje de los de titularidad pública.

TITULARIDAD	FICHEROS	INSCRITOS	%
Pública	29	20.198	0,19
Privada	1.198	192.097	0,62
TOTAL	**1.237**	**212.295**	**0,58**

Transferencias internacionales. Titularidad Pública

La tabla siguiente muestra la distribución de las transferencias internacionales de datos que han sido inscritas en el Registro.

Prácticamente la totalidad de los ficheros con transferencias internacionales de datos pertenecen a organismos encuadrados en la Administración General del Estado, pudiéndose observar que la mayor parte de éstas se efectúan a

las autoridades competentes de países que cuentan con un nivel de protección equiparable al determinado por la Ley Orgánica (84,62%). Además, en un 76,92% de los casos, están amparadas en Convenios o Tratados de los que España forma parte.

Las transferencias dinerarias, que representan el 35,90%, corresponden al Banco de España, por sus operaciones con el exterior, y a los organismos que reciben o gestionan ayudas y subvenciones del presupuesto comunitario. Este es el caso del Ministerio de Hacienda, respecto de los fondos FEDER y el de Ministerio de Agricultura, respecto de los fondos FEOGA.

Para prestar auxilio judicial internacional y en aplicación de los acuerdos, tratados y convenios (Maastricht, Interpol, Schengen y Viena), la Dirección General de la Policía y Guardia Civil transfieren datos a los autoridades competentes de la Unión Europea.

SUPUESTOS EN VIRTUD DEL CUAL SE REALIZA	FICHEROS	%
Se efectúa con destino a algún país de los citados en el reglamento con nivel de protección equiparable al que presta la presente Ley	33	84,62
Se ampara en tratado o convenio del que España forma parte	30	76,92
Se refiere a transferencias dinerarias	14	35,90
Se realiza a efectos de prestar auxilio judicial internacional	8	20,51
Tiene por objeto intercambiar datos de carácter médico y así lo exige el tratamiento del afectado o la investigación epidemiológica	4	10,26
TOTAL DE FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES	**39**	

* Un mismo fichero puede realizar transferencias acogiéndose a más de un supuesto legal.

Distribución de ficheros inscritos por finalidad. Titularidad privada

Como se puede observar en la tabla TR23, las dos terceras partes de los ficheros contemplan como fin la gestión contable, fiscal y administrativa. Ello es debido a la práctica generalizada de mecanizar la gestión contable, automatizando así, no solo la propia contabilidad y gestión, sino también el cumplimiento de las obligaciones tributarias.

Por otra parte, cerca de la mitad de los ficheros tiene como finalidad la gestión de cobros y pagos. Ello se justifica, ante todo, por la existencia de ficheros automatizados de nóminas en la mayoría de las entidades. A su vez, también son muy comunes en las empresas los ficheros de clientes y proveedores, lo que concuerda con el hecho de que prácticamente un tercio de los ficheros inscritos contemplen como finalidad la gestión de clientes y que un 15% incluya el mantenimiento de históricos de relaciones comerciales.

Otro tipo de ficheros muy comunes son los relativos a personal, incluyendo su selección. La cuarta parte de los ficheros inscritos presentan como finalidad la gestión de personal, correspondiendo casi un 2% a la selección del mismo.

Lo mismo ocurre con la obtención de estadísticas diversas, más de la cuarta parte de la inscripción refleja esta finalidad, que evidentemente puede estar presente en muy variados tipos de ficheros.

Las entidades financieras tienen también una presencia acusada a través de finalidades como la gestión de seguros y planes de pensiones, las cuentas de crédito, las cuentas de depósito y la gestión de tarjetas de crédito y similares, lo que representa el 4% de los ficheros inscritos. Los servicios financieros de todo tipo, la información sobre la solvencia patrimonial y el crédito, la gestión de patrimonios y el registro de acciones y obligaciones, cuentan con una presencia importante, que llega a sobrepasar la cifra del 4% de la inscripción.

Ocupan también un lugar destacado las finalidades de prospección de mercado y publicidad, tanto propia como para terceros, así como las encuestas de opinión. Cerca del 15% de los ficheros inscritos contemplan este tipo de finalidades.

La fuerte actividad del sector del seguro está presente en varias rúbricas del cuadro de finalidades, como seguros de vida y salud y otro tipo de seguros, que engloban un 10% de la inscripción.

También se detecta el aumento de actividades empresariales de seguridad y control interno, lo que se refleja en una

inscripción superior al 6% con esta finalidad. La misma cifra se presenta para ficheros con finalidades de auditoría y asesoría.

Por el contrario se ha detectado un bajo nivel de inscripción en sectores como educación, investigación y medicina privada así como en las agencias de viajes y los medios de comunicación social.

FINALIDAD	FICHEROS	%
Gestión contable, fiscal y administrativa	128.363	66,82
Gestión de cobros y pagos	83.862	43,66
Gestión de clientes	60.920	31,71
Obtención de estadísticas diversas	51.054	26,58
Gestión de personal	49.453	25,74
Históricos de relaciones comerciales	30.524	15,89
Publicidad propia	17.446	9,08
Prestaciones sociales	12.704	6,61
Auditorías, asesorías y servicios relacionados	12.679	6,60
Seguridad y control interno	9.267	4,82
Prospecciones de mercado	6.055	3,15
Otro tipo de seguros	5.225	2,72
Seguros de vida y salud	5.070	2,64
Cuenta de crédito	3.827	1,99
Otros servicios financieros	3.450	1,80
Selección de personal	3.308	1,72
Información sobre la solvencia patrimonial y crédito	2.778	1,45
Encuestas de opinión	2.434	1,27
Publicidad para terceros	2.269	1,18
Gestión de fondos de pensiones y similares	2.058	1,07
Cuenta de depósito	1.954	1,02
Gestión administrativa de los integrantes de los clubes	1.794	0,93
Gestión de patrimonios	1.739	0,91
Registro de acciones y obligaciones	1.737	0,90
Historial clínico	1.676	0,87
Gestión y control sanitario	1.484	0,77
Formación profesional	1.345	0,70
Otras enseñanzas	1.345	0,70
Gestión de tarjetas de crédito y similares	1.149	0,60
Servicios de telecomunicación	1.013	0,53
Investigaciones científicas y médicas	611	0,32
Educación universitaria	610	0,32
Seguridad	586	0,31
Educación secundaria	481	0,25
Educación infantil primaria	421	0,22
Investigación	408	0,21
Medios de comunicación social	408	0,21
Reserva y emisiones de billetes	282	0,15
Educación especial	265	0,14
Investigaciones privadas a personas	83	0,04

Procedencia de los datos y procedimiento de recogida. Titularidad Privada

Como se puede observar en la tabla TR24, y dado que la mayoría de la inscripción privada corresponde a ficheros de contabilidad, gestión, nóminas, clientes y proveedores, es lógico que más del 80% de los ficheros declaren como procedencia de los datos el propio interesado o su representante legal. Asimismo, el procedimiento de recogida de la información para este tipo de ficheros, suele ser mediante declaraciones, formularios, encuestas y entrevistas, utilizando como soporte el papel, que dan precisamente los porcentajes más altos en las correspondientes tablas de procedimiento de recogida. (TR25 Y TR26).

También se observa un porcentaje significativo de ficheros cuyos datos proceden de entidades privadas. Normalmente este tipo de ficheros suelen provenir de cesiones de otras empresas. Si se observa la tabla de cesiones (TR19), el porcentaje de ficheros cedidos es algo superior al de ficheros cuyos datos proceden de una entidad privada. La diferencia corresponde a las cesiones de datos hechas por las empresas privadas a destinatarios de titularidad pública.

Por otra parte, prácticamente un 4% de los ficheros inscritos declaran la procedencia de los datos de fuentes accesibles al público. Ello concuerda con la cifra de inscripción cuyo procedimiento de recogida son los directorios telefónicos y comerciales, catálogos y memorias.

Aproximadamente un 1,5% de la inscripción declara su procedencia de las Administraciones Públicas, que generalmente corresponde a la información obtenida de registros públicos y de domiciliaciones de cobros y pagos (nóminas, recibos..) de los organismos públicos al sector Bancario. La tabla de procedimiento de recogida presenta este tipo de inscripción en el apartado de registros públicos. El soporte puede ser variado, con predominio del papel. El uso del soporte informático es sensiblemente inferior que en el sector público.

El apartado "otras personas distintas del afectado" de la tabla de procedencia de los datos, basa su contenido, sobre todo, en los métodos indirectos de recogida de la información, como pueden ser los cuestionarios múltiples, las entrevistas con preguntas encadenadas, los cupones con información cruzada, etc. El procedimiento de recogida para este tipo de información suele ser las declaraciones o formularios y las encuestas o entrevistas en soporte papel.

PROCEDENCIA	FICHEROS	%
El propio interesado o su representante legal	172.620	89,86
Entidad privada	24.575	12,79
Fuentes accesibles al público	8.258	4,30
Administraciones Públicas	3.032	1,58
Otras personas distintas del afectado o su representante	3.776	1,97

PROCEDIMIENTO DE RECOGIDA	FICHEROS	%
Declaraciones o formularios	79.681	41,48
Encuestas o entrevistas	41.873	21,80
Directorios telefónicos, comerciales, catálogos, memorias	8.586	4,47
Registros públicos	3.370	1,75
Transmisión electrónica de datos	2.868	1,49
Otros procedimientos de recogida (facturas, el propio interesado)	66.214	34,47

TIPOLOGÍA DE DATOS	FICHEROS	% TOTAL
Soporte papel	154.788	80,58
Soporte informático/magnético	26.686	13,89
Vía telemática	4.339	2,26
Otros soportes (facturas, oral, telefónica)	32.816	17,08

Cesiones de Datos. Titularidad Privada

Dentro de los supuestos legales en virtud de los cuales se realizan las cesiones de datos de ficheros automatizados de carácter personal, el más común es la existencia de una norma reguladora que las autoriza. Ello está en consonancia con el hecho que las finalidades más corrientes en la declaración de ficheros sean la gestión contable, fiscal y administrativa y la gestión de cobros y pagos, referidas sobre todo a ficheros de contabilidad, gestión y nóminas, que suelen ser cedidos a la Agencia Tributaria y a la Tesorería General de la Seguridad Social.

El consentimiento de los afectados para la cesión de los datos es el supuesto legal que ocupa el segundo lugar en la inscripción, lo cual también es lógico dado que la mayoría de las cesiones no amparadas en norma no pueden justificarse de otra forma. Los ficheros con finalidades como gestión de personal, gestión de clientes, históricos de relaciones comerciales, publicidad, prospecciones de mercado, estadísticas diversas y encuestas de opinión, que representan un fuerte porcentaje de la inscripción total, suelen justificar sus cesiones con el consentimiento de los afectados.

También es muy común el supuesto legal para la cesión, de la existencia de una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros. Este hecho está justificado con la existencia de ficheros referentes a la domiciliación de recibos, transferencias bancarias, pagos de nóminas, gestión de tarjetas de crédito, compra de acciones, correduría de seguros y todo tipo de relaciones de intermediación.

También se contempla, en menor medida, la recogida de los datos de fuentes accesibles al público, hecho que está directamente relacionado con la inscripción de ficheros cuya procedencia de datos son las fuentes públicas.

SUPUESTOS LEGALES EN VIRTUD DE LOS CUALES REALIZA LA CESIÓN	FICHEROS
Existe consentimiento de los afectados	15.859
Existe una norma reguladora que las autoriza	18.190
Existe una relación jurídica cuyo desarrollo, control y cumplimiento implica necesariamente la conexión del fichero con ficheros de terceros	11.881
Se trata de datos recogidos de fuentes accesibles al público	2.015

Ficheros sobre los que se reconocen transferencias internacionales. Titularidad Privada

SUPUESTO EN VIRTUD DEL CUAL SE REALIZA	FICHEROS	%
Se efectúa con destino a algún país de los citados en el reglamento con nivel de protección equiparable al que presta la presente Ley	968	72,55
Se refiere a tranferencias dinerarias	293	25,75
Tiene por objeto intercambiar datos de carácter médico y así lo exige el tratamiento del afectado o la investigación epidemiológica	18	1,70
TOTAL DE FICHEROS INSCRITOS CON TRANSFERENCIAS INTERNACIONALES	**1.198**	

* Un mismo fichero puede realizar transferencias, acogiéndose a más de un supuesto legal.

Sistemas de tratamiento. Titularidad privada

Tipo de sistema de tratamiento en que residen los ficheros de titularidad privada inscritos en 1994. Los porcentajes se calculan respecto al número total de ficheros privados inscritos.

TIPO DE SISTEMA	FICHEROS	%
Ordenador personal	98.949	51,51
Ordenador personal en red	36.535	19,02
Eqipos medios (minis,..)	46.858	24,39
Grandes eqipos (Mainframes...)	9.755	5,08
TOTAL FICHEROS INSCRITOS	**192.097**	**100**

Número de ficheros inscritos de titularidad privada para los que se reconocen conexiones remotas: 21.930 (11,42%).

4. LA INSPECCIÓN DE DATOS

La efectiva protección de los derechos reconocidos a los ciudadanos por la Ley Orgánica en relación con sus datos personales, así como la garantía de los principios que en materia de tratamiento automatizado de datos personales establece la Ley, exigían dotar a la Agencia de Protección de Datos de competencias que le permitieran inspeccionar los sistemas e instalaciones utilizados para dichos tratamientos y sancionar las posibles infracciones cometidas.

Así lo hace la Ley, atribuyendo potestades de inspección a la Agencia de Protección de Datos (artículo 39) y estableciendo en su Título VII un sistema de infracciones y sanciones (artículos 42 a 48). Por su parte, el Estatuto de la Agencia establece la Inspección de Datos como órgano de la misma y desarrolla sus funciones en los artículos 27 a 29.

Sin embargo, es con la aprobación del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica, y en particular la tutela de los derechos reconocidos por la misma y el procedimiento sancionador, cuando queda completado el mecanismo de garantía que para dichos derechos constituye la inspección de datos.

La aplicación de una Ley tan ambiciosa en materia de protección de datos, y tan estricta en la represión de sus infracciones, en la sociedad y el momento histórico en que se produce, en los que la informatización de procesos de todo tipo se ha desarrollado considerablemente en ausencia de cauces que previamente regularan de algún modo el procesamiento indiscriminado de datos personales, ha de ser conducida con especial prudencia.

Este principio de prudencia aconsejaba dar prioridad en el tiempo a las acciones informativas frente a las específicamente sancionadoras. En este sentido, la actuación de la Agencia se ha dirigido preferentemente tanto a informar a los responsables de ficheros de datos personales de las obligaciones que para ellos se desprenden de la Ley Orgánica, como a conocer la situación de partida que en materia de tratamiento de datos personales presentaba la sociedad española en el momento de su entrada en vigor.

Esta actitud no ha significado, evidentemente, renuncia o dejación de las responsabilidades y competencias que tanto en materia de tutela de derechos como de sanción de infracciones tiene atribuidas la Agencia. Pero sí ha supuesto que, en relación con la potestad sancionadora, la Agencia de Protección de Datos haya actuado durante 1994 únicamente a partir de las denuncias presentadas, dando de este modo una mayor oportunidad o plazo a los responsables de ficheros de datos personales para ajustar su actuación a los principios y reglas establecidos por la Ley Orgánica en tanto en cuanto no hubiera reclamación o denuncia de posibles perjudicados por su funcionamiento.

Dos circunstancias adicionales han limitado la actuación inspectora de la Agencia durante 1994. En primer lugar, un hito fundamental del sistema de garantías establecido por la Ley Orgánica lo constituye la notificación e inscripción inicial de ficheros en el Registro General de Protección de Datos. Este proceso fundamental no sólo constituye una obligación impuesta por la Ley a los responsables de ficheros, sino el punto de partida para el ejercicio de los principales derechos que ésta reconoce a los ciudadanos en relación con sus datos personales: información, acceso, rectificación y cancelación. La tardía aprobación del Reglamento que desarrollaba el proceso de inscripción de ficheros, unido a la fecha que marcaba el final del plazo legal para la inscripción de los existentes con anterioridad a la Ley y al breve plazo disponible tanto para los obligados como para la propia Agencia, ha retrasado el momento en que los

ciudadanos han dispuesto de información adecuada sobre dónde ejercer sus derechos con carácter previo a la interposición de una eventual reclamación o denuncia.

En segundo lugar, una de las áreas de trabajo de mayor repercusión en la futura actividad de inspección de la Agencia de Protección de Datos es, sin duda alguna, la de las medidas de seguridad que garantizan la adecuada protección de la confidencialidad e integridad de los datos personales tratados o almacenados por medios automatizados. La Ley Orgánica eleva la seguridad a la categoría de principio de protección de datos, pero remite a desarrollo reglamentario el establecimiento de requisitos y condiciones específicos, con lo que la actuación de la inspección no cuenta en esta materia sino con los criterios generales establecidos en el artículo 9.1 de la Ley.

RECLAMACIONES Y DENUNCIAS

Aún cuando los primeros escritos conteniendo reclamaciones o denuncias en materia de protección de datos se remontan a finales del año 1993, puede afirmarse que la Subdirección General de Inspección de Datos comienza a tener una actividad significativa en materia de tutela de derechos e instrucción de expedientes sancionadores una vez transcurrido el plazo de inscripción inicial de ficheros en el Registro General de Protección de Datos.

Esta situación se explica fácilmente si se considera que, dada la novedad de la Ley y el escaso impacto que su entrada en vigor tuvo en la opinión pública española, la campaña desarrollada por la Agencia con ocasión del proceso de inscripción inicial de ficheros fue sin duda alguna la primera actividad de difusión a gran escala de los principios, derechos y obligaciones establecidos por la Ley en materia de protección de datos.

Sin embargo, las características de las actuaciones de difusión realizadas por la Agencia en este período, orientadas principalmente hacia los responsables de los ficheros, han constituido un factor limitativo del impacto informativo sobre los ciudadanos en general y ello se ha traducido en un nivel relativamente bajo de conocimiento de los derechos y posibilidades de ejercicio de los mismos que la Ley y la Agencia les ofrecía. Por consiguiente, el número de reclamaciones y denuncias presentadas por los ciudadanos en este primer ejercicio ha sido muy reducido, registrándose la entrada de únicamente 81 escritos de esta naturaleza.

A pesar de su reducido número y a pesar del riesgo de que no constituyan una muestra muy representativa de las preocupaciones e inquietudes de los ciudadanos españoles en materia de protección de datos, de su análisis parecen emerger algunas pautas que podrían arrojar luz acerca de nuestras prioridades colectivas respecto de la intimidad o privacidad. El hecho de que dichas pautas no parecen muy diferentes de las detectadas en otros países de nuestro entorno socioeconómico y cultural, con estadísticas y series temporales de comportamiento más representativas y consolidadas, contribuye a dar verosimilitud a las tendencias que las reclamaciones y denuncias de este primer año de actividad de la Agencia apuntan.

De la clasificación de las mismas, reflejada en la tabla adjunta, destaca con toda claridad un primer tipo de datos personales que, aunque no calificado de especialmente sensible por la Ley, parece concentrar las preocupaciones de nuestra sociedad: los datos de naturaleza económico-financiera y, entre ellos, especialmente, los relativos a la solvencia, el crédito y la morosidad.

RECLAMACIONES Y DENUNCIAS RECIBIDAS
CLASIFICADAS POR TIPO DE ENTIDAD DENUNCIADA

RECLAMACIONES Y DENUNCIAS RECIBIDAS
CLASIFICADAS POR TIPO DE ENTIDAD DENUNCIADA

	NUMERO	PORCENTAJE*
Información sobre solvencia patrimonial, crédito y morosidad	45	56%
Entidades financieras	11	14%
Administraciones Públicas (sin incluir fuerzas de seguridad)	5	6%
Fuerzas y Cuerpos de seguridad	3	4%
Compañias de seguros	3	4%
Empresas de publicidad y marketing	2	2%
Otros sectores	12	15%
TOTAL:	81	100%

(*) La suma aparente no corresponde al 100% debido al redondeo

(*) La suma aparente no corresponde al 100% debido al redondeo

Casi tan notorias como las presencias son, de otra parte, las ausencias. Así, es de señalar que, pese a la consideración de los datos relacionados con la salud como *especialmente protegidos* por la Ley, las organizaciones directamente relacionadas con ellos no parecen haber sido objeto de público escrutinio en relación con los datos personales que manejan. También parece sorprendente la escasa preocupación manifestada por los ciudadanos hacia los datos personales procesados por las fuerzas y cuerpos de seguridad de los distintos ámbitos administrativos con competencias en la materia (dada su potencial incidencia sobre la intimidad) así como hacia los relacionados con actividades de publicidad y marketing (particularmente intensivas en el tratamiento masivo de datos personales).

Sin embargo, parece prematuro extraer en estos últimos casos conclusiones claras acerca de las prioritarias preocupaciones de los españoles sobre la incidencia de la informática en su intimidad, dado el tamaño de la muestra disponible.

En cuanto a la procedencia geográfica de las denuncias, destaca la provincia de Madrid, seguida a considerable distancia de la de Barcelona y mostrando gran dispersión geográfica el resto de las denuncias recibidas. Los factores población y disponibilidad de información parecen explicar fácilmente esta distribución geográfica.

ACTUACIONES DE LA INSPECCION DE DATOS

La potestad de inspección de la Agencia de Protección de Datos, instituida por el artículo 39 de la Ley Orgánica, viene atribuida por el Estatuto de la Agencia a la Inspección de Datos, a la que en sus artículos 27 a 29 asigna las competencias necesarias para su ejercicio, clasificándolas en dos tipos de funciones: funciones inspectoras y funciones instructoras.

Las primeras, enumeradas en el artículo 28 del Estatuto, abarcan las actuaciones de examen, análisis y prueba de sistemas, ficheros, documentos, dispositivos y, en general, de todos aquellos elementos relacionados con los posibles tratamientos automatizados de datos personales objeto de investigación.

Las segundas, relacionadas con el ejercicio de la potestad sancionadora, incluyen la tramitación de los expedientes administrativos iniciados como consecuencia de reclamaciones o denuncias recibidas en la Agencia y relacionadas con la protección de datos personales.

Este segundo grupo de actuaciones está estructurado en la normativa vigente en torno a tres procedimientos diferenciados, según se trate de tutelar los derechos reconocidos por la Ley Orgánica, instruir y resolver expedientes sancionadores o tramitar expedientes derivados de infracciones cometidas en ficheros cuyo responsable es una Administración Pública.

En el primer caso, el procedimiento está regulado por el artículo 17 Reglamento; en el segundo, por los artículos 18 y 19 del mismo; en el último caso, por el artículo 45 de la propia Ley.

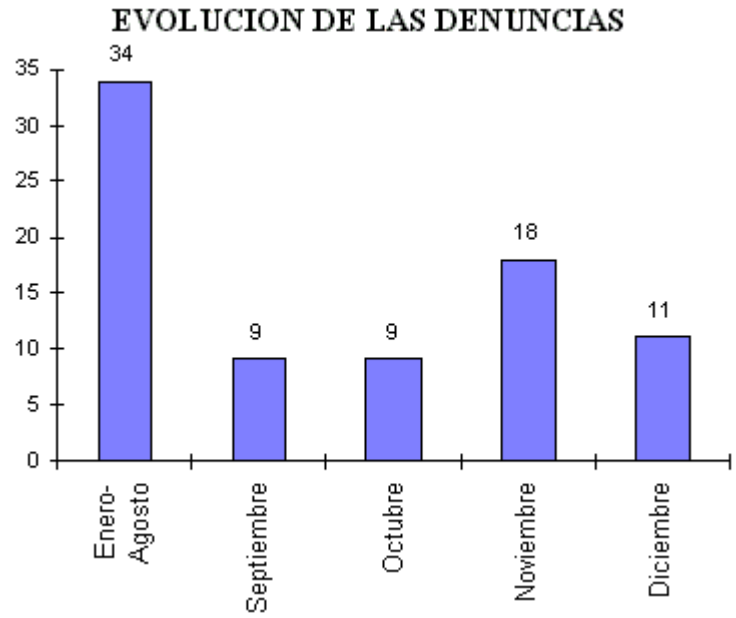
La práctica ha puesto de manifiesto que los escritos recibidos en la Agencia requieren frecuentemente un proceso previo de análisis de contenido y obtención de información adicional, antes de ser encaminados hacia uno de los procedimientos sustantivos. En ocasiones, estas actuaciones previas permiten determinar la no procedencia de iniciar procedimiento alguno, por faltar alguno de los supuestos que determinan la competencia de la Agencia para iniciar

actuaciones o bien por no haberse cumplido algún requisito previo.

Durante el ejercicio, la circunstancia más frecuente que ha motivado la no iniciación de procedimiento alguno como consecuencia de una reclamación o denuncia ha sido la de tratarse de datos relativos a personas jurídicas, expresamente excluidos del ámbito de aplicación de la Ley.

De los procedimientos iniciados durante 1994, cuatro han correspondido a la tramitación de expedientes sancionadores, nueve a procedimientos de tutela de derechos y dos a procedimientos por infracciones relativas a ficheros de alguna Administración Pública. Adicionalmente, al cierre del ejercicio, 12 expedientes se encontraban en situación de actuaciones previas y 10 pendientes de actuación por diversas causas, habiendo sido archivado el resto de las actuaciones seguidas como consecuencia de los escritos recibidos.

En cuanto a las actuaciones de inspección, éstas no comenzaron hasta el mes de noviembre, por las razones antes apuntadas. Pese a ello, en 1994 se realizaron ocho inspecciones, de las que cuatro correspondieron a actuaciones relacionadas con ficheros del sector de publicidad y marketing, tres al sector de solvencia, crédito y morosidad y una al comercio minorista. Es de señalar que, en base al criterio anteriormente expuesto, todas las inspecciones efectuadas se derivaron de la presentación de reclamaciones o denuncias de ciudadanos que recabaron la tutela de sus derechos ante la Agencia de Protección de Datos.



LA SEGURIDAD EN EL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES

Entre los principios de protección de datos establecidos por la Ley Orgánica en su capítulo primero, figura de modo

destacado el principio de seguridad. Además de las implicaciones que en materia de seguridad de los sistemas de información se derivan de otros principios establecidos por la Ley -y especialmente de los principios de calidad de datos y de deber de secreto de responsables e intervinientes en el tratamiento de datos personales- la Ley dedica su artículo 9 a establecer y delimitar el principio de seguridad de los datos.

En su primer apartado, el citado artículo de la Ley delimita de un modo extraordinariamente amplio el concepto de seguridad en relación con la protección de los datos personales y establece unos criterios generales de interpretación para su aplicación en la evaluación de situaciones concretas. Sin embargo, en sus apartados 2 y 3, el artículo 9 condiciona el establecimiento de los requisitos y condiciones que deban reunir los ficheros automatizados de datos personales y las personas que intervengan en su tratamiento al futuro desarrollo reglamentario.

Finalizado el año 1994, todavía no se ha producido el desarrollo reglamentario previsto por la Ley en esta materia, y no es aventurado anticipar que todavía puede demorarse un tiempo considerable, dada la extraordinaria dificultad de regular una materia en evolución tecnológica tan rápida y de presencia tan ubicua y multiforme en la sociedad actual como las tecnologías de tratamiento de la información. Por lo tanto, se hace necesario analizar el contenido y aplicabilidad de los elementos recogidos en el artículo 9.1, desde una interpretación sistemática de la Ley, y relacionarlo tanto con la doctrina y práctica profesional en la materia como con la realidad social y técnica sobre la que deben operar, para poder construir un marco operativo, aún provisional, que guíe la actuación de la Agencia en materia de seguridad de los sistemas de tratamiento automatizado de datos personales.

Un punto de partida natural en este proceso de interpretar el alcance de las previsiones contenidas en la Ley en materia de seguridad de datos personales es poner en relación los *objetivos de seguridad* enunciados por el artículo 9.1 con los generalmente aceptados por la doctrina académica y práctica profesional en el ámbito de la seguridad de sistemas de información. En este sentido, puede establecerse un paralelismo muy estrecho entre unos y otros. Así, el citado precepto establece como objetivos de seguridad evitar la *alteración, pérdida, tratamiento o acceso no autorizado*. Es fácil establecer una correspondencia directa con los tres objetivos clásicos de la seguridad de los sistemas de información: *integridad* , *disponibilidad* y *confidencialidad* .

En efecto, tomando como referencia las definiciones aportadas por el documento *Líneas Directrices de la OCDE para la Seguridad de los Sistemas de Información* (Recomendación del Consejo de la OCDE, de 26 de noviembre de 1992), se entiende por *integridad* de los datos o informaciones el hecho de ser exactos y completos, y la preservación de este carácter; por *disponibilidad*, el hecho de ser accesibles y utilizables en el tiempo deseado y del modo requerido; y por *confidencialidad*, el estar únicamente al alcance del conocimiento de las personas o entidades autorizadas, en los momentos autorizados y de una manera autorizada. Y, de acuerdo con las citadas *Directrices*, la seguridad de los sistemas de información tiene por objetivo la protección frente a los perjuicios imputables a defectos de disponibilidad, de confidencialidad y de integridad. Por consiguiente, el alcance y contenido de los objetivos de seguridad enunciados en el artículo 9.1 de la Ley Orgánica puede ser interpretado, en principio, como equivalente al alcance y contenido de los conceptos confidencialidad, integridad y disponibilidad: la integridad evita la alteración indebida de los datos personales, la disponibilidad previene de su pérdida y la confidencialidad impide su tratamiento o acceso no autorizados.

Sin embargo, una interpretación del principio de seguridad tan amplia como la que se desprende de este primer análisis podría conducir a incluir en el ámbito de protección de la Ley Orgánica riesgos que difícilmente pueden ser considerados como amenazas al honor o a la intimidad de los ciudadanos. En particular, la inclusión de la disponibilidad dentro del ámbito de objetivos de seguridad de los datos personales amparados por ella obligaría a contemplar riesgos tales como la destrucción accidental de ficheros o las interrupciones de servicio de los sistemas informáticos, que no pueden concebiblemente poner en peligro los derechos al honor y a la intimidad que constituyen la razón última de la Ley. Por el contrario, la alteración o pérdida parcial de los datos relativos a una persona pueden, en ciertas circunstancias, conducir a la desfiguración del perfil informativo del individuo, afectando negativamente su reputación o fama y perjudicándole en sus relaciones con los demás.

En consecuencia, si bien los objetivos enunciados por el artículo 9.1 de la Ley Orgánica pueden ser interpretados como sinónimos de los tres principios clásicos de confidencialidad, integridad y disponibilidad, parece claro que su aplicación debe ser contemplada en función de los riesgos concretos que cada situación presenta para el honor e intimidad de las personas cuyos datos están siendo tratados.

Con objeto de garantizar la consecución de los objetivos de seguridad enunciados, la Ley Orgánica impone al responsable del fichero la obligación de adoptar medidas de seguridad. Por una parte, el artículo 9.1 establece esta obligación en términos generales: *las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal*. Por otra parte, el art. 9.2 prohibe el almacenamiento de datos personales en ficheros que no reúnan las condiciones que reglamentariamente se determinen. Adicionalmente, el artículo 43.3 h) tipifica como infracción grave el mantener los ficheros, locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. Estos preceptos legales plantean importantes cuestiones a la hora de su aplicación.

En primer lugar, la referencia a medidas técnicas y organizativas viene a consagrar legalmente un principio de gran importancia práctica, como es el carácter multidisciplinar de la seguridad de los sistemas de información. Este principio, recogido en multitud de recomendaciones, estándares y guías de actuación, está también incluido en el citado documento de Directrices de Seguridad de la OCDE, así como en los recientes trabajos de normalización internacional

sobre criterios de seguridad (GSSP, Common Criteria), y supone el reconocimiento de que la seguridad no puede ser lograda y mantenida por la simple instalación de dispositivos físicos o lógicos, sino que requiere la consideración de múltiples puntos de vista y la acción concertada de medidas de variada naturaleza, entre las que las relacionadas con los factores humanos no son menos importantes que las tecnológicas.

En segundo lugar, la remisión a un futuro desarrollo reglamentario plantea la cuestión de la exigibilidad de medidas de seguridad hasta tanto no sean aprobados los reglamentos que las determinen. Con vistas a la actuación de la Agencia en este su primer año de andadura, dos consideraciones contrapuestas han sido tenidas en cuenta. De un lado, la supeditación de toda exigencia de medidas de seguridad a la aprobación de sus reglamentos de desarrollo podría dejar, por tiempo indefinido, vacío de contenido el principio de seguridad de los datos personales establecido en la Ley y, perdido el soporte de la seguridad, venirse abajo el sistema de garantías de la privacidad diseñado por ésta. De otro, un sistema de seguridad de datos personales no puede ser improvisado y, en consecuencia, la autoridad de control (la Agencia) ha de tener en cuenta la situación general que en materia de seguridad de los sistemas de información predomina en España en el momento de entrar en vigor la Ley, y hacer posible una transición ordenada hacia una nueva situación más acorde con los principios y garantías establecidos por ella.

En tercer lugar, el propio artículo 9.1 establece criterios para determinar cuáles son las medidas a adoptar para garantizar la seguridad de los datos personales requerida por la Ley. Estos criterios, basados en el principio general de proporcionalidad, son de tres órdenes distintos: el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que dichos datos se encuentran expuestos.

El estado de la tecnología delimita y afecta a las medidas de seguridad que deben ser adoptadas de múltiples formas. Por una parte, la tecnología determina el ámbito de lo factible en un lugar y momento dados, tanto desde el punto de vista de las amenazas a la seguridad como desde el de las contramedidas que pueden ser adoptadas. En este sentido, puede decirse que la tecnología establece y acota el terreno de juego en que se libra la batalla de la seguridad y su continua evolución introduce nuevas fuentes de riesgo que deben ser previstas, evaluadas y controladas, pero también nuevas posibilidades de protección que deben ser tenidas en cuenta en el diseño de medidas de seguridad. En el año 1994 hemos asistido al surgimiento o expansión de fenómenos tecnológicos que afectaban a uno y otro lado de la balanza de la seguridad: la rápida difusión mundial en el uso comercial o general de la red Internet (por contraposición a su utilización hasta hace poco reducida a ámbitos de investigación o docencia) es un buen ejemplo de cómo la tecnología (o su difusión en la sociedad) puede afectar al equilibrio de la balanza por el lado del riesgo; por otro lado, el surgimiento y evolución de tecnologías para la privacidad, tales como dispositivos físicos o lógicos que facilitan el anonimato en determinadas transacciones electrónicas (algunos tan accesibles y difundidos como el programa Pretty Good Privacy), constituye una muestra de cómo la tecnología también incide en dicho equilibrio por el lado de la protección.

Pero la tecnología es un criterio relevante no sólo porque acota el ámbito de lo factible, sino también porque influye en su coste y su consideración nos conduce al segundo de los criterios establecidos por la Ley: la naturaleza de los datos almacenados. Las medidas de seguridad tienen costes, tanto explícitos (como el tiempo y dinero invertidos en ellas) como implícitos (como pueden ser la agilidad, eficacia o cualesquiera otros objetivos de la organización que han de ser en alguna medida sacrificados para lograr un nivel dado de seguridad). El principio de proporcionalidad aconseja fijar como objetivo un nivel de seguridad eficiente, esto es, un nivel tal que el coste de las medidas de seguridad sea proporcionado al coste de la "no seguridad", es decir, a los perjuicios de todo tipo que se deriven del riesgo a que están expuestos los datos almacenados. Sobre este equilibrio deseable entre los "costes de la seguridad" y los "costes de la no seguridad" influyen múltiples factores, pero tres de ellos lo hacen de forma decisiva.

El primero, ya considerado, es la tecnología. Las tecnologías de la información no sólo han evolucionado espectacularmente en los últimos años en términos de funcionalidades, sino también de costes. Los efectos combinados de los avances técnicos, la estandarización de componentes y la globalización de los mercados han ocasionado drásticas reducciones de costes en los elementos que integran los actuales sistemas de tratamiento de datos, alterando el equilibrio de la ecuación de costes de la seguridad.

El segundo de estos factores lo constituyen los datos almacenados. Ellos integran el activo a proteger y, por lo tanto, el patrón fundamental para medir lo que es razonable y justo invertir en su seguridad.

Finalmente, y tal como la Ley establece, el riesgo a que los datos personales almacenados o tratados están expuestos es el tercer gran factor a considerar a la hora de determinar cuáles son las medidas de seguridad razonables en cada caso. Si la naturaleza de los datos proporciona la medida del valor a proteger y por lo tanto del perjuicio a evitar, el riesgo a que están expuestos determina la probabilidad de que tal perjuicio se materialice. Por consiguiente, es la combinación de ambos factores (datos a proteger, riesgo a que están expuestos) la que determina el daño esperable que se derivaría de una inadecuada protección, y por lo tanto el nivel de protección exigible.

Podemos concluir, por lo tanto, que la Ley Orgánica proporciona un sistema de objetivos y criterios en materia de seguridad de los datos personales compatible con los principios y criterios generalmente aceptados en el mundo de la seguridad de los sistemas de información y que, aplicado de modo sistemático y complementado en lo necesario con las reglas, técnicas y procedimientos imperantes en dicho mundo, puede permitir discernir la aceptabilidad del conjunto de medidas de protección adoptadas en cada caso, hasta tanto no se plasmen dichos criterios en una regulación detallada como la prevista en los apartados 2 y 3 del artículo 9 de la Ley Orgánica.

5. LA SECRETARÍA GENERAL

Las principales actividades realizadas por la Secretaría General durante 1994 han ido dirigidas a poner en funcionamiento la Agencia para lo que se han efectuado las siguientes tareas y funciones:

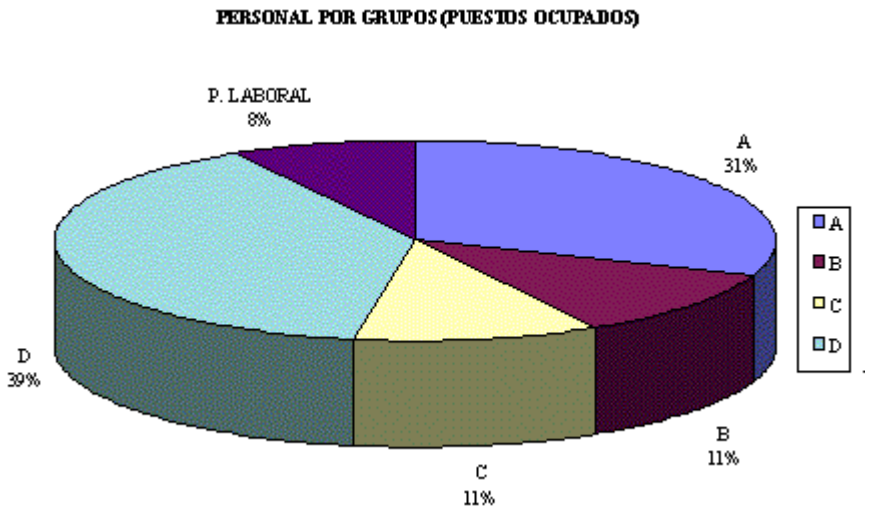
PLANIFICACIÓN, ORGANIZACIÓN Y GESTIÓN DE RECURSOS HUMANOS.

En esta materia se han realizado las siguientes actuaciones:

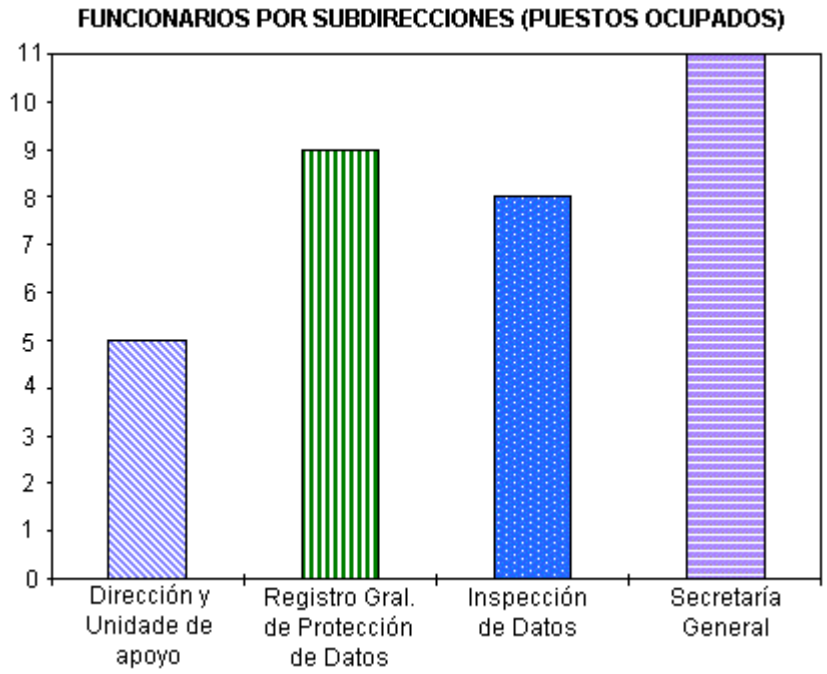
- Aprobación de la Relación de Puestos de Trabajo de la Agencia. La plantilla inicial de la Agencia con 33 puestos de trabajo no daba respuesta definitiva al gran volumen de actividad y desarrollo de competencias propias de la misma por lo que se manifiesta la necesidad de contar con personal altamente especializado, fundamentalmente en la Subdirección de Inspección, para el desempeño de las funciones inspectoras e instructoras que la Ley Orgánica atribuye a la Agencia, motivo por el cual se elaboró una propuesta de ampliación de la Relación de Puestos de Trabajo que, una vez aprobada, constituye su actual RPT con 46 puestos de trabajo que se proveen por funcionarios y 3 ordenanzas con vínculo laboral.

- La Agencia se estructura en los siguientes órganos:
  - El Director de la Agencia
  - El Consejo Consultivo

- El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General como órganos jerárquicamente dependientes del Director de la Agencia. Los puestos de trabajo de éstos órganos son los que integran la Relación de Puestos de Trabajo y son desempeñados por funcionarios.



Para la realización de los gráficos se ha tenido en cuenta la RPT partiendo de los puestos de trabajo efectivamente ocupados, ya sea con carácter definitivo o temporal.



- 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, así como cobertura por personal laboral eventual de las tres plazas de Ordenanzas.

- Programación de la futura Acción Social del Ente Público, siguiendo las recomendaciones previstas en el Acuerdo de Administración-Sindicatos para el periodo 1995-1997 sobre condiciones de trabajo en la Función Pública.

- Gestión y administración del personal funcionario y laboral destinado en la Agencia , y gestión de retribuciones y habilitación del mismo. Para la gestión de personal se ha implantado el sistema informático BADARAL proporcionado por el Ministerio para las Administraciones Públicas. En lo que se refiere a la elaboración y pago de nóminas se ha procedido a la instalación y utilización del sistema informático Nómina Estándar Descentralizada de la Administración del Estado (NEDAES).

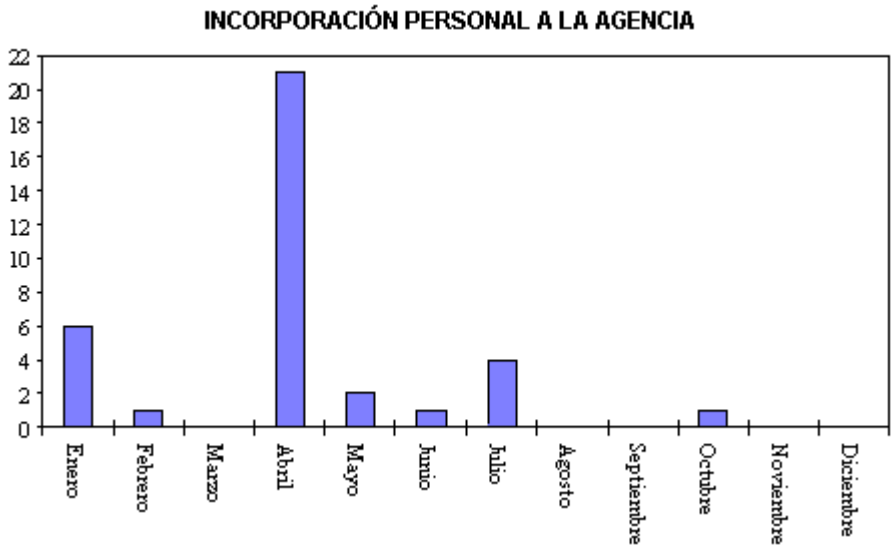
GESTIÓN ECONÓMICA Y PRESUPUESTARIA

- En materia presupuestaria, se ha constatado que el hecho de haberse confeccionado el presupuesto para 1994 cuando aún no existía la Agencia, hacía necesario la dotación, a través de un crédito extraordinario, de aquéllas partidas o conceptos presupuestarios que la implantación de la Agencia como Ente de Derecho Público de nueva creación fuera requiriendo, para acometer el desarrollo de proyectos, cuya óptima ejecución exigía dotaciones presupuestarias no contempladas en los iniciales presupuestos. Con objeto de resolver esta situación se ha tramitado un expediente dirigido a la concesión de una transferencia de crédito desde la sección 31 de Imprevistos a la Agencia, por un importe de 367.055.200 pts, distribuidas entre los Capítulos II (Gastos Corrientes) y VI (Inversiones), lo que ha permitido hacer frente al coste del funcionamiento, equipamiento, e inversiones necesarios para la inicial puesta en marcha de la Agencia.

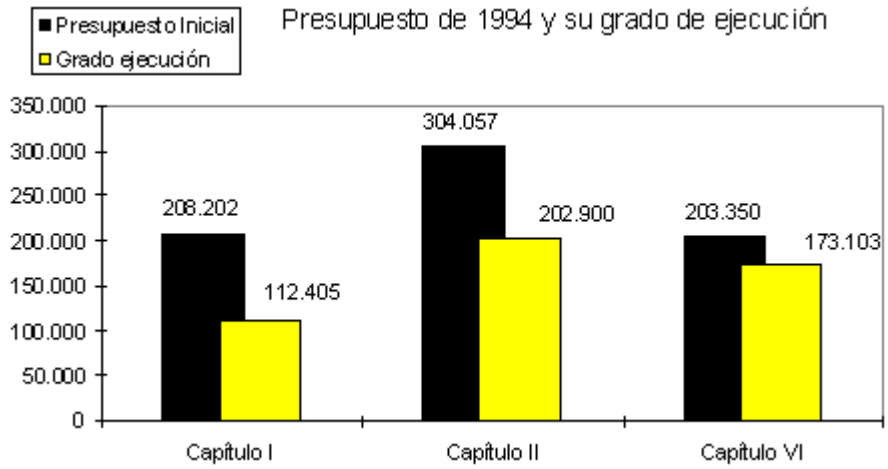
- Se ha implantado un Sistema Informático de Contabilidad (SICAI) con la colaboración y asesoramiento técnico de la Intervención General del Estado, lo que facilita el control financiero y contable del Ente Público.

- La ejecución y seguimiento presupuestario durante 1994 han ocupado buena parte de las actividades propias de la Secretaría General.

Asimismo debe ponerse de relieve que la incorporación de funcionarios a la Agencia se ha producido de manera escalonada a lo largo de todo el ejercicio, ocasionándose la mayoría de las incorporaciones en el mes de abril, sin que a su finalización, como se ha señalado anteriormente, estuviera completamente cubierta la Relación de Puestos de Trabajo. Esta circunstancia ha determinado que el grado de ejecución del gasto en Capítulo I (Gastos de Personal) en relación con el presupuesto asignado alcanzara el 54%.



Por lo que se refiere al grado de ejecución del gasto en relación con el Presupuesto de Gastos asignado en Capítulo II (Gastos Corrientes) y Capítulo VI (Inversiones) alcanzó el 67% y el 85% respectivamente. Estos porcentajes, especialmente el relativo al Capítulo II , tienen su fundamento en el hecho de que la puesta en marcha del Ente Público se produjera en 1994, siendo éste su primer año de funcionamiento, que no llegó a desarrollarse íntegramente hasta mediados de año, a lo que debe añadirse el hecho de que, hasta el mes de mayo, la Agencia ocupó instalaciones cedidas por el Ministerio de Justicia.



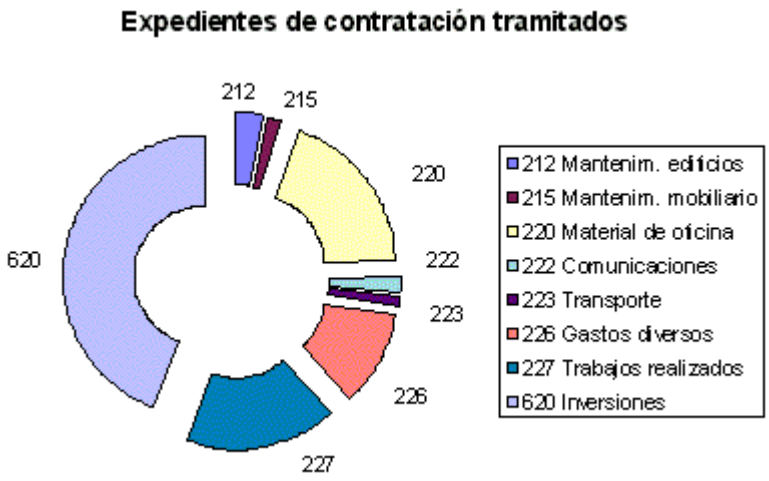
- Se han efectuado las modificaciones presupuestarias indispensables para ajustar las consignaciones presupuestarias a las necesidades reales, al amparo del artículo 34.2 del Estatuto de la Agencia, que atribuye al Director la competencia para autorizar las modificaciones internas del presupuesto que no incrementen la cuantía del mismo y sean consecuencia de las necesidades surgidas durante el ejercicio.

- Se ha suscrito un contrato de arrendamiento de las plantas 3ª, 4ª y 5ª del edificio del Paseo de la Castellana nº 41, con una extensión de 1.725 metros cuadrados, cifrándose el alquiler en 2.500 pesetas m² y 525 m² los gastos de comunidad. La duración de dicho contrato es hasta el 31 de diciembre de 1997 y la superficie alquilada permitirá hacer frente a las ampliaciones de plantilla previstas.

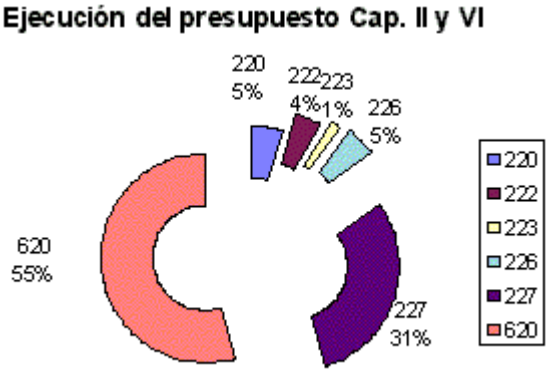
- Se ha elaborado y aprobado un Manual de Procedimiento sobre la gestión presupuestaria y del gasto de la Agencia, al amparo del artículo 34.3 de la Ley Orgánica que establece que la Agencia en sus adquisiciones patrimoniales y contratación estará sujeta al Derecho Privado, y del artículo 36 de su Estatuto que se expresa en similares términos. En el mismo se regulan, además de una norma provisional para la gestión interna de los créditos de la Agencia, el procedimiento de contratación que contempla diversas modalidades referidas a las distintas situaciones, peculiaridades y

cuantías objeto de la misma ,así como la regulación de las modificaciones internas del Presupuesto.

- Durante el año 1994 se tramitaron por la Agencia 154 expedientes de contratación que se imputaron a los capítulos II sobre gastos corrientes en bienes y servicios y VI de inversión nueva asociada al funcionamiento operativo de los servicios del Presupuesto de Gastos.



De estos datos 154 expedientes, 68 correspondieron a proyectos de inversión encaminados al equipamiento y puesta en marcha de la Agencia, habiéndose adquirido equipos de proceso de datos, ordenadores personales e impresoras. Además se llevó a cabo la adquisición de herramientas informáticas, tales como gestor de bases de datos, desarrollo de aplicaciones a medida para la gestión e implantación del Registro General de Protección de Datos, herramientas de productividad personal y mobiliario. Dentro del capítulo II son los conceptos 220 y 227 los que resaltan en cuanto al número de expedientes tramitados, ya que debió procederse a la adquisición del material de oficina ordinario e informático no inventariable y a la contratación de otras empresas para la realización de trabajos técnicos que no podían ser realizados con los recursos humanos y materiales de la Agencia, por no haber sido provistos todos los puestos de trabajo contemplados en la Relación de Puestos de Trabajo y por tratarse de actividades no constitutivas de los trabajos habituales de la Agencia, a lo que se unió la urgencia de la entrada en funcionamiento de los procesos e infraestructura informática que permitieran el cumplimiento de las funciones encomendadas a ella.



- Se suscribió un contrato con TABACALERA para la distribución y venta de los disquetes necesarios para la inscripción de ficheros automatizados, públicos o privados, que contengan datos de carácter personal en el Registro General de Protección de Datos. El ejercicio de este cometido supuso la venta de 62.388 disquetes, de los que 13.908 fueron vendidos directamente por la Agencia, obteniéndose unos ingresos de 7.649.470 pesetas, y 48.480 distribuidos por Tabacalera, obteniéndose unos ingresos de 19.007.039 pesetas una vez descontada la cantidad correspondiente por gastos derivados de la distribución.

El importe final recabado en concepto de venta de disquetes asciende a final de 1994 a 26.656.509 pesetas. Estos ingresos han sido incorporados a los recursos económicos propios del Ente Público de acuerdo con lo establecido en el artículo 32 c) de su Estatuto en el que se establece que éstos comprenderán, entre otros, los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades.

- Se han ingresado como recursos propios de la Agencia 4.844.896 pesetas en concepto de intereses, al amparo del artículo 32 d) del Estatuto que atribuye tal naturaleza a las rentas y productos de los bienes y derechos integrantes de su patrimonio.

OTRAS FUNCIONES Y TAREAS RECOGIDAS EN LOS ARTÍCULOS 30 Y 31 DEL ESTATUTO DE LA AGENCIA

- Se ha procedido a la elaboración del inventario de los bienes y derechos que integran el patrimonio de la Agencia.

- Se ha iniciado la formación de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales.

- Se organizó la Conferencia Internacional de Agencias de Protección de Datos de la Unión Europea cuya celebración tuvo lugar en Madrid durante los días 25 y 26 de mayo.

- Por último, 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 10 reuniones celebradas durante el año 1994.

INFORMACION AL CIUDADANO

La Ley Orgánica establece en el artículo 36 apartados d) y e) la función de la Agencia de atender las peticiones y reclamaciones formuladas por las personas afectadas y proporcionar información a los afectados acerca de sus derechos en materia de tratamiento automatizado de datos de carácter personal. El artículo 31. d) del Estatuto atribuye dicha función a la Secretaría General.

Desde abril de 1994, momento en que el Área de Atención al Ciudadano ha empezado a funcionar, la misión principal ha sido de apoyo al Registro en la Campaña de inscripción masiva, a través de la información directa a los destinatarios de la Ley Orgánica por una parte, y de otra, a través de la preparación de una campaña de información telefónica con una empresa especializada en el sector.

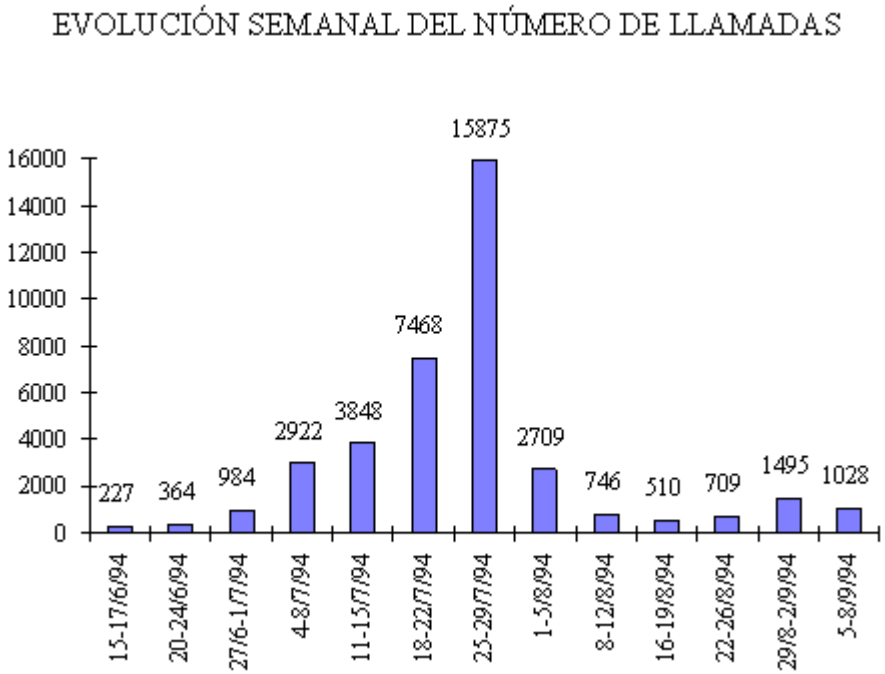
Una vez finalizada la campaña masiva, se ha prestado información telefónica, presencial y en contestaciones a consultas por escrito a ciudadanos, empresas y Administraciones Públicas.

A continuación se analizan las tareas llevadas a cabo en esta materia

La campaña telefónica para la inscripción masiva de ficheros automatizados.

Se realizó del 15 de Junio al 8 de Septiembre.

Durante el mismo el volumen de llamadas registradas en el período total ronda las 40.000. El número de llamadas que aproximadamente se ha recibido directamente en la Agencia ha sido del orden de las 4.000. En el siguiente cuadro se expresa la evolución del número de llamadas durante la campaña.



Paralelamente con la campaña telefónica se han emprendido otras acciones de difusion de la obligacion de inscribir ficheros en el Registro General de Proteccion de Datos.

Entre ellas por su importancia merecen destacarse:

Junio

- *Día 16 de junio* : anuncios en la prensa nacional de mayor tirada y en los periódicos regionales.

- *Día 21 de junio*: remisión de una circular de la Agencia a los Ayuntamientos recordándoles la necesidad de proceder a la publicación de una norma de creación o de adaptación del fichero, con fecha límite el 31 de julio.

- *Día 23 de junio* : intervención radiofónica del Director de la Agencia en la cadena SER.

- *Día 24 de junio*: dos intervenciones del Director de la Agencia televisadas en Telemadrid a las 14 horas, y en el Tele - diario de la primera cadena estatal a las 21 horas.

- *Día 26 de junio* : anuncios en la prensa nacional y regional de mayor tirada.

- *Día 28 de junio* : envío de 30.000 cartas a las empresas posibles titulares de ficheros automatizados.

Julio

- *Día 11 de julio*:a) Nuevo envío a las mismas empresas de recordatorio de la obligación de inscribir y con la adverten - cia de la sanción.b) Carta informativa a las Diputaciones Provinciales.

- *Día 18 de julio* : envío de 20.000 cartas a otras empresas diferentes para informar de la obligatoriedad de inscribir.

- *Día 18 de julio*: nuevo envío a las mismas empresas de recordatorio de la obligación de inscribir y con la advertencia de la sanción.

Observando la diferente resonancia de las distintas medidas, parece claro que el medio que ha tenido mayor acepta - ción y respuesta es el mailing. Los anuncios en prensa no han tenido excesiva repercusión. Sin embargo, las noticias recogidas en la prensa en forma de artículos y a pesar de algunos errores conceptuales, o incluso opiniones adversas, han tenido una repercusión importante en el número y calidad de las llamadas.

Probablemente, la mayor dificultad de los anuncios en prensa es, de un lado, la saturación existente en el mercado, y

del otro, el que el destinatario de la norma, al desconocerla completamente, no se reconoce como destinatario de la obligación, por lo que sólo sirve a los ya sensibilizados con el tema. El mailing combinado con la información telefónica salva muy bien este inconveniente.

Por otra parte, el carácter novedoso y complejo de la inscripción determina la necesidad de una información cualificada a los posibles destinatarios a través de sus Asociaciones, Colegios Profesionales, Cámaras de Comercio y demás entes de este carácter, lo que requiere necesariamente de su cooperación. Para el futuro, y dado que la campaña de inscripción tiene carácter continuo podría ser conveniente usar esta vía de información secundaria. El slogan podría ser "formar/informar a los posibles informadores".

El enfoque de la campaña posterior de información al ciudadano tendrá en cuenta la experiencia adquirida a este respecto.

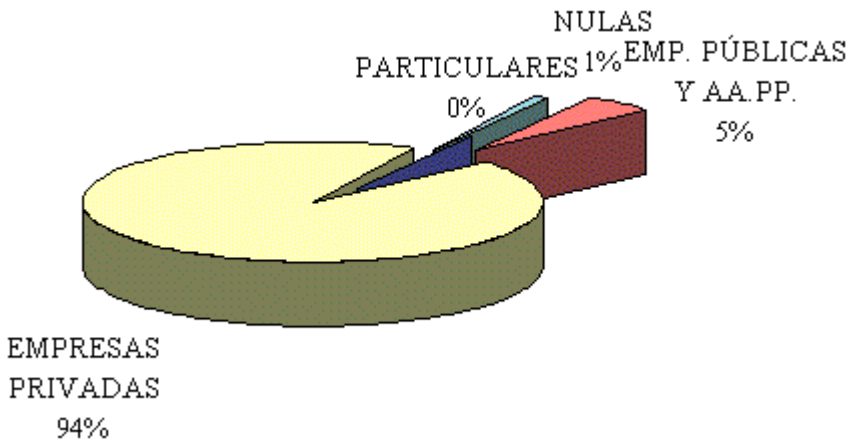
Distribución de llamadas por sectores

En el mes de junio el porcentaje de consultas llevadas a cabo por empresas privadas es del 61%, frente al 31% de Administraciones Públicas y el 2% de particulares. En julio y agosto el porcentaje de consultas de aquéllas frente a éstas es del 96% frente al 4%. Las consultas de los particulares son prácticamente inexistentes. La razón de la disminución porcentual de las llamadas de Administraciones y Empresas Públicas es que su número es más limitado que el de las empresas privadas, así como que disponen de más información oficial con la propia Agencia y a través de los órganos horizontales del Ministerio para las Administraciones Públicas. El mayor número de llamadas procede de los Ayuntamientos.

El incremento porcentual de las llamadas privadas se hace mucho más significativo desde la recepción del envio masivo por correo de la obligación de inscribir.

Seguidamente se refleja en el gráfico la distribución de llamadas por sectores.

Distribución de Llamadas por Sectores



Preguntas tipificadas

La pregunta más frecuente es el concepto de fichero inscribible, que representa prácticamente la mitad de las cuestiones, seguida por los datos que deben suministrarse en la notificación de los ficheros que representa en torno al 5%.

En otro orden de cosas, el 10% de las preguntas versa sobre aspectos relativos a cuestiones técnicas del modelo de inscripción en disquete.

Al margen de las preguntas tipificadas existen otras también muy frecuentes como la fecha de publicación de la ley o el reglamento, o los estancos en los que se puede adquirir el disquete, que suelen ir unidas a las anteriores, formando con ellas el núcleo de las consultas.

PORCENTAJE DE LA DISTRIBUCION DE LLAMADAS POR TIPOS DE PREGUNTAS

0.1 Responsable y titular del fichero	3,53%
0.2 Declarante	1,22%
0.3 Fichero Automatizado	0,93%
0.4 Fichero automatizado público y privado	0,53%
0.5 Datos de carácter personal	1,29%
1.1 Ficheros inscribibles	65,93%
1.2 Qué información debe suministrarse en relación con los ficheros automatizadoscon datos de carácter personal?	8,34%
1.3 Cuestiones relativas a la ubicación del fichero	0,95%
1.4 Cuestiones relativas al origen de los datos	0,53%
1.4.1 Cuestiones relativas a las fuentes accesibles al público	0,19%
1.4.1.1 Cuestiones relativas al Censo	0,07%
1.5 Cuestiones relativas a las cuestiones meramente técnicas del disquete.	13,92%
2.1 Cuestiones relativas a la calidad de los datos (adecuados, pertinentes y no excesivos para las finalidades legítimas).	0,39%
2.2 Cuestiones relativas al consentimiento e información en la recogida de los datos	0,19%
2.3 Cuestiones relativas a datos de carácter personal se carácter sensible	0,08%
2.4 Cuestiones relativas a la seguridad de los datos	0,19%
2.5 Cuestiones relativas al deber de conservación de los datos	0,03%
2.6 Cuestiones relativas al deber secreto	0,01%
3.1 Cuestiones relativas al concepto de cesión	1,02%
3.2 Cuestiones relativas a los requisitos y el modo de prestar el consentimiento para la cesión	0,14%
3.3 Cuestiones relativas a las excepciones del consentimiento de la cesión	0,04%
4.1 Cuestiones relativas al concepto de transferencia	0,28%
4.2 Necesidad de autorización	0,03%
4.3 Necesidad de comunicación en la inscripción	0,03%
5.1 Cuestiones relativas al ejercicio directo por los afectados	0,05%
5.2 Cuestiones relativas al ejercicio mediante representación (representante, abogado, uniones de consumidores)	0,01%
5.3 Cuestiones relativas a la tutela de los derechos por parte de la Agencia de Protección de datos (denuncias, quejas, reclamaciones y similares) a instancia de los particulares	0,06%
5.4 cuestiones relativas a la tutela de los derechos por parte de los Tribunales	0,001%

Consultas telefónicas realizadas directamente a la agencia desde el final del período de inscripción masiva hasta final de año.

Se ha realizado un promedio de 70 llamadas diarias desde los primeros días de septiembre hasta final de año, de las que el 85% han sido llamadas relacionadas con la subsanación de defectos de la notificación de inscripción, el 5% han sido llamadas en relación con la obligación de inscribir ficheros automatizados y el 10% restante tienen relación con solicitud de información sobre el ejercicio de los derechos de los ciudadanos y formas de reclamación. La información en relación con la inscripción en el Registro ha ido disminuyendo paulatinamente mientras se incrementaba la solicitud de información sobre los derechos reconocidos en la Ley Orgánica.

Temas principales de las consultas por escrito

Consultas realizadas por organismos públicos

A.El carácter obligatorio de la inscripción para los Colegios Profesionales:

- La Agencia considera que los ficheros que utilizan los Colegios Profesionales, integrados por datos tales como el nombre, dirección, especialidad a la que se dedican, entre otros, sólo cumplirían la finalidad de publicidad prevista en el artículo 2.2 a) de la Ley en la medida en que la finalidad y usos de esta base de datos fuera tan sólo la de publicidad con carácter general, con lo que quedarían exentos en principio de la obligación de inscribir estos ficheros.

- Por otra parte, estos ficheros suelen usarse además con otras finalidades, por lo que deben inscribirse en el Registro, dado que de acuerdo con la definición del artículo 1.3. del Reglamento tendrían el carácter de datos accesibles al público, 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.

B.Cesión de datos de diversas Administraciones a la Administración Tributaria (Del Estado, de las Comunidades Autónomas o de la Administración Local).

La cesión por parte de cualesquiera Administraciones Públicas de los datos solicitados para los fines de recaudación tributaria, no requeriría del consentimiento del afectado por ser de aplicación el artículo 111 de la Ley General Tributaria, de conformidad con lo establecido en el artículo 11. 2 a) de la Ley Orgánica, estableciendo que no se requerirá el consentimiento del afectado cuando una Ley prevea otra cosa. En el artículo 111 de la Ley General Tributaria se establece con carácter general que:

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

De acuerdo con lo previsto en el párrafo anterior en particular:

4. Los funcionarios públicos, incluidos los profesionales oficiales, están obligados a colaborar con la Administración de la Hacienda Pública para suministrar toda clase de información con trascendencia tributaria de que dispongan, salvo que sea aplicable:

a) El secreto del contenido de la correspondencia.

b) El secreto de los datos que se hayan suministrado a una Administración para una finalidad exclusivamente estadística.

6. Los datos, informes o antecedentes obtenidos por la Administración Tributaria, en virtud de lo dispuesto en este artículo, sólo podrá utilizarse para los fines tributarios encomendados al Ministerio de Economía y Hacienda y en su caso, para la denuncia de los hechos que puedan ser constitutivos de delitos monetarios, de contrabando, contra la Hacienda Pública y, en general, de cualesquiera delitos públicos."

C.Cesión de datos del padrón municipal y padrones fiscales a la Tesorería General de la Seguridad Social.

La Agencia considera que la solicitud de tales datos por parte de la Tesorería General de la Seguridad Social no es acorde con la Ley Orgánica, dado que la misma ni estaba prevista en una ley, ni estaba prevista en términos generales en las normas de creación de los ficheros, ni se trataba de competencias iguales o que versen sobre las mismas materias. No obstante, ley 42/94 de 30 de diciembre habilita a la Seguridad Social para recabar los datos necesarios dentro del procedimiento de apremio de cualesquiera Administraciones y particulares para el cumplimiento de esa función.

D.Cesión de datos del padrón municipal para estudios privados.

Para poder proceder a la cesión, sin el consentimiento del interesado y sin que lo autorice una Ley, sería necesario el previo procedimiento de disociación, entendido como todo tratamiento de datos personales de modo que la información

que se obtenga no pueda asociarse a persona determinada o determinable, es decir, que el Ayuntamiento en cuestión podría ceder la información resultante de la operación de la despersonalización de la misma, por lo que los datos cedidos tendrán entonces un valor meramente estadístico, tal y como se prescribe en el artículo 11.6 de la Ley Orgánica.

E.Cesión de datos del padrón municipal para estudios epidemiológicos.

Se han solicitado datos para diversos programas de prevención de diferentes enfermedades. La Agencia considera que la cesión de los datos personales para realizar estudios, a una Institución Sanitaria de carácter público, es conforme con la Ley Orgánica siempre que se respeten los principios a que hace referencia la legislación sanitaria (el artículo 8 de la Ley Orgánica que se remite a los artículos 8, 10 y 23 de la Ley General de Sanidad).

En estos preceptos de la Ley General de Sanidad se considera como actividad fundamental del sistema sanitario la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica, en concordancia con los principios tales como el respeto a la personalidad, dignidad humana e intimidad, así como la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas.

Para la consecución de estos objetivos, de intervención pública en relación con la salud individual y colectiva, las Administraciones Sanitarias, de acuerdo con sus competencias, pueden crear Registros y elaborar los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse actuaciones de la autoridad sanitaria.

Estos preceptos deben interpretarse dentro del respeto a los principios establecidos en el artículo 4.1. de la Ley Orgánica; a saber, que los datos sean pertinentes y no excesivos en relación con el ámbito y finalidades para las que se recogieron. Esto significa que no son conformes a la Ley Orgánica las peticiones genéricas de datos no asociadas a un programa concreto de estudio o investigación epidemiológica, ni aquellos en que los datos solicitados no sean pertinentes para la finalidad que se persigue en los mismos.

F.La tarjeta sanitaria como elemento identificativo con la posibilidad de incorporar el historial clínico.

La posibilidad de cifrar los datos que van incluidos en la tarjeta, sin el conocimiento del usuario atentaría gravemente contra el derecho a la información en la recogida de los datos, reconocido en la Ley Orgánica en su artículo 5 en general, y en concreto en el apartado c), dado que en este caso se estaría ocultando las consecuencias de la obtención de los datos, y además podrían acabar utilizándose los datos relativos a la salud en contra del propio afectado.

En definitiva, se estaría atentando contra el derecho de acceso considerado en un sentido amplio como un derecho a conocer los datos de carácter personal incluidos en un fichero automatizado, como garantía a su vez de la exactitud y veracidad de los datos tratados automatizadamente.

Consultas realizadas por particulares

A.Ficheros de empresas administradas por gestorías, asesorías, o análogos: determinación del sujeto obligado a efectuar la inscripción.

Dada la división entre titularidad de los datos, que corresponde a la empresa que los aporta y la informatización de éstos que corresponde a la gestoría, la decisión sobre quién debe figurar como responsable en la declaración corresponde en último término a la empresa en relación con su Asesoría o Gestoría, dado que la Agencia considera ajustadas a derecho ambas posibilidades, de acuerdo con el artículo 3 d) que define al responsable del fichero como la persona física o jurídica, de naturaleza pública o privada que decida sobre la finalidad, uso y contenido del tratamiento.

B.Sobre el deber de inscribir los ficheros automatizados de contabilidad, nóminas, proveedores y clientes.

El criterio determinante para proceder a la inscripción de un fichero es el tratamiento automatizado de los datos relativos a personas físicas; por lo que si se poseen ficheros automatizados de contabilidad, proveedores, clientes o nóminas, o cualesquiera otros que contengan datos de esta clase se deberá proceder a la inscripción del fichero en el Registro.

C.Ejercicio del derecho de acceso, rectificación y cancelación.

Algunos ciudadanos se han dirigido a la Agencia para ejercer estos derechos, bien en la creencia de que ésta era la depositaria de todos los datos, o que a través de la misma podía hacer efectivos de manera directa tales derechos.

En virtud de la legislación vigente en esta materia, los derechos de acceso, rectificación y cancelación son personalísimos, y deben, por tanto ser ejercidos directamente sus titulares ante cada uno de los responsables de los ficheros automatizados, lo que significa que el afectado debe dirigirse a cada uno de ellos.

La Agencia sólo puede suministrar la dirección de la oficina designada por el titular del fichero para ejercer los derechos de acceso, rectificación y cancelación, de aquellas entidades o personas de las que se solicite de manera individualizada, bien por tener el conocimiento a ciencia cierta de que poseen datos relativos a quien efectúa la consulta, bien porque se puede presumir que los tienen, para que con esta información el afectado se dirija directamente a los titulares de los ficheros automatizados.

En el caso de que en el plazo de un mes, para el derecho de acceso, y de 5 días, para los de rectificación y cancelación, desde la recepción de la solicitud en la oficina referida, no haya sido atendida adecuadamente, podrá dirigirse a la Agencia con copia de la solicitud cursada para que ésta a su vez se dirija al responsable del fichero con el objetivo de hacer efectivo el ejercicio de los derechos solicitados.

D.Ejercicio de acceso, rectificación y cancelación

***** En especial: cancelación de los ficheros de marketing

Aquellas personas que reciben información comercial y desean la cancelación de los datos en los ficheros de marketing deben seguir el procedimiento general. Ahora bien, para facilitar esta tarea, la Asociación de Marketing Directo ha creado la lista Robinson, con el fin de excluir de la publicidad de las empresas que componen su Asociación a aquellas personas que no deseen recibir publicidad comercial, para lo que deberán indicar su voluntad de ser incluido en esa lista para este fin.

En el caso de empresas que no pertenezcan a esta Asociación el afectado deberá dirigirse a los responsables de los ficheros de modo individualizado para que cancelen sus datos de los ficheros correspondientes.

E.Sobre el consentimiento para la cesión

La expresión "consentimiento previo" del afectado a que se hace referencia en el artículo 11 se debe interpretar de modo sistemático en el conjunto de la Ley. En términos generales podemos establecer tres modos o formas básicas de consentimiento: expreso, tácito y presunto.

El consentimiento expreso se manifiesta mediante un acto positivo y declarativo de la voluntad. El consentimiento tácito se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume o se presupone como un acto de aquiescencia o aceptación. Por último, cabe el consentimiento presunto, que no se deduce ni de una declaración, ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

La Agencia viene interpretando que el consentimiento a que se hace referencia en el artículo 11, ha de ser previo, pero puede ser tanto expreso o tácito, como presunto, porque de una interpretación sistemática de la Ley Orgánica, se deducen claramente aquellos supuestos en los que la Ley exige que el consentimiento sea expreso, como en el caso de los datos especialmente protegidos (artículo 7), que además debe otorgarse por escrito. *Sensu contrario,* cuando no se requiere que sea expreso, la Agencia interpreta que el consentimiento en cualquiera de las modalidades referidas es conforme a la Ley Orgánica, lo que será de aplicación para la cesión, en cuyo caso sólo se exige que el consentimiento exista con carácter previo, debiendo además señalarse que, de acuerdo con lo establecido en el artículo 11.4 de la Ley Orgánica, el consentimiento es revocable en cualquier momento.

F.Diferencia entre la prestación de servicios automatizados y cesión de datos de carácter personal

En el artículo 27 de la Ley Orgánica se regula la figura de la prestación de servicios de tratamiento automatizado de datos de carácter personal. En este precepto se establece la obligación de que quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de esta clase, 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, a terceras personas.

Por tanto no se trata de un supuesto de cesión de los regulados por el artículo 11 de la Ley Orgánica sino de una actividad empresarial para una finalidad concreta y determinada, que es la señalada e impuesta con las limitaciones que se describen en el artículo 27.

MEMORIA DE 1994 - CÓDIGOS TIPO

Durante 1994 se presentaron para su inscripción en el Registro General de Protección de Datos dos proyectos de códigos tipo: uno, por Telefónica de España S.A. y otro, perteneciente a la Asociación denominada ASEICO, (relativa a informes comerciales). Ambas peticiones se hallaban justificadas, la primera por el importante volumen comercial de la empresa solicitante y por tratarse de una materia tan especial como son las comunicaciones desde el punto de vista de la defensa de la intimidad, y la segunda, por referirse a una materia específicamente regulada en el artículo 28 de la Ley Orgánica. Las dos solicitudes tenían igualmente fundamento en las expresiones "acuerdos sectoriales" y "decisiones de empresa" contenidas en el artículo 31 de la misma.

Ha de señalarse que, en la tramitación de la inscripción que de los códigos tipo se establece en el número 2 del citado precepto, se ha establecido la obligación de cumplir con varios requisitos, bien dirigidos a dar participación en la tramitación de los mismos al Consejo Consultivo, con el fin de que pueda formular las alegaciones que estime procedentes, bien a establecer un sistema que permita conocer en cada momento el número y denominación de las empresas afectadas por los acuerdos sectoriales y a comunicar a la Agencia cualquier sanción que por la Asociación pueda imponerse como consecuencia de algún incumplimiento del código deontológico.

Durante 1994 solamente se ha inscrito en la Agencia el Código tipo de Telefónica de España S.A. con el contenido que se establece en el anexo II de la presente Memoria.

MEMORIA DE 1994 - ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES DE LOS DISTINTOS PAÍSES EN MATERIA DE PROTECCIÓN DE DATOS

LA DIRECTIVA MARCO DE PROTECCIÓN DE DATOS

Dentro de la Unión Europea, e indirectamente dentro del Espacio Económico Europeo, la regulación de la protección de datos tiene como referente obligado la propuesta modificada de Directiva de protección de las personas físicas en lo relativo al tratamiento de datos personales y a la libre circulación de los mismos, o Directiva marco de protección de datos (SYN 287). El 18 de julio de 1990, fue presentada por la Comisión al Consejo una primera propuesta, dentro de un paquete, que comprendía otra propuesta de Directiva de protección de datos en el contexto específico de los servicios de telecomunicación prestados mediante las redes públicas digitales de servicios integrados y las redes públicas de telefonía móvil, más una propuesta de Decisión sobre seguridad en los entornos informáticos, una recomendación sobre la aplicación de la Directiva por parte de las instituciones comunitarias, y una recomendación por la que se propugnaba la adhesión de la Comisión Europea al Convenio del Consejo de Europa de 1981 (Convenio 108). Esta primera propuesta acusaba una marcada influencia de la entonces reciente ley federal alemana de protección de datos de 1990, mediante la cual se había revisado la de 1977 para recoger la doctrina sentada por el Tribunal Constitucional Federal en la sentencia relativa a la Ley del Censo de Población de 1982.

La propuesta de Directiva preveía, por ello, un tratamiento diferenciado de los ficheros del sector público, de una parte, y los ficheros del sector privado, de otra. Asimismo, recogía una definición de fichero, inspirada en dicha ley, que permitía hacer extensivo el régimen protector a los ficheros no informatizados o manuales. La propuesta recogía, a modo de complemento, preceptos de otras leyes, tales como la ley francesa de 1978 (prohibición de decisiones basadas exclusivamente en tratamientos informatizados, notificación obligatoria e indiferenciada de todos los ficheros). Tambíen en la misma se recogía del Derecho alemán conceptos como los de interés preferente y mejor derecho, que correspondían a un ordenamiento jurídico basado en un mayor arbitrio judicial que los de los demás Estados. La mayoría de los Estados miembros, aun admitiendo la conveniencia de una actuación comunitaria sobre la materia, mostraron reservas sobre la propuesta de Directiva. Ante todo, dada la incidencia de la regulación prevista de la problemática de los derechos y libertades individuales, resultaba dudoso que la Comunidad Europea, cuyos fines institucionales son esencialmente económicos, tuviera una legitimación para reglamentar esta materia. En segundo lugar, el excesivo detalle de la regulación (una treintena de artículos, frente a un máximo de nueve o diez que suelen comprender en general las directivas) invitaba a un cambio de postura que, para algunos Estados miembros, debía consistir en aceptar con algunos retoques el Convenio 108 del Consejo de Europa y elaborar un Reglamento, solución que ha seguido la Comisión en otros contextos. Iniciadas las negociaciones en febrero de 1991, la base jurídica invocada por la Comisión (artículo 100 A del Tratado de la Comunidad Económica Europea) trajo consigo la sumisión al procedimiento de cooperación con el Parlamento Europeo (artículo 189A). El Parlamento emitió dictamen en los primeros meses de 1992, siendo aprobado el dictamen el 11 de marzo de 1992.

La Comisión redactó una nueva propuesta, en la que se recogían las modificaciones del dictamen del Parlamento Europeo y en septiembre de 1992 elevó la nueva propuesta al Consejo, reanudándose las negociaciones en dicha fecha. La nueva propuesta modificaba sustancialmente la primera, suprimiendo la distinción formal entre las regulaciones de ficheros del sector público y del sector privado, haciendo hincapié en el concepto de tratamiento, en lugar del de fichero, y flexibilizando lo referente a la exigencia del consentimiento y a la notificación e inscripción de los tratamientos, como condición del ejercicio de los derechos de acceso y rectificación. Dentro de esta segunda etapa, y a instancia de algunas delegaciones, el Servicio Jurídico de la Comisión se pronunció acerca del problema de la legitimación comunitaria para regular la materia de protección de datos, precisando que el objetivo básico de la Directiva no era instrumentar una protección uniforme de los datos personales, sino sólo en tanto en cuanto que dicha protección constituía una restricción obligada de la libre circulación de la información en el seno de la Comunidad. La Directiva sólo pretendía, pues, fijar un presunto nivel máximo de protección a escala comunitaria, de tal suerte que la protección de los datos personales no pudiera invocarse como una restricción a la libre circulación de los mismos.

El proceso negociador se inició en febrero de 1991, bajo presidencia luxemburguesa y a continuado bajo las presidencias de los Países Bajos (1991), Portugal (1992), Reino Unido (1992), Dinamarca (1993), Bélgica (1993), Grecia (1994) y Alemania (1994). La presidencia del Grupo negociador ha sido ejercida por las Autoridades de protección de datos (Luxemburgo, Países Bajos, Dinamarca, Alemania), por los ministerios de Justicia (Bélgica, Portugal), por personal de la Representación Permanente (Reino Unido) o por personas designadas al efecto (Grecia). La Agencia de Protección de Datos ha contribuido a la negociación de la propuesta de Directiva, asistiendo, de enero a marzo de 1994, a las sesiones del Grupo negociador, y con posterioridad evacuando informes sobre aspectos concretos de la propuesta: artículo 4 (Derecho aplicable), artículo 9 (libertad de expresión, protección de datos y creación artística y literaria), aplicación a los ficheros manuales (propuesta del Reino Unido). La Agencia organizó asimismo los días 25 y 26 de mayo una conferencia plenaria de las Autoridades de protección de datos de los Estados de la Unión Europea, que tuvo lugar en Madrid, y en la cual se deliberó sobre la revisión, en su caso, de la posición común que había sido adoptada sobre la propuesta de Directiva en las conferencias plenarias celebradas por dichas Autoridades en Dublín (diciembre 1992), Boppard de Rhin (marzo 1993) y París (abril 1993). Las deliberaciones de Madrid no dieron lugar a una nueva posición común de las Autoridades de protección de datos. Tampoco en la XVI Conferencia mundial de Autoridades de protección de datos, que se celebró en La Haya los días 6-8 de septiembre, se estimó conveniente revisar dicha posición, por estimar que existía un consenso suficiente a escala comunitaria sobre el texto y que las discrepancias aún apreciables no tenían una entidad tal que aconsejara una nueva toma de posición en aspectos de detalle.

La Conferencia mundial apoyó tácitamente el esfuerzo de la presidencia alemana del Consejo de la Unión por llegar a

la posición común en el seno del Consejo dentro de su semestre. Al margen de estas actuaciones conjuntas, las distintas Autoridades de protección de datos se han ido pronunciando sobre la propuesta en sus memorias anuales. Los Estados miembros no se han pronunciado sobre la propuesta fuera del ámbito de las negociaciones del Consejo, si se exceptúa Francia, cuya Asamblea Nacional ha emitido dos informes, el 4 de diciembre de 1991 (documento núm. 2403, 9ª legislatura) y el 2 de junio de 1993 (documento núm. 264, 10ª legislatura), ambos referidos a la incidencia de la Directiva en el Derecho francés. Por último, organizaciones diversas se han pronunciado sobre la propuesta: UNICE, la Federación Bancaria de la Comunidad Europea, Amnesty International, European Savings Bank Group, Confederation of British Industry, American Express y la F.E.D.I.M. (*Data Protection Law and Practice in the European Union*, 1993). El proceso negociador se ha prolongado más de lo que es habitual en estas actuaciones, debido a algunas posiciones irreductibles expuestas por las delegaciones en el seno del Grupo Negociador del Consejo. Este retraso ha tenido una repercusión desfavorable con relación a otras iniciativas que inciden de un modo u otro en la protección de datos. Es el caso de las Directivas de telecomunicaciones (oferta de red abierta, telefonía vocal, servicio universal telefónico) y de la propia propuesta de Directiva de protección de datos en las redes digitales de servicios integrados (SYN 288), incluida en el primitivo paquete de la Comisión. Asimismo, la Directiva sobre ventas a distancia (SYN 411). El retraso en la aprobación de la Directiva SYN 287, o Directiva marco, ha determinado una pérdida de conciencia progresiva sobre los problemas de protección de datos en los contextos sectoriales.

Por todo ello, a partir del segundo semestre de 1993, pudo advertirse un esfuerzo por parte de las Presidencias del Consejo, por acelerar el proceso negociador y llegar a una posición común lo antes posible, incluso dentro del semestre respectivo. Durante las presidencias belga y helénica no fue posible esta posición común. Al fin, la presidencia alemana, correspondiente al segundo semestre de 1994, ha logrado llegar a esta posición común, que fue aprobada en principio en el Consejo de Mercado Interior que tuvo lugar el 6 de diciembre en Bruselas, y examinada de nuevo en el Consejo de Sanidad del 21 de diciembre, en el cual se llegó a un acuerdo sobre el único punto que, al parecer, era objeto de discrepancia, el de la modalidad de ejercicio de las competencias de ejecución que, dentro del marco de la Decisión 87/373/CEE, el texto atribuye a la Comisión Europea. Se espera que la posición común del Consejo quede aprobada durante el próximo año. Con ello no queda todavía aprobada la Directiva, puesto que, a tenor del Tratado de la Unión Europea de 1991 (artículos 100A y 189B), el texto deberá ser sometido al Parlamento Europeo, por el cauce del procedimiento de codecisión.

El texto acordado es resultado de una afinación progresiva de la propuesta modificada de Directiva de 1992. La sistemática de la propuesta se ha mantenido. Las modificaciones se han hecho por cauces diversos: supresión de los primitivos artículos 10, 20, 24 y 29 e inclusión de sus preceptos en otros artículos; adición de nuevos "Considerandos" y propuesta de declaraciones de delegaciones o conjuntas de la Comisión y del Consejo para su inclusión en el acta de la sesión del Consejo pertinente. Se han reelaborado los artículos 4, 5, 7, 8, 14, 17, 18, 21, 27, y 28 y se han añadido los actuales artículos 17 y 20. Si bien los "Considerandos" tienen un valor interpretativo del articulado, las declaraciones del acta del Consejo no tienen un valor jurídico, sino meramente indicativo de las posiciones nacionales o de orientación a efectos de la transposición.

En términos generales, la concepción que inspirara la primitiva propuesta de 1990 ha variado en diversos aspectos. Desde la propuesta primitiva de 1990, la protección de los datos de carácter personal ha sido contemplada, no como un mecanismo protector de las libertades y derechos, sino como una limitación a la libre circulación de los datos en el seno de la Comunidad. Como tal, debía ser objeto de interpretación restrictiva, a diferencia del Convenio 108 del Consejo de Europa, cuyo artículo 11 autoriza a los Estados parte a elevar el nivel de la protección del Convenio. La Directiva no podría, por ello, ser invocada como una traba para dicha libre circulación. En contrapartida, el nivel de protección habría de ser el más elevado. Sólo así se garantizaría un equilibrio entre la libre circulación de los datos en cuanto condición indispensable de la plena efectividad del mercado interior, y la protección de los derechos y libertades de las personas.

El texto de la posición común desvirtúa este propósito de equilibrio, en la medida en que el nivel de protección ha descendido. En términos generales, el nivel de protección es tanto más elevado cuanto mayor sea el control que sobre sus propios datos pueda ejercer el interesado. La memoria explicativa de la propuesta primitiva definía el "alto nivel de protección" sobre la base de varios criterios: en primer lugar, el ámbito de cobertura. El alto nivel de protección exige que la misma se aplique a todos los supuestos en los que el tratamiento de los datos lleva consigo un riesgo para los interesados. En consecuencia, la Directiva debe aplicarse a ficheros automatizados y manuales y a ficheros públicos y privados. En segundo lugar, el nivel de protección viene definido por la exigencia de unos criterios de licitud (calidad de los datos, consentimiento del interesado), unas normas sobre cesión de datos a terceros, notificación de los ficheros con miras a hacer posible su conocimiento o un control previo, responsabilidad patrimonial del responsable del tratamiento. En cualquier caso, el texto de la posición común reduce el control del interesado sobre sus datos. Este menor control se refleja en una reducción del ámbito de aplicación y en una relajación de los demás elementos.

La primera variable que determina el nivel de protección viene dada por el ámbito de aplicación de la Directiva. Varios son los aspectos que cabe distinguir en este contexto. En primer lugar, el ámbito de aplicación *ratione materiae.* La posición común lo ha acotado mediante la incorporación de conceptos que no estaban presentes en la primitiva propuesta ni en la de 1992. Siguiendo una iniciativa francesa, se deliberó sobre la conveniencia, en su caso, de hacer extensivo el concepto de "datos" a la información consistente en imágenes y sonidos. El texto excluye de la aplicación de la Directiva los datos que se derivaren de esta información, estimando en el "Considerando" 15º que sólo quedan cubiertos por la Directiva en la medida en que sean susceptibles de tratamiento auatomatizado o registro estructurado que contenga como criterio de organización un sistema que permita acceder con facilidad a datos de carácter personal. Con esto se recoge, aunque sólo en el contexto interpretativo, y con una fundamentación distinta, la solución de la ley federal alemana, cuyo § 3 excluye del concepto de fichero no automatizado los documentos que consistieren en soportes de imágenes o sonidos. Habida cuenta, por otra parte, de que el problema de fondo que se había suscitado en Francia se refería, en realidad, al uso de la información de esta naturaleza recogida mediante dispositivos de vigi-

lancia magnetoscópica emplazados en lugares públicos por las Autoridades de policía, la cuestión incidía a la vez en el problema general de la aplicabilidad de la Directiva a los ficheros policiales. Por ello, el "Considerando" 16º precisa que estos datos, cuando procedan de actuaciones policiales de vigilancia magnetoscópica, no están incluidos en la Directiva por tratarse de materias ajenas al Derecho comunitario. Otro aspecto del ámbito de aplicación *ratione materiae* es la cuestión de la aplicabilidad de la Directiva a los expedientes y a los documentos de papel impreso.

El concepto de "expediente" procede de la ley alemana federal, cuyo § 3, párrafo segundo, define el expediente (*Akte*) como todo documento que no pueda ser calificado de fichero automatizado, ni de fichero no automatizado. Los expedientes y colecciones de expedientes no son ficheros, a menos que puedan ser reordenados o explotados por procedimientos automáticos. Son, por tanto, cualesquiera otros documentos, oficiales o de servicio, aun cuando consistieren en soportes de imágenes o de sonidos. Esta exclusión ha sido recogida, no en el texto articulado, ni tampoco en los "Considerandos", sino en una declaración que el Consejo y la Comisión proponen incluir en el acta del Consejo que apruebe la posición común. En la misma propuesta de declaración se excluyen los documentos de papel impreso, haciendo extensiva la exclusión a los producidos mediante aparatos de telefax, los cuales estarán sujetos a las normas aplicables a los datos manuales y, como tales, sólo estarán cubiertos por la Directiva si figuran en un fichero no automatizado. Este concepto de "fichero no automatizado", pese a que la Directiva le es aplicable, tampoco está definido en el articulado, sino asimismo en el "Considerando" 15º: "ficheros estructurados según criterios específicos relativos a las personas, al objeto de hacer posible un acceso fácil a los datos de carácter personal".

Desde la primitiva propuesta, los *ficheros no automatizados,* manuales o convencionales, se han considerado incluidos en el ámbito de aplicación de la Directiva, pues así resulta de la definición de fichero del artículo 2(c). Esta definición concuerda con la de la ley federal alemana de 1990 (§ 3, párrafo segundo). En el curso de la negociación hubo siempre una oposición irreductible del Reino Unido, secundada a veces por Irlanda, en contra de la aplicación de la Directiva a estos ficheros. A modo de compromiso, el artículo 33 prevé un periodo transitorio de tres años para adaptar la Directiva a estos ficheros, siempre que se trate de ficheros utilizados en el momento de la aprobación de la Directiva. Este plazo se eleva a doce años en lo que respecta a la adaptación de las disposiciones de los artículos 6, 7 y 8, es decir, los principios sobre calidad de los datos, criterios de licitud de los tratamientos, y tratamiento de los datos sensibles. En todo caso, aun durante el periodo transitorio, los Estados deberán reconocer a los interesados los derechos de rectificación, cancelación o bloqueo de sus datos, previo su acceso, siempre que los datos no sean completos o exactos o se hayan almacenado de forma incompatible con los fines legítimos del responsable del tratamiento. Este régimen transitorio podrá no aplicarse a los datos que se conservan sólo con fines de investigación histórica.

El ámbito de aplicación se perfila con la disposición del artículo 3.2. El Tratado de la Unión Europea, en especial los Títulos V y VI (artículos J y K), incorporaron nuevas competencias a la Unión Europea. Cabía entender que el sistema protector de la Directiva se hacía extensivo a tratamientos de datos creados y utilizados en el marco de la política exterior y de seguridad común y de la cooperación en materia de justicia e interior. El nuevo artículo 3.2 aclara que estos tratamientos no están cubiertos por la Directiva, precisándose en el "Considerando" 13º que tales actividades no están comprendidas en el Derecho comunitario.

El ámbito de aplicación se acota en parte para los tratamientos efectuados para determinadas finalidades, como son las de investigación histórica, científica o estadística. Estas finalidades pueden dar lugar a restricciones en cuanto a la aplicación de los principios de finalidad y de conservación limitada de los datos en función de los fines del tratamiento (artículo 6.1 (b) y (e) del texto de la posición común), así como del deber de informar al interesado con ocasión de la recogida de datos (artículo 11.2) y del derecho de acceso (artículo 13.2).

También en función de la finalidad se acota en parte el ámbito de aplicación. Es el supuesto del artículo 9, que dispone que los Estados miembros establecerán excepciones, respecto de las disposiciones del Capítulo II, IV y VI, que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión. Las excepciones se refieren a los Capítulos II (condiciones generales de licitud de los tratamientos), IV (transferencia de datos a terceros países) y VI (Autoridad de control), prácticamente todo el sistema protector de la Directiva. La primera causa de excepción, la libertad de expresión periodística, se halla ausente de la ley española, por ejemplo, pero está presente en las leyes de Francia y de Alemania. Es lo que se viene denominando el "privilegio de los medios de comunicación social" y su finalidad es no coartar el uso del tratamiento automatizado de datos en las tareas de redacción de artículos y noticias de prensa, radio y televisión. El artículo 9 contempla el problema de la conciliación entre los derechos que reconocen los artículos 8 (base de la Directiva) y 10 (libertad de información) ambos del Convenio Europeo de Derechos Humanos de 1950. En consecuencia, los Estados miembros deberán prever las excepciones que el respeto a la libertad de expresión requiriere con relación a las disposiciones de los capítulos II, IV y VI de la Directiva. El precepto podría haber quedado así, con lo cual cada Estado habría dispuesto de un mayor margen de maniobra para estimar si existe o no conflicto entre ambos derechos. La introducción de una referencia a supuestos determinados en los cuales deba primar la libertad de expresión sobre la protección de datos introduce cierta confusión.

El precepto habla de "tratamientos de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria". Esta última fórmula fue introducida en el artículo 9 durante la Presidencia belga, no en su forma actual sino en la de "creación literaria o artística". El uso de la voz "creación" podría hacer pensar que la protección de datos habría de ceder ante la protección de las obras del ingenio integradas por una colección de datos de carácter personal, cualquiera que fuera su modalidad específica. Por ello, este artículo ha sido objeto de una declaración conjunta del Consejo y la Comisión, a incluir en el Acta del Consejo, en la que se precisa, en primer lugar que "la protección por el derecho de autor de las creaciones literarias o artísticas no interfiere con la presente Directiva" y, segundo, que tanto el derecho cuya protección instrumenta la Directiva como el derecho a la libertad de información están amparados por el Convenio Europeo de Derechos Humanos, mencionándose expresamente el artículo 10 con respecto a la libertad de información. En principio, parece conjurado el riesgo de "vaciar" de hecho la aplicación de la Directiva en aras de la protección de la

creación literaria o artística, aun cuando en su día existirá una protección a escala comunitaria de las bases de datos en cuanto obra del ingenio. A este respecto conviene tener en cuenta que la mayor parte de los ficheros de datos de carácter personal revestirán la forma de bases de datos.

La declaración prevista parece salir al paso de la conclusión antedicha. Habrá que entender, por tanto, que si en la preparación de las noticias o de reportajes, destinados a medios periodísticos, radiofónicos o televisivos, se utiliza un tratamiento de datos de carácter personal, valiéndose de sistemas de bases de datos o de tratamientos de textos, el redactor o el medio de comunicación en cuanto responsables del tratamiento no tendrán que ajustarse al sistema protector de la Directiva y, por tanto, no tendrán que informar a los titulares de datos del hecho de la recogida de sus datos cuando esta sea indirecta, ni de las cesiones de tales datos, como tampoco estarán obligados a dar acceso a los datos a los titulares de los mismos.

Del mismo modo, si en la preparación de una obra biográfica en todo o en parte se utilizan técnicas de procesos de textos, o si se hace acopio previo de datos sobre el biografiado o personas conexas, creando al efecto ficheros de datos personales, tampoco será preciso ajustarse a la Directiva y por tanto no será necesario informar a los interesados del hecho de la recogida, etc., por cuanto que estos tratamientos y ficheros tienen por finalidad la mera "expresión literaria o artística". La delegación de Suecia incluirá igualmente en el Acta del Consejo una declaración según la cual estos tratamientos privilegiados sólo se refieren a la expresión y no al contenido. A su vez, la Delegación francesa incluirá en el Acta otra declaración según la cual Francia hará uso de las excepciones autorizadas por este precepto en el campo del sector audiovisual. Esto significa que en Francia el uso de los tratamientos automatizados de datos personales vinculado a una finalidad de expresión audiovisual artística estará igualmente exento de las exigencias de la protección de los datos personales. A la vista de lo que antecede, existen dudas razonables para admitir que estas excepciones en aras de la protección de la expresión literaria o artística no interfieren realmente con la propiedad intelectual de las creaciones literarias o artísticas, sobre todo habida cuenta de que, por definición, la propiedad intelectual no protege ideas o contenidos sino la expresión. No será fácil precisar en una obra literaria o artística, escrita o audiovisual, hecha con datos de carácter personal, donde acaba la *expresión* y donde empieza el *contenido*. Este problema del conflicto potencial de la protección de datos y la propiedad intelectual no es una mera posibilidad conceptual, sino que se ha suscitado en la práctica en el Derecho español, en un contexto distinto, aunque dentro del marco de los derechos de la personalidad.

Existe jurisprudencia reciente, de Audiencias Provinciales y del Tribunal Supremo, de lo años 1990 a 1993, en la que se refleja este conflicto, principalmente en relación con el uso de imágenes y obras audiovisuales.

La Directiva no había previsto una regulación del derecho de acceso a los documentos conservados en archivos públicos (*open Government*). Algunas legislaciones, como la ley de Quebec de 1986 y la ley húngara de 1990, han incluido la regulación de la protección de datos y el acceso a los documentos administrativos en un mismo cuerpo legal. El "Considerando" 71º trata de tender un puente hacia una regulación armónica de ambas cuestiones, declarando que " *la Directiva permite tener en cuenta en la aplicación de las normas que instaura, el principio del derecho de acceso del público a los documentos administrativos* ".

Otra cuestión relacionada con el ámbito de aplicación es la de la modalidad de aplicación del sistema protector a los *datos sensibles*. El texto parece partir de dos posibles opciones: prohibir su uso y, por tanto excluir estos datos de la aplicación de la Directiva, o aceptar dicho uso con unas garantías adecuadas. La propuesta modificada adopta una solución intermedia. Como norma, prohibe el uso de estos datos en el artículo 8.1. La posición común ha mejorado el texto de la propuesta modificada. Subsiste la concepción básica del precepto, que proclama la obligación de los Esta - dos miembros de prohibir el tratamiento de estos datos, a saber, los que revelen el origen racial y étnico, la opinión política, las convicciones religiosas, filosóficas o morales, la afiliación sindical y las informaciones relacionadas con la salud y la vida sexual. Acto seguido, el precepto habilita a los Estados miembros a dejar sin efecto la prohibición en aras de intereses diversos. La concepción del precepto es menos afortunada que la del artículo 6 del Convenio del Consejo de Europa, según el cual estos datos "no podrán tratarse automáticamente, a menos que el Derecho interno prevea garantías apropiadas". Cabe entender que no se ha querido siempre condicionar la licitud del tratamiento a unas garantías específicas.

El texto del apartado 1 se ha mantenido en su redacción anterior. El Consejo y la Comisión, sin aceptar el criterio de cuatro delegaciones (Reino Unido, Alemania, Irlanda y Dinamarca), incluirán en el acta del Consejo una declaración según la cual los Estados miembros, al amparo del artículo 5 -que habilita a los Estados miembros a determinar las condiciones de licitud de los tratamientos-podrán precisar aquellos datos que, entre los enumerados en el artículo 8.1, deban considerarse sensibles, en función de "las características jurídicas y sociológicas del país, por ejemplo en lo que respecta a la identidad genética, a la afiliación política, a la condición física, a las convicciones o hábitos personales, etc. ". Este criterio repercutirá sustancialmente en la armonización intracomunitaria y, por tanto, en el nivel de protección a escala comunitaria.

El nuevo texto ha mejorado, en cambio, la concepción y alcance de las excepciones a esta norma prohibitiva. El texto de la propuesta modificada era impreciso, puesto que sólo preveía dos opciones: el consentimiento del interesado, prestado directamente o a través de una fundación o asociación sin ánimo de lucro cuya finalidad esté basada en el uso de datos sensibles, o la existencia de disposiciones legales o reglamentarias habilitantes basadas en motivos de orden público. El texto contenía una tercera opción, la de que el tratamiento se efectuara en condiciones tales que resultara manifiesto que no atentaba contra la intimidad o las libertades, lo que, en realidad, era una cláusula residual o una formulación genérica de la norma del artículo 8.1. La opción de la disposición habilitante no era suficiente, puesto que se corría el riesgo de una interpretación extensiva de la noción de "motivos importantes de orden público". Había que explicitar en qué consistían esos motivos capaces de dejar sin efecto una norma prohibitiva y además había que

definirlos con carácter limitativo, pues, de lo contrario, cada Estado podía legislar libremente sin sujeción a patrón o criterio alguno. En cambio, la previsión de una lista limitativa de supuestos de excepción permitía, a su vez, acotar el alcance de las respectivas excepciones. El texto de la posición común ha seguido un doble criterio: explicitación limitativa de supuestos y cláusula residual. Según el texto, el apartado 1, es decir, la prohibición de tratar datos sensibles, cualesquiera que éstos sean, no es aplicable en seis supuestos. En primer lugar, cuando el interesado haya dado su consentimiento, salvo disposición del Derecho interno que no permita que el solo consentimiento deje sin efecto la prohibición. Con ello, en realidad, el texto autoriza a los Estados miembros a prever esta posibilidad o a dejar a salvo disposiciones internas en tal sentido.

El segundo supuesto, incluido a propuesta de la delegación de Alemania, contempla la posibilidad de tratar en materia laboral datos sensibles que sean necesarios para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y esta prevea garantías adecuadas. El tercer supuesto, necesidad del tratamiento para la defensa de intereses vitales del interesado o de un tercero, recoge una de las causas que el artículo 9.2 del Convenio del Consejo de Europa incluye con carácter general como excepción a la aplicación del régimen protector. Habrá que entender que la prohibición de tratar datos sensibles no procederá cuando el tratamiento beneficie al interesado o a otros, en la medida en que les permita defender sus intereses vitales. Asimismo, la prohibición no será aplicable si el objeto del tratamiento lo constituyen datos que el interesado ha hecho públicos de manera manifiesta; igualmente, si el tratamiento es necesario para el reconocimiento, ejercicio o defensa en juicio de un derecho. Otra de las excepciones, en cuya inclusión jugó un papel importante la delegación francesa, apoyada por la española, entre otras, la constituyen los datos de salud. Es decir, no procede prohibir el tratamiento de los datos de carácter personal cuando el tratamiento es necesario para fines propios de la medicina preventiva, el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios sanitarios. La única condición que ha de cumplirse es la de que el tratamiento debe ser efectuado por un profesional de la sanidad sujeto al secreto profesional por disposición legal o en virtud de códigos deontológicos.

El apartado 4 contiene una cláusula residual que es poco afortunada, puesto que, en parte, desnaturaliza el criterio anterior, al habilitar a los Estados miembros a que prevean excepciones por motivos importantes de orden público, siguiendo para ello el cauce de una disposición legal o de una rsolución de la Autoridad de control y, por otra parte, equipara en este contexto la Autoridad de control y los órganos legislativos.

El ámbito de aplicación *ratione loci* queda definido por el artículo 4. Este precepto se hace cargo del problema del Derecho aplicable a los tratamientos de datos cuando un tratamiento tuviere lugar en más de un Estado miembro o en un Estado distinto de aquél en que residiere el responsable del tratamiento. Esta es una cuestión que sólo las legislaciones de Bélgica y los Países Bajos habían tenido en cuenta. La propuesta modificada de 1992 se basaba en el Estado en que el responsable del tratamiento estuviera establecido, como criterio de determinación del Derecho aplicable. Este criterio suscitó una cierta resistencia, principalmente por parte de las Autoridades de protección de datos, que celebraron contactos diversos, entre sí y con la Comisión, con el fin de sustituirlo por otro u otros criterios más adecuados, o incluso suprimir el precepto y promover un Convenio intracomunitario al amparo del artículo 220 del Tratado. El criterio del Estado de establecimiento no parecía satisfactorio, debido a que, precisamente en un contexto de mercado interior y de libre circulación de personas, productos, capitales y servicios, un tratamiento de datos puede tener lugar en más de un Estado, de tal manera que parte de las operaciones se efectúe en un Estado y parte en otro, como es el caso, por ejemplo, de una prestación social causada en un Estado por un súbdito de otro. Cabe asimismo que parte de las operaciones tenga lugar en un tercer Estado, exterior a la Unión. La flexibilización del sistema protector, que se observa en el texto de la posición común, abre la vía a discrepancias importantes entre las legislaciones internas, precisamente en cuanto al nivel de la protección, en la medida en que el texto reconoce a los Estados opciones diversas de regulación.

Es posible, por ello, que en un Estado el nivel sea más alto que en otro, lo cual puede dar lugar a evasiones de las legislaciones más restrictivas, incluso en el ámbito jurisdiccional, dando pie a prácticas de *forum shopping* en casos de litigios derivados de la aplicación del sistema protector. El nuevo texto ha optado por un criterio mixto: se aplicará a los tratamientos el Derecho del Estado en el que estuviere establecido el responsable y en el cual tuviere lugar el tratamiento. Si el responsable del tratamiento estuviera establecido en varios Estados, el responsable deberá ajustarse para cada fase del tratamiento al Derecho interno de cada uno de los Estados. Este nuevo criterio se completa con la posibilidad de que las Autoridades de control ejerzan sus potestades a instancia de Autoridades de control de otros Estados miembros, con el fin de evitar evasiones de la legislación de transposición.

Dentro de este aspecto, del ámbito de aplicación *ratione loci*, cabe incluir algunas modulaciones aportadas por el nuevo texto a la regulación de las transferencias de datos a terceros estados carentes de una legislación de un nivel de protección adecuado. A las excepciones que el primitivo artículo 26 preveía se han agregado otras. Son los casos en los que la transferencia sea necesaria para celebrar o cumplir un contrato o se haga a partir de un registro público que, por disposición legal o reglamentaria, estuviere destinado a informar al público y estuviere abierto a la consulta pública o de personas que acreditaren un interés legítimo. El "Considerando" 58º precisa que en tales supuestos la transferencia no podrá ser de la totalidad del fichero, ni hacerse sin el consentimiento del interesado. El nuevo artículo 26 introduce otra excepción, inspirada en prácticas de algunos *länder* alemanes y en recomendaciones del Consejo de Europa, según la cual, sea cual fuere el nivel de protección del Estado tercero, podrán autorizarse las transferencias de datos si existen garantías apropiadas, en especial si las mismas se derivan de cláusulas contractuales pactadas al efecto entre el transferente y el destinatario de los datos.

Además del ámbito de aplicación, condicionan el nivel de protección otras variables: el papel que juega el *consentimiento del interesado* en cuanto al tratamiento, y el margen que se reconoce al ejercicio de los derechos del interesado sobre sus datos. Son los instrumentos que permiten al interesado ejercer un control, mayor o menor, sobre sus datos. A

diferencia de la propuesta primitiva de 1990, el consentimiento sólo aparece en los artículos 7 y 8, como una de las posibles opciones que condicionan la licitud del tratamiento de los datos, y en el artículo 26, como un supuesto de excepción a la norma de la prohibición de transferir datos a terceros Estados carentes de nivel adecuado de protección. En el nuevo texto, el centro de gravedad del sistema protector se desplaza a *las condiciones de licitud* del tratamiento, cuya determinación atribuye el artículo 5 a los Estados miembros. Este precepto deja a los Estados miembros un cierto margen en cuanto a la determinación de las condiciones de licitud de los tratamientos, sin más referente que el respeto a los principios proclamados en el artículo 6, coincidentes con los del Convenio 108 del Consejo de Europa, y las opciones del artículo 7. Para determinar si un tratamiento o no es lícito, las legislaciones nacionales deberán, por tanto, exigir imperativamente la observancia de los principios del artículo 6 y, además, optar por una de las alternativas del artículo 7. Por consiguiente, un Estado podrá decidir que unicamente sea lícito un tratamiento si, además de observar dichos principios, el responsable ha recabado previamente el consentimiento del interesado con relación al tratamiento, según este se define en el artículo 2 b).

O puede optar por cualquiera otra de las alternativas previstas en el precepto: necesidad del tratamiento para cumplir un contrato o una obligación jurídica del responsable, necesidad del tratamiento para proteger el interés vital del interesado, para cumplir una misión de interés público inherente al ejercicio del poder público y conferida al responsable, o por último para satisfacer el interés legítimo del responsable o de terceros cesionarios de los datos. La exigencia del consentimiento previo no es, pues, una norma general, susceptible de excepciones, sino una opción de licitud, análoga a la celebración de un contrato, los contactos precontractuales, la existencia de una obligación legal, etc. Esta norma dará lugar a importantes diferencias entre los Estados miembros. Sólo las leyes de Alemania y los Países Bajos contienen disposiciones condicionantes de la licitud de los tratamientos, en tanto que las legislaciones de Bélgica, Francia, Irlanda o Luxemburgo se basan en una presunción de licitud de los tratamientos, de tal manera que la notificación o inscripción subsiguiente en el registro de ficheros es un mero acto certificante de la existencia de un fichero o tratamiento y de todo aquello que se requiere para que el interesado pueda ejercer sus derechos sobre los datos. La licitud se determina *a posteriori*, por vía de inspecciones o reclamaciones. La ley alemana (§ 4) dispone que sólo será lícito elaborar y usar datos personales si lo autoriza la propia ley o una disposición legal o reglamentaria o si el interesado ha dado su consentimiento. Según la ley holandesa (artículo 4) sólo puede crearse un fichero si lo es para un fin concreto vinculado a los intereses del titular y siempre que el fin no sea contrario a la ley, el orden público o las buenas costumbres. El nuevo texto ha introducido como norma obligatoria el control previo de licitud en el artículo 20.

La Autoridad de control procederá a determinar, una vez notificado el tratamiento, si el mismo lleva consigo riesgos específicos para los derechos y libertades de las personas. Los "Considerandos" 52º, 53º y 54º matizan el alcance de este control, precisando lo que debe entenderse por tales "riesgos específicos". El "Considerando" 52º estima que normalmente será suficiente el control *a posteriori*, pero que ciertos tratamientos, como aquellos que tuvieren por objeto excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato o utilizaren una tecnología nueva debe entenderse que ofrecen tales riesgos específicos. El artículo 28 completa esta regulación, atribuyendo a la Autoridad de control la potestad de conocer de reclamaciones en casos de duda sobre la licitud de un tratamiento.

En el otro aspecto, el referente al margen de ejercicio de los derechos del interesado, la posición común ha relajado el control del interesado sobre sus datos, en la medida en que permite que los Estados establezcan excepciones importantes. Ya el Convenio 108 del Consejo de Europa preveía en su artículo 9 la posibilidad de excepciones al sistema protector, pero dentro del marco del Convenio de Derechos Humanos. Es decir, cabe admitir excepciones, siempre que la excepción en concreto constituya una medida que, en una sociedad democrática, sea necesaria para proteger unos bienes jurídicos determinados. El precepto enumera como tales bienes, la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado, las exigencias de la represión de los delitos, y la protección del propio interesado o de los derechos y libertades de otros. La Directiva ha perfilado los derechos del interesado, mejorando en tal sentido los artículos 5 a 8 del Convenio citado. Estos derechos son los siguientes: a) derecho a ser informado del tratamiento de los datos con ocasión de la recogida (artículos 10 y 11 de la posición común); b) derecho de acceso, rectificación y cancelación (artículo 12); c) derecho de oposición al tratamiento (artículos 14 y 15); d) derecho a la seguridad física y lógica del tratamiento (artículo 17); e) derecho de indemnización por daños o perjuicios causados por incumplimiento de la Directiva (artículo 23); y f) derecho de recurso jurisdiccional frente a las decisiones del responsable (artículo 22). Cabría añadir que la notificación y el registro de los tratamientos es un instrumento condicionante del ejercicio de los derechos de acceso, rectificación y cancelación. El artículo 13 enumera unas excepciones que hacen referencia a los distintos derechos, con alcance diverso en cada caso. Los Estados pueden limitar "las obligaciones y derechos" previstos en varios preceptos.

Según esto, los Estados pueden limitar la observancia de los principios de la protección de los datos (artículo 6.1), en aras de las salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención y represión de los delitos, un interés económico y financiero importante del Estado miembro o de la Unión, una función de control, inspección o reglamentación relacionada con la seguridad pública, la prevención y represión de los delitos y el interés económico y financiero del Estado o de la Unión y, por último, la protección del interesado o de los derechos y libertades de otro. Asimismo, en aras de la misma finalidad pueden limitarse el derecho del interesado a ser informado del tratamiento (artículos 10 y 11.1) y el derecho de acceso, rectificación, bloqueo y cancelación (artículo 12), sin perjuicio de otras excepciones que se prevén para tratamientos vinculados a finalidades históricas o de investigación. El texto de la posición común ha añadido otra causa habilitante para estas excepciones en el artículo 13.1 d), según el cual los Estados podrán asimismo limitar las citadas obligaciones y derechos cuando sea necesario para salvaguardar, no sólo las necesidades de la prevención y represión de los delitos, sino asimismo de las *infracciones de la ética en las profesiones reglamentadas.* El "Considerando" 43º no explica la razón de esta adición, limitándose a incluir una referencia a las violaciones de las normas deontológicas de las profesiones reguladas. Los demás derechos que reconoce la Directiva, tales como el derecho de oposición (artículos 14 y 15), el derecho a la seguridad de los datos (artículo 17) y los derechos de recurso jurisdiccional (artículo 22) y de indemnización (artículo 23) no podrán sin embargo ser objeto

de limitación.

La propuesta modificada introdujo un cambio importante en la regulación prevista para la notificación de los tratamientos. Los artículos 7 y 11 de la propuesta primitiva imponían la obligación de notificar los ficheros del sector público y los del sector privado, estos últimos sólo cuando los datos se destinaran a ser cedidos y no procedieran de fuentes accesibles al público. La propuesta modificada, además de unificar la regulación, desechando en éste y otros aspectos la distinción entre sector público y sector privado, ha previsto en el artículo 18 la posibilidad de eximir de la notificación a determinados tratamientos o de simplificar la notificación. El texto de la posición común mantiene esta opción en el artículo 18. La norma (artículo 18.1) es la notificación obligatoria. La posición común no ha querido, sin embargo, implantar con todo rigor esta norma, habida cuenta de que varias legislaciones (Países Bajos, Irlanda, Dinamarca) admiten una notificación selectiva, en razón de criterios diversos (ficheros ya conocidos del interesado sin necesidad de consultar un registro de ficheros, ficheros de datos sensibles, etc.), otras legislaciones (Francia) prevén la posibilidad de notificaciones simplificadas, y por último, la ley federal alemana sólo prevé la notificación de los titulares de los ficheros privados (§ 37). Por último, algunas legislaciones prevén la inscripción constitutiva, no de los ficheros, sino de los usuarios de datos (Reino Unido) o una autorización administrativa en lugar de la notificación (Suecia, Luxemburgo). La posición común ha relajado, por ello, considerablemente la norma de la notificación obligatoria, en un esfuerzo por dar cabida en el sistema protector a todas las opciones nacionales ya existentes. El nuevo texto permite a los Estados prever supuestos de exención o simplificación. El artículo 18 enumera tres supuestos.

En primer lugar, que en razón de los datos a tratar, no fuere previsible que el tratamiento atentara contra los derechos o libertades del interesado.

El "Considerando" 53º ofrece un criterio a título de ejemplo, para determinar si un tratamiento atenta contra los derechos o libertades: son los tratamientos cuyo alcance o finalidad sea excluir a los interesados "del beneficio de un derecho, de una prestación o de un contrato". En otros términos: los tratamientos de datos limitativos de derechos. El segundo supuesto está inspirado en la ley alemana de 1990, que instaura la figura del comisionado o delegado privado de protección de datos para empresas de más de cinco empleados permanentes o de veinte si sólo utilizan tratamientos no automatizados. El artículo 18.2, supuesto segundo, de la Directiva permite eximir de la obligación de notificar si el responsable del fichero (empresa o persona jurídica) ha designado a un empleado para que ejerza esta función en la organización. En tal caso, no será precisa la notificación, ya que el comisionado privado dispone de la información necesaria acerca de los tratamientos que se utilizan en la organización. El tercero se refiere a tratamientos cuya única finalidad sea la de llevar registros que, con arreglo al Derecho nacional estén destinados a facilitar información al público en general, lo que coincide fundamentalmente con nuestro artículo 2.2. a). El texto de la posición común define una compleja organización de control de la aplicación de la Directiva, que combina un dispositivo de audiencia de las Autoridades nacionales de control y la atribución a la Comisión Europea de determinadas potestades. En cuanto a la atribución y ejercicio de dichas potestades, el texto no crea una estructura específica, sino que elige una de las opciones previstas al efecto en la Decisión 87/373/CEE, de 13 de julio de 1987. No se trata, pues, de una estructura creada expresamente para la aplicación de esta Directiva, sino de la elección de una de las opciones definidas por la citada Decisión con carácter general para los supuestos de atribución a la Comisión de competencias de ejecución.

Las Autoridades de control se reunen en el Grupo de Protección de Datos -réplica a escala comunitaria de la "Conferencia de Comisarios"-, cuya función es asesorar a la Comisión sobre cualesquiera proyectos de modificación de la Directiva u otras medidas que incidan en los derechos y libertades, dictaminar sobre los códigos de conducta comunitarios, examinar toda cuestión suscitada por las disposiciones nacionales de transposición con miras a contribuir a su aplicación homogénea, y emitir dictamen para la Comisión sobre el nivel de protección existente en la Unión. El texto atribuye a la Comisión unas potestades, dentro de la opción III, variante b), de la Decisión. La Comisión estará asesorada por un Comité compuesto de representantes de los Estados miembros y de la Comisión. Los Estados tienen, pues, una doble representación: en el Grupo de Protección de Datos (delegados de las Autoridades de control) y en el Comité Consultivo (representantes designados por los Estados miembros). La Comisión es el órgano destinatario de las actuaciones del Grupo, tiene competencias propias y controla el Comité a través de su presidente.

El nuevo artículo 28 exige que la Autoridad de control ejerza sus funciones "con toda independencia". El nuevo texto ha modificado el apartado 1 del artículo 30 de la propuesta modificada, que, al igual que el 26 de la primitiva propuesta, imponía a los Estados miembros la obligación de designar a una "Autoridad independiente". El "Considerando" 62º mantiene esta expresión, que, sin duda, es equívoca, puesto que no está claro si define un órgano u organismo simplemente especializado o "separado", o un ente no inserto en la estructura de la Administración, con presupuesto separado y exento de instrucciones de todo órgano, constitucional o administrativo. Tampoco se ofrece criterio alguno sobre si la independencia está o no vinculada a la forma de elección o designación del titular o los componentes de la Autoridad de control. La situación actual se caracteriza por su gran diversidad en todos esos aspectos. No existe un "modelo" que, por abstracción integrara a todas las manifestaciones concretas y al cual se ajusten por exceso o por defecto las Autoridades existentes. El texto se ha inclinado por una noción de independencia referida a la no sujeción a instrucciones, siguiendo la opción de la Comisión francesa o austríaca o de la Agencia española. Esto no implica necesariamente una determinada modalidad de elección o designación (Parlamento, Gobierno), ni una financiación autónoma, ni tampoco una exterioridad a la estructura del Ejecutivo.

En cuanto a las funciones de las Autoridades de control, el texto de la posición común ha agregado a las funciones de la propuesta modificada la de la obligatoriedad de consultarlas con ocasión de la elaboración de medidas reglamentarias o administrativas en materia de protección de datos (artículo 28.2). Asimismo, y con el fin de articular la nueva concepción del artículo 4, sobre el Derecho aplicable, se ha añadido en el artículo 28.6 una función de cooperación forzosa, en la medida en que cada Autoridad de control puede ser requerida a ejercer sus funciones a instancia de una Autoridad de otro Estado miembro. Con ello se recoge, en realidad, la norma del artículo 13 del Convenio 108 del

Consejo de Europa, que prevé una cooperación entre los Estados parte en términos análogos. Por lo demás, las funciones de la Autoridad de control no han variado, en la medida en que subsisten las potestades primitivas de policía administrativa (potestad de intervención), que se concreta en una autorización administrativa para los supuestos de tratamientos previstos en el artículo 20 (tratamientos capaces de atentar contra los derechos y libertades) y en una potestad de ordenar la cesación de tratamientos el bloqueo o supresión de datos, así como de dirigir amonestaciones y apercibimientos a los responsables. Dentro de esta función se encuadra la de acudir al Parlamento o "a otras instituciones políticas". Asimismo subsisten la capacidad de ejercer la acción pública en los supuestos de infracción de las disposiciones de transposición, y la potestad de resolver recursos y reclamaciones, entre ellas las referentes a la licitud de un tratamiento. A todas estas funciones, el artículo 18.5 ha añadido la posibilidad de dictar normas de exención o simplificación de la notificación de los tratamientos.

De lo que antecede puede deducirse que, pese al objetivo armonizador de la Directiva, la regulación de la protección de datos ofrecerá necesariamente divergencias sustanciales entre los distintos Estados miembros. Varios artículos dejan a los Estados miembros opciones varias para la transposición, en la medida en que les permiten elegir una regulación u otra. Estas opciones abren la vía a disparidades del Derecho sustantivo. La propia Directiva admite la posibilidad de diferencias importantes en el Derecho sustantivo. El artículo 30.2 admite esta posibilidad y confiere al Grupo de Protección de Datos la función de informar a la Comisión cuando observe divergencias graves entre las legislaciones o la práctica de los Estados miembros en materia de protección de datos personales. Estas divergencias pueden determinar que un Estado dado tenga un régimen más favorable que otro desde el punto de vista del titular de los datos.

Cabría apreciar una influencia indirecta de la negociación de la Directiva en algunas modificaciones legislativas nacionales. Esta puede ser la explicación de la reforma de la ley austríaca de 1978 de protección de datos. La ley de 1978 ha sido modificada en los años 1981, 1982, 1986, 1987, 1988, 1989 y 1993. Las últimas modificaciones hacen referencia a las funciones de la Autoridad de control, la Comisión de Protección de Datos (§§ 14, 36, 37, 50) y tiene por objeto reforzar su competencia. Las modificaciones entrarán en vigor en el año 1995. En el texto anterior, la Comisión tenía una función jurisdiccional subsidiaria, en la medida en que si había ya en curso de instrucción un procedimiento de reclamación por razón de los derechos de acceso, rectificación o cancelación, ante otra Autoridad, competente por razón de la materia, la Comisión quedaba vinculada por la resolución que dicha Autoridad dictare. Según el nuevo texto del § 14, la situación se invierte y la otra Autoridad deberá suspender la instrucción del procedimiento hasta tanto la Comisión hubiere resuelto la reclamación. En el supuesto de que, por razón de posible demora, el reclamante pudiere sufrir perjuicio, la Comisión podrá incluso suspender las cesiones de datos o parte del tratamiento. Estas funciones de control se amplían aún más en el nuevo § 36, que tiene rango de disposición constitucional. El nuevo § 37 sólo admite contra las resoluciones de la Comisión el recurso ante el Tribunal Supremo Contencioso-Administrativo.

LOS PROBLEMAS PENDIENTES

Al margen de la conveniencia de una armonización de la protección de datos en el seno de la Unión, la propuesta de Directiva es importante, sobre todo, porque, tanto en el curso de la negociación, como en el texto de la posición común, incluidos los "considerandos", han ido aflorando los problemas básicos de la protección de datos, de tal manera que la Directiva ha venido a ser un "punto de encuentro" de las actitudes y tendencias actuales. La Directiva no resuelve, sin embargo, todos los problemas, ni los que resuelve ofrecen una regulación suficientemente pormenorizada. Por ello, ofrece interés examinar las innovaciones que en el transcurso del año 1994 se han ido produciendo con relación a problemas específicos sobre los cuales existía ya una reflexión a escala europea y mundial desde hacía varios años. Desde mediados de los años ochenta, la especulación doctrinal y la actividad normativa dentro del contexto de la protección de datos habían ido reflejando la preocupación de los medios competentes por tres órdenes de problemas: a) el uso de los datos generados por la utilización de los servicios de telecomunicación, b) el uso de los datos de salud, comprendidos los datos genéticos, c) la incidencia del uso de sistemas de vigilancia magnetoscópica en lugares públicos. Estos trabajos han fructificado en propuestas de actos multilaterales a escala internacional o comunitaria que, en el transcurso del año 1994 han sido objeto de decisiones importantes. Asimismo, algunas reformas legislativas se han hecho eco de estos trabajos.

Los trabajos sobre la problemática de la protección de los datos personales utilizados y generados en el marco de los servicios de *telecomunicación* se remontan a los últimos años de la década de los años ochenta. Tres organizaciones comenzaron casi simultáneamente a estudiar estos problemas: la Conferencia de Autoridades de Protección de Datos, el Consejo de Europa y la Comisión Europea. Fue en la 11ª Conferencia de las Autoridades de Protección de Datos, celebrada en Berlín en 1989, cuando por primera vez se acometieron estos problemas. Los trabajos han ido cristalizando en resoluciones de la Conferencia, que fueron aprobadas en la 12ª Conferencia (París, 1990), en el proyecto de Recomendación del Consejo de Europa y en la propuesta de Directiva SYN 288. Dentro del año 1994 ha habido innovaciones importantes en relación con estas dos últimas iniciativas. La problemática analizada hace referencia a la necesidad de modular, en su caso, los principios de la protección de datos generalmente aceptados, en función del contexto de los servicios de telecomunicación, en primer lugar en relación con las clases de datos utilizados: datos de base (datos del abonado a los servicios, sin los cuales el servicio no puede ser prestado ni satisfecha la contraprestación por su uso, a saber, nombre y dirección del abonado), datos de tráfico (generados por el uso, o sea, datos del llamante y del llamado, servicios concretos utilizados, tiempo de la utilización), y datos de contenido (contenido de los mensajes, cualquiera que sea el servicio en concreto). De otra parte, cada modalidad de servicio (retrollamada, identificación de la línea, localización de llamadas maliciosas, etc.) requiere modulaciones específicas de los principios. Asimismo, la noción de responsable del fichero había de ser sustituida por la de responsable de la red, operador de la red, prestador de servicios, etc. Los distintos textos en proyecto se han hecho cargo de esta problemática en forma distinta.

El Comité de Expertos (Grupo de Proyecto) de Protección de Datos del Consejo de Europa, en su 28ª reunión plenaria (11-14 de octubre) y el Comité Europeo de Cooperación Jurídica, asimismo del Consejo de Europa, en su 62ª reunión (5-8 de diciembre) aprobaron, para su remisión al Comité de Ministros, el texto del proyecto de Recomendación que venía siendo elaborado desde 1989. Un primer texto había sido ya aprobado por el Comité Europeo de Cooperación Jurídica en la reunión de 22-25 de junio de 1992. Sin embargo, en dicha reunión algunas delegaciones consideraron conveniente que el texto fuera sometido al Comité Director de los Derechos Humanos, por conducto del Comité de Ministros, no obstante lo cual el texto fue aprobado en la reunión citada por 23 votos a favor, ninguno en contra, y las abstenciones de Francia, Luxemburgo y Liechtenstein. Sometido el texto al Comité Director de los Derechos Humanos, en la reunión de 22-26 de noviembre, el Comité emitió dictamen, en el que, aceptando la conveniencia de la iniciativa, entre otras razones por estimar que el texto regulaba problemas no cubiertos por la jurisprudencia del Tribunal Europeo de los Derechos Humanos, hizo algunas sugerencias tendentes a ajustar el texto al Convenio Europeo de los Derechos Humanos de 1950, en especial al artículo 8. El Comité se mostró más restrictivo que el texto en cuanto a la posible cesión de los datos de contenido, aun de los obtenidos previa autorización de los órganos jurisdiccionales u otros competentes, así como en cuanto a las excepciones que la propia Recomendación prevé con respecto a sus principios, exigiendo que las mismas fueran objeto de formulación precisa y restrictiva.

El Comité eludía expresamente todo pronunciamiento en abstracto sobre la conformidad de los principios de la Recomendación con relación al artículo 8 del C.E.D.H., estimando que tal conformidad es función "de la formulación, la interpretación y la aplicación de las disposiciones del Derecho interno en el ámbito abarcado por la Recomendación". El Grupo de Proyecto de Protección de Datos, en su reunión plenaria de 11-14 de octubre, acordó elevar un nuevo texto, modificado según las observaciones del Comité Director de los Derechos Humanos, al Comité Europeo de Cooperación Jurídica, el cual, a su vez, en la sesión 62ª (5-8 de diciembre) acordó elevarlo al Comité de Ministros para su aprobación definitiva. El Grupo de Proyecto estimó que el texto era válido y que los escasos puntos de discrepancia no justificaban una continuación de las negociaciones, habida cuenta de que otras innovaciones tecnológicas ("autopistas de la información", etc.), cuya incidencia no es, por el momento, claramente definible requerirán otras actuaciones.

La propuesta de Directiva SYN 288 fue incluida originariamente en el "paquete" de actos comunitarios de 1990, juntamente con la "Directiva marco" (SYN 287) y otros actos comunitarios relacionados con la protección y seguridad de los datos personales. A diferencia de la Recomendación del Consejo de Europa o de las resoluciones de la Conferencia de Autoridades de Protección de Datos, el propósito de esta Directiva no es tanto la protección de los datos en el contexto específico de las redes digitales públicas de servicios integrados y de las redes, asimismo públicas, de telefonía móvil, sino facilitar la implantación de los nuevos servicios, indispensables dentro del mercado único. La exposición de motivos de la propuesta de 1990 (página 10) decía expresamente que "la protección efectiva a escala comunitaria de los datos de carácter personal y de la vida privada viene a ser una condición previa esencial para la aceptación social de las nuevas redes y servicios digitales". Iniciada la negociación en febrero de 1991, sólo se celebró una sesión del Grupo negociador del Consejo. El Parlamento Europeo dictaminó la propuesta en 1992, y no ha habido nuevo texto hasta abril de 1994. El texto ha sido objeto de cambios importantes, debidos principalmente a la incidencia del principio de subsidiaridad del Tratado de la Unión Europea (artículo 3B, párrafo segundo). El nuevo texto fue presentado por la Comisión al Consejo el 13 de junio de 1994 (documento COM (94) 128 final-COD 288).

Hasta ahora sólo ha habido un pronunciamiento sobre la nueva propuesta, que ha sido acordado por las Autoridades de Protección de Datos, en reunión celebrada en Berlín el 23 de diciembre. En dicha reunión se convino en una posición común, que se encuadra en un marco de actuación acordado en la Conferencia celebrada en Madrid los días 25 y 26 de mayo, en un documento que subrayaba la necesidad de que en los actos comunitarios relativos a los servicios de telecomunicación y redes transeuropeas se incluyeran disposiciones específicas sobre protección de datos. La Conferencia estimó que el nuevo texto constituye un paso importante en la dirección propugnada.

Dentro del marco acordado en la Conferencia de Madrid se encuadra asimismo el documento elaborado por las Autoridades de Protección de Datos sobre el Libro Verde de la Comisión sobre las comunicaciones móviles y personales (COM (94) 145 final). El documento fue acordado en la reunión celebrada por el grupo de trabajo ad hoc de la Conferencia de Autoridades de Protección de Datos reunido en Berlín el 5 de agosto, siendo remitido a la D.G. XIII de la Comisión el 9 de agosto. El documento formula algunas observaciones de carácter general e insta a la Comisión a que requiera en fase temprana el parecer de estas Autoridades sobre cualesquiera propuestas que se derivaren del Libro Verde. Igualmente, la Conferencia se ha pronunciado en reunión celebrada el 7 de noviembre, sobre el informe de la Comisión acerca de la Directiva 90/387/CEE o Directiva marco de Oferta de Red Abierta (ONP)en especial sobre la aplicación de esta Directiva marco a la propuesta de Directiva sobre Telefonía Vocal (COM (93) 182 final SYN 437), subrayando algunas deficiencias de las disposiciones de protección de datos.

Aun cuando la propuesta de Directiva COD 288 y la Recomendación del Consejo de Europa no han sido todavía aprobados, los trabajos preparatorios han ejercido una influencia indirecta que se refleja, por ejemplo, en la ley austríaca de Telecomunicaciones (*Fernmeldegesetz*), aprobada el 28 de diciembre de 1993 y que entró en vigor el 1 de abril de 1994. La ley dedica ocho parágrafos (28 a 35, que forman la Sección V) a la protección de los datos utilizados en los servicios de telecomunicación. La Sección V sigue la sistemática de los cuatro Reglamentos que en 1991 fueron siendo aprobados en Alemania en desarrollo de la ley federal de Protección de Datos de 1990: prestaciones de servicios de TELEKOM (TDSV, de 24 de junio), gestión de empresas privadas prestadoras de servicios de telecomunicación (UDSV, de 18 de diciembre), protección de datos en las actividades del POSTBANK (PB-DSV, de 24 de junio) y protección de datos en las prestaciones de servicios del POSTDIENST (PD-DSV, de 24 de junio). La Sección V se estructura en función de las clases de datos que se usan o generan con la utilización de estos servicios, así como de las modalidades de los servicios prestados. La ley austríaca concuerda con la Recomendación del Consejo de Europa en sustancia.

Otro de los problemas pendientes lo constituye la regulación del uso de los datos de salud. Ya las primeras leyes de Suecia, Noruega y Dinamarca habían tratado este problema. Las leyes más recientes, como la ley de Luxemburgo de 1992, de Reforma de la de 1979, y la ley belga de 1992, contienen disposiciones específicas sobre estos datos. El problema ha sido objeto de atención incluso desde antes de la apertura a la firma del Convenio 108 del Consejo de Europa. En 1981 el Comité de Ministros aprobó la Recomendación R (81) 1, de 23 de enero, sobre los bancos de datos médicos. Esta Recomendación se limitaba al uso de los datos automatizados generados o aportados en el marco de la relación entre médico y enfermo. Con el tiempo se ha puesto de manifiesto la insuficiencia de este punto de vista, por lo cual en octubre de 1989 el Comité de Expertos de Protección de Datos del Consejo de Europa decidió revisar dicha Recomendación. A tal efecto creó un grupo de trabajo, al cual confirió dicho mandato, que fue ampliado más adelante en el sentido de que los trabajos del grupo comprendieran asimismo la investigación médica y genética, así como los problemas que suscita el uso de los datos relativos a enfermedades incurables. El grupo de trabajo celebró un total de 7 sesiones, fruto de las cuales fue un borrador que se espera que sea sometido al Comité de Ministros en los primeros meses de 1995, habiendo sido informado favorablemente a lo largo del año 1994 por el Comité de Expertos y por el Comité de Bioética. El borrador de la Recomendación constituye, al igual que las demás Recomendaciones elaboradas dentro del marco del Convenio 108, una modulación de los principios de este con relación al contexto específico a los datos médicos o de salud.

La primera cuestión que suscita este contexto es lo que deba entenderse por "datos médicos" o "datos de salud", habida cuenta de que el objeto de la recomendación no son los datos de salud generados en el marco de la relación médico-enfermo, sino los datos de salud "donde quiera que se utilicen" es decir, en el sector de los seguros, de la medicina de empresa, empleo, escolaridad, e incluso identificación de las personas. La Recomendación considera datos médicos todos aquellos que guardan una relación "manifiesta y estrecha" con la salud de una persona. Por consiguiente son datos médicos los datos sobre el comportamiento de una persona, su vida sexual, su estilo de vida, consumo de drogas, abuso del alcohol o del tabaco, etc. Los datos comprenden los relativos a la salud presente y pasada, por lo cual son datos médicos los que resultan de tomas de sustancias de origen humano, de las implantaciones y trasplantes de tejidos u órganos. Igualmente son datos médicos los datos *genéticos* resultantes de la observación del fenotipo, tales como las características hereditarias o determinadas genéticamente, los antecedentes familiares, análisis de laboratorio o los datos obtenidos con el uso de la tecnología del ADN. No son datos genéticos, en cambio, los referentes a la sangre, los tejidos, el cabello, el esperma, aun cuando de ellos puedan obtenerse datos genéticos. Sólo son datos genéticos los datos familiares, en la medida en que conste que una enfermedad o una característica de un individuo esté determinada o influida por lo genes, o si una enfermedad aparece en la familia de tal manera que se la pueda considerar hereditaria (línea genética). Quedan fuera del concepto los datos administrativos generados como consecuencia de la asistencia médica.

En términos generales, la Recomendación contiene una modulación de los principios de la protección de datos con el fin de precisar el *plus* que en cuanto a garantías jurídicas exige el artículo 6 del Convenio como condición para que estos datos puedan ser tratados automaticamente. Un primer aspecto lo constituye el acotamiento del colectivo de personas que pueden recoger o tratar datos de salud. El principio 3.2 limita estas operaciones a los profesionales de la medicina y al personal paramédico que esté sujeto a obligaciones de secreto profesional. Dentro de este mismo espíritu de reforzamiento de las garantías, la Recomendación sólo admite una recogida directa de los datos, admitiendo sólo con carácter excepcional una recogida indirecta, cuando así lo exija la finalidad del tratamiento o si el interesado no puede facilitar los datos. En todo caso, es preciso un título habilitante para la recogida y tratamiento, que el principio 4.3 precisa: existencia de una obligación legal, fundada en la salvaguardia de los intereses vitales del interesado o de un tercero, la protección o promoción de la salud pública o habilitación legal a efectos de medicina preventiva o de diagnóstico o asistencia del interesado o de un pariente incluido en su misma línea genética. En defecto del título habilitante, cabe la recogida indirecta si el interesado o su representante legal caso de los *nasciturі* presta su consentimiento al efecto o personas incapaces. El principio 4.3 admite la recogida indirecta cuando se trata de prevenir un peligro concreto o de perseguir una infracción penal. Esta norma concuerda con uno de los principios de la Recomendación R (87) 15 sobre uso de datos a fines policiales, si bien hay que admitir que los supuestos de peligro concreto como título habilitante deberán ser distintos. La Recomendación contiene asimismo algunas modulaciones en cuanto al derecho de acceso a los datos de salud.

En primer lugar, consagra el principio del acceso por conducto de un médico, cuando así lo prefiera el interesado (principio 8.1, recogido en algunas legislaciones). Asimismo el texto prevé la posibilidad de negar el acceso cuando la información revele datos de terceros o, si se trata de datos genéticos, la información pudiere causar un daño grave a parientes consanguíneos o uterinos o a personas que tuvieren un vínculo directo con la línea genética. Por último, el principio 8.4 prevé la posibilidad de negar el acceso a datos resultantes de un análisis genético si dichos datos implican el descubrimiento de hechos o situaciones inesperados (parentesco desconocido, ausencia del parentesco familiar presunto). Puede admitirse que esta información excede de los fines del análisis genético y su registro sería contrario al principio de pertinencia de los datos. Sólo excepcionalmente, en casos de peligro para la vida del interesado o si la información inesperada reviste una importancia terapéutica o preventiva directa podía darse acceso a esta información.

Al margen de la asistencia médica, privada o pública, el uso de datos de salud ofrece una vertiente más compleja constituida por la investigación médica y epidemiológica. Con estos estudios no se pretende sólo mejorar el conocimiento de las patologías o de conocer otras hasta ahora desconocidas, sino que a partir de ellos es posible estimar determinados riesgos, definir políticas sanitarias, en especial preventivas, y planificar los sistemas de salud pública y evaluar sus costes. Por esta razón, el borrador de Recomendación dedica una atención especial a la atención médica. Los principios 12.1 a 12.5 contienen un cuadro normativo general, basado en la obligación de despersonalizar los datos utilizados en un proyecto de investigación, la información del interesado y la obtención de su conocimiento, y la publicación de los resultados de tal suerte que los interesados no puedan ser identificados. El principio 12.4 invita a los

Estados miembros a regular, dentro de lo posible, los problemas éticos y científicos que pudiere suscitar la investigación médica realizada a partir de datos de carácter personal.

Estos trabajos en torno a la problemática de los datos de salud han tenido asimismo un reflejo en reformas legislativas concretas. La ley francesa de Informática y Libertades de 1978 ha sido objeto de una reforma parcial por la ley 94-548, de 1 de julio, sobre la investigación en materia de salud. La ley añade un Capítulo V bis, que comprende diez artículos, del 40.1 al 40.10, mediante los cuales se modulan diversos preceptos de la ley. La gestación de esta ley se remonta a octubre de 1990, en que un grupo de senadores presentó una proposición de ley que no fue objeto de debate. El antecedente inmediato es un proyecto presentado por Hubert Curien, Ministro de Investigación y Tecnología del Gobierno presidido por Edith Cresson, que tuvo entrada en la Asamblea Nacional en marzo de 1992. La ley puede considerarse como parte de un conjunto de leyes aprobadas a lo largo del año 1994 relacionadas de algún modo con la problemática bioética (Ley 94-653, de 29 de julio, sobre el respeto al cuerpo humano; Ley 94-654, de 29 de julio, sobre donación y utilización de elementos y productos del cuerpo humano, asistencia médica para la procreación, y diagnóstico prenatal). La ley elude los problemas de bioética y se limita a una formalización jurídica del uso de las innovaciones tecnológicas en la investigación en materia de salud.

Objeto de la ley es integrar en el régimen general de la ley de 1978, de Informática y Libertades, los tratamientos automatizados realizados con fines de investigación médica. Estos tratamientos sólo quedan excluidos de la aplicación de los artículos 15, 16 y 17 (trámites previos al uso de los tratamientos), 26 (derecho a oponerse al tratamiento) y 27 (información del interesado, previa a la recogida de datos), todos ellos de la ley de 1978. Esta exclusión no es total, sino que la ley contiene en el nuevo capítulo las modulaciones pertinentes de dichos preceptos. La regulación sólo contiene dos excepciones: los tratamientos cuya finalidad sea el seguimiento terapéutico o médico individual de los pacientes, es decir, los tratamientos de los datos recogidos en el contexto de la relación médico-enfermo, y los tratamientos de investigación realizados a partir de estos datos (artículo 40.1, párrafo segundo). En todo caso unos y otros están amparados por los demás preceptos de la ley de 1978.

La nueva regulación refuerza las potestades de la C.N.I.L. en la medida en que, a diferencia del régimen general de la ley de 1978, estos tratamientos requieren una autorización previa de la C.N.I.L., a la cual se dota, a su vez, de un Comité consultivo que deberá juzgar en cada caso sobre la metodología de la investigación, la necesidad de utilizar datos personales y la pertinencia de estos para la finalidad de la investigación. Con ello el artículo 40.2 ha optado por una modulación de la norma del artículo 15 de la ley de 1978. Dicho artículo exige como trámite previo a la instauración de un tratamiento cuyo responsable sea una administración pública, una disposición reglamentaria previo dictamen favorable de la C.N.I.L. Si el dictamen no es favorable, es precisa una norma de rango de decreto, dictaminado por el Consejo de Estado. Este procedimiento no sería viable en el caso de tratamientos realizados por cuenta de entes privados que, en la mayoría de los casos serían los responsables de los tratamientos de investigación médica. Por ello la nueva regulación ha previsto un procedimiento de control previo aplicable a cualquier tratamiento, cualquiera que fuera el responsable.

En cuanto al régimen protector de los datos, los nuevos artículos 40.3, 40.4 y 40.5 contienen disposiciones que derogan o modulan disposiciones de la ley de 1978 y de otras leyes. El primero permite que los profesionales de la medicina cesan datos personales para que sean utilizados en tratamientos de investigación autorizados por la C.N.I.L., pero para ello, los datos deberán ser codificados antes de ser cedidos. Esta norma de la codificación previa puede, sin embargo, ser dejada sin efecto en casos de tratamientos vinculados a estudios de vigilancia farmacéutica o de proyectos de cooperación nacional o internacional o "si así lo exigiere una particularidad de la investigación". En todo caso, la exposición de los resultados de la investigación deberá ser despersonalizada, de tal manera que no sea posible identificar directa o indirectamente a los interesados. El artículo 40.4 refuerza el derecho de oposición del interesado, en la medida en que para dicha oposición no es preciso invocar "razones legítimas". El consentimiento del interesado, si bien no es viable cuando se trata de investigaciones epidemiológicas, se exige sin embargo como condición previa de tratamiento cuando la investigación requiera tomas de sustancias o tejidos que permitan identificar al interesado. También en el caso de personas fallecidas es preciso contar con el consentimiento del interesado para utilizar información sobre el mismo, incluida la información contenida en certificados de defunción. Para ello se requiere que dicho consentimiento haya sido prestado en vida por el interesado. Por último el derecho a ser informado de la recogida y de determinadas circunstancias, regulado por el artículo 27 de la ley de 1978, ha sido modificado para estos tratamientos por el nuevo artículo 40.5, añadiendo a las informaciones previstas por aquél las referentes a la naturaleza de la información recogida y a la finalidad del tratamiento.

Las demás disposiciones añadidas por la nueva regulación prevén la posibilidad de una sanción en la forma de la revocación de la autorización de la C.N.I.L. (artículo 40.8) en caso de incumplimiento de las nuevas disposiciones, así como la exigencia de cifrar los datos personales objeto de estos tratamientos cuando hubieren de ser transferidos a un Estado cuya legislación no prevea una protección equivalente a la de la legislación francesa (artículo 40.9).

El 12 de julio de 1994 se publicó la ley federal austríaca por la que se regulan los trabajos con organismos modificados con técnicas genéticas, la liberación y puesta en circulación de estos organismos, y asimismo la aplicación a las personas de los análisis genéticos y la terapia génica (*Gentechnikgesetz*). En su Sección IV, referente al análisis genético y la terapia génica realizados en personas, está incluido el parágrafo 71, sobre protección de datos. Asimismo, la Sección X regula lo referente a la confidencialidad de datos (§§ 105 y 106), y en la Sección XI (§ 107) el intercambio internacional de información, todo ello con relación al análisis genético y la terapia génica. El § 71 contiene una regulación específica del uso, manual y automatizado, de los datos obtenidos en el marco de estos trabajos. Dispone que la persona objeto de análisis debe ser informada de todos los datos que le conciernan; asimismo debe ser informada de los resultados inesperados que tuvieren trascendencia clínica inmediata o que ella misma hubiera pedido expresamente. Los datos obtenidos sólo pueden ser difundidos para una finalidad distinta si el interesado presta su consenti-

miento o previa su despersonalización. En todo caso, sólo pueden ser comunicados a personas de la institución en la cual se hicieren los análisis y que directamente tuvieren a su cargo la elaboración o explotación de los datos, al propio interesado, al médico que hubiera ordenado el análisis y a las personas que el interesado autorizare. Los datos no despersonalizados sólo pueden ser tratados automáticamente en la institución en la cual se hicieren los análisis y bajo el control del médico, deberán ser almacenados separadamente y sólo podrán acceder a ellos personas autorizados por la ley. El acceso sólo podrá hacerse por unas vías de acceso separadas. La ley general de protección de datos se aplica supletoriamente.

Los §§ 105 á 107 prevén, respectivamente, limitaciones para la difusión de estos datos, su cesión a organismos públicos e intercambio internacional de datos.

El tercero de los aludidos órdenes de problemas, el de la calificación que, desde el punto de vista de la protección de datos deba darse a la grabación magnetoscópica de imágenes mediante equipos instalados en lugares públicos, ha sido objeto de especial atención en el transcurso del año 1994. Este problema había sido contemplado ya en el frustrado proyecto belga de Ley de Protección de Datos de 1976 (proyecto Vanderpoorten), que había tratado de integrar la problemática de los ficheros de datos de carácter personal, las escuchas de comunicaciones y las grabaciones magnestocópicas. En el transcurso del año 1994 el problema se ha suscitado en el marco del Grupo Negociador de la Directiva SYN 287, en el cual la delegación francesa trató de ampliar la definición de datos a la información consistente en sonidos o imágenes. La Comisión francesa de Informática y Libertades se ha planteado a este respecto dos problemas: a) las imágenes como parte del concepto de "datos de carácter personal", b) la consideración de fichero automatizado o manual de estas grabaciones magnetoscópicas. La C.N.I.L. aprobó el 21 de junio el Acuerdo núm. 94-056, por el que se adoptaba una Recomendación sobre el uso de los dispositivos de vigilancia magnetoscópica instalados en lugares públicos y en lugares de acceso público. La Recomendación de la C.N.I.L. traspone al contexto del uso de estos dispositivos las disposiciones de fondo de la ley de Informática y Libertades, pero no considera que la información recogida constituya un fichero automatizado. La Recomendación da normas rigurosas sobre la conservación de la información. Las imágenes grabadas deben ser destruidas en un plazo de quince días o, de lo contrario, entregadas en original a la autoridad judicial o, bajo el control de ésta, a la policía judicial, sin que la persona responsable del dispositivo de grabación masgnetoscópica pueda conservar copia, salvo con autorización judicial.

La Recomendación dispone asimismo que el público sea informado de la colocación de estos dispositivos.

La doctrina sentada por la C.N.I.L. ha sido recogida en el articulado del proyecto de ley de Seguridad privada. El artículo 8 regula pormenorizadamente el uso de estos equipos y excluye las grabaciones visuales de vigilancia magnetoscópicas de la noción de "información nominativa" de la ley de Informática y Libertades, a menos que se utilicen para constituir ficheros de datos personales (ficheros nominativos). El proyecto francés ha motivado que el Consejo de Europa se pronunciara sobre esta cuestión. El Comité consultivo del Convenio 108, en su sesión 10ª (23-25 de noviembre) acordó elevar al Comité de Ministros un informe sobre la inclusión de voz e imágenes en el concepto de "datos de carácter personal" definido en el artículo 2 a) del Convenio. El Comité consideró que el proyecto francés podía crear un precedente peligroso en la medida en que podría dar lugar a interpretaciones dispares entre los Estados parte, lo cual, a su vez, repercutiría en la eficacia práctica de la norma del artículo 12, que condiciona la transferencia transfronteriza de datos a la existencia en el Estado destinatario de una protección equivalente a la de la legislación del Estado transferente. Por otra parte, la progresiva difusión de las técnicas de multimedia, que permiten registrar a la vez textos, imágenes y sonidos acarrea riesgos no sólo para los datos personales sino, asimismo en relación con otras libertades. Por ello, el Comité consultivo del Convenio 108 estimó que convenía revisar la definición del artículo 2 a) del Convenio, haciendo algunas precisiones. En primer lugar, distinguir entre imágenes y sonidos objeto de tratamiento digital o de tratamiento analógico. Los primeros entran plenamente en el ámbito del Convenio. Los segundos, una vez recogidos, sólo entrarían en dicho ámbito en la medida en que fueran sometidos a un tratamiento automatizado con miras de identificar a las personas interesadas.

En todo caso, los sonidos e imágenes entrarían en el ámbito de aplicación de la opción del artículo 3.2 c) del Convenio, según la cual cada Estado parte puede o no aplicar el Convenio a datos no automatizados, formulando la declaración pertinente.

LOS FICHEROS MULTINACIONALES

Dentro del año 1994 ha sido posible al fin superar los distintos problemas técnicos sin cuya solución no podía entrar en funcionamiento el Sistema de Información de Schengen, según lo previsto en el artículo 139 del Convenio de aplicación de 1990. El Comité Ejecutivo, reunido el 22 de diciembre, acordó fijar para la plena entrada en funcionamiento, la fecha de 26 de marzo de 1995, en que habrá quedado ultimada una fase preparatoria. A partir de dicha fecha, los usuarios del sistema podrán servirse de él normalmente. En todo caso, el Sistema quedará limitado a los Estados que han cumplido los compromisos del Convenio, entre ellos la incorporación al Derecho interno de una ley de protección de datos que cumpla con el Convenio 108 del Consejo de Europa y la Recomendación R (87) 15 del Consejo de Europa, por lo cual quedan por el momento excluidos del Sistema Italia y Grecia. En la fecha citada quedará extinguida la Autoridad Provisional Común de Control y se constituirá la Autoridad Común de Control prevista en el artículo 115 del Convenio.

En la Conferencia de Autoridades de Protección de Datos de la Unión celebrada en Madrid los días 25 y 26 de mayo se puso de manifiesto la preocupación de dichas Autoridades por la proliferación de convenios y proyectos de convenios de cooperación intracomunitaria que, siguiendo en buena parte el patrón de los Acuerdos de Schengen, inciden en la

protección de los datos de carácter personal, en la medida en que crean grandes sistemas de información de carácter personal con datos generalmente sensibles. Actualmente se hallan en curso de negociación tres de tales convenios: El Sistema de Información Europeo, complementario del Convenio sobre el Cruce de las Fronteras Exteriores de la Unión, el Sistema de Información Aduanero y el Convenio EUROPOL previsto en el artículo k.1, apartado 9, del Tratado de la Unión Europea. Estos convenios vienen suscitando la preocupación de las Autoridades nacionales de protección de datos, debido a que no todos contienen disposiciones homogéneas y suficientemente precisas en la materia, ni todos contemplan el supuesto de los ficheros no automatizados. Asimismo, se ha suscitado el problema de la interrelación y acceso recíproco, en especial entre EUROPOL y el Sistema de Información Europeo, así como con relación a los ficheros automatizados de la O.I.P.C. (INTERPOL). De los tres convenios, el del Sistema de Información Europeo es el que se encuentra más adelantado en el plano de la negociación. A diferencia del Convenio de Schengen, este convenio no está concebido como un marco general de cooperación policial y judicial, cuyo instrumento sea una base de datos con partes nacionales y una unidad central de apoyo sino que se limita a dicha base de datos, la cual, a su vez está limitada a los datos referentes a la lista conjunta de personas cuya entrada está vedada en la Unión según lo previsto en los artículos 10 y 13 del citado Convenio sobre cruce de las Fronteras Exteriores.

La última versión es de 9 de diciembre y comprende, en lo que respecta a la protección de datos, un total de 19 artículos, que reproducen casi literalmente los correspondientes del Convenio de aplicación de Schengen, sin más diferencia que la de prever expresamente un órgano que asuma el control de los datos no automatizados, complementarios de los incluidos en la base de datos ("SIRENE"). Subsiste, en todo caso, el problema de base del Convenio sobre el cruce de Fronteras Exteriores, referente a la consideración de Gibraltar como frontera exterior, y que por el momento ha dado lugar a un bloqueo por parte del Reino Unido y España, sin que se prevea una solución a corto plazo.

La Conferencia de Madrid aprobó una declaración conjunta de las Autoridades de Protección de Datos sobre estos sistemas de información multinacionales, reafirmado la necesidad de que en todos ellos exista un sistema coherente de principios de protección de datos, incluyendo una autoridad de control independiente a nivel nacional e internacional, que debería ser considerada como una condición *sine qua non* para el intercambio de datos de carácter personal. La Conferencia subrayó asimismo la necesidad de una armonización de las disposiciones de protección de datos, sugiriendo la posibilidad de integrar las Autoridades de Protección de datos previstas en cada convenio en una sola que siguiera el patrón del artículo 115 del Convenio de Schengen, estimando que la existencia de una única autoridad a escala internacional evitaría divergencias en la interpretación de las disposiciones de protección de datos. La presidencia alemana del Consejo de la Unión se ha hecho cargo de estas sugerencias en relación con los trabajos de negociación del Convenio EUROPOL, existiendo un pronunciamiento expreso al efecto del Ministro Federal alemán del Interior.

LA PROTECCIÓN DE DATOS EN OTROS PAÍSES

La XVI Conferencia mundial de autoridades de protección de datos

En los días 6 a 8 de septiembre se celebró en La Haya la XVI Conferencia Mundial de Autoridades nacionales de Protección de Datos ("Conferencia de Comisarios"), que se viene reuniendo anualmente desde 1979, en que el Comisario Federal alemán convocó con carácter oficioso a las Autoridades a la sazón existentes y que desde entonces se ha reunido ininterrumpidamente en distintas capitales: Bonn (1979), Ottawa (1980), París (1981), Londres (1982), Estocolmo (1983), Viena (1984), Luxemburgo (1985), Lisboa (1986), Quebec (1987), Oslo (1988), Berlín (1989), París (1990), Estrasburgo (1991), Sydney (1992), Manchester (1993). Estas Conferencias permiten actualizar el panorama mundial de la protección de datos y reflejan a través de las ponencias y de los informes nacionales las tendencias y las preocupaciones, generalmente recurrentes, de los órganos que tienen a su cargo la aplicación de las distintas legislaciones.

La Conferencia de 1994 hizo hincapié en los grandes dilemas que ofrece la protección de datos -*Facing Dilemmas*- fue el tema básico de debate, en el que se pronunciaron profesores, sociólogos, gestores públicos y proveedores de servicios informáticos. Estos dilemas resultan del conflicto básico de intereses que caracteriza la protección de datos: el grado de aceptación social de los servicios que se prestan con ayuda de los procesos informáticos de datos personales, en sus múltiples formas, desde el fichero ordinario masivo de empresa hasta la tarjeta de microprocesador y los grandes sistemas de transmisión masiva de datos, y los riesgos múltiples y cambiantes que el uso incontrolado de los datos y de la inferencia automática crean por la propia dinámica de la tecnología, sin que el interesado cuestione estos procesos ni tampoco los acepte de manera consciente y responsable. Estos dilemas se van agudizando con las últimas innovaciones de la tecnología, como las llamadas "autopistas de la información". Entre los temas tratados, reveladores de una preocupación por parte de estos órganos, hay que mencionar los sistemas de calificación por puntuación a efectos de concesión de créditos (delegaciones de Francia y Reino Unido), los riesgos potenciales de INTERNET (Reino Unido), las tarjetas de microprocesadores (Hamburgo, Francia), correo electrónico y protección de datos (Ontario), directorios X500 (Berlín). La XVII Conferencia se celebrará en Copenhague los días 5 a 7 de septiembre de 1995. Para la XVIII Conferencia (1996) son candidatos Canadá y España.

Por lo que respecta al movimiento legislativo en general, ninguna innovación importante ha tenido lugar en el ámbito extraeuropeo, si se exceptúa la actividad preparatoria de las provincias y territorios del Canadá que todavía no cuentan con una legislación protectora de datos, de carácter general o limitada al sector público.

MEMORIA DE 1994 - LA PROTECCIÓN DE DATOS A ESCALA NACIONAL

Es innegable que a lo largo del año 1994 el marco normativo de la protección de datos se ha ido completando. Así, junto a la propia Ley Orgánica y al Estatuto de la Agencia, textos jurídicos vigentes con anterioridad, se ha incorporado el Reglamento de la misma, aprobado por Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica, haciendo posible la aplicación de concretos preceptos de su articulado en materias tan fundamentales como las transferencias internacionales de datos, la notificación e inscripción de ficheros, el ejercicio y tutela de los derechos del afectado y la regulación del procedimiento sancionador. Desarrollo reglamentario que sin duda deberá ser completado en materias como la de seguridad de los datos y la conservación integra de los mismos atendiendo sus valores históricos.

Por tanto, desde el punto de vista de la aplicación de la normativa de protección de datos personales, ha de considerarse que la existente es, en principio, suficiente para la realización de la tarea encomendada. Ahora bien, debe tenerse presente en este punto que dentro de un breve periodo de tiempo penetrarán en nuestro derecho interno una serie de disposiciones de derecho comunitario derivado que se encuentran en este momento en un estado muy próximo a su aprobación (Directiva 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), o en situación muy adelantada en cuanto a su tramitación, (protección de datos personales en relación con las telecomunicaciones, SYN 288, o con la venta a distancia), o proyectos de Convenio por los que se crea Europol o el Sistema de Información Europeo, que sin duda van a producir cambios sustanciales en nuestro derecho interno.

Si a todo lo anterior se une, por un lado, las futuras resoluciones del Tribunal Constitucional que pondrían fin a los recursos de inconstitucionalidad interpuestos contra la Ley Orgánica y, por otro, las deficiencias que en la aplicación de la misma se vayan poniendo de manifiesto, es claro que puede predecirse la necesidad de una modificación próxima de la Ley que atienda y resuelva todas estas cuestiones.

PROBLEMAS QUE SE HAN PUESTO DE MANIFIESTO EN LA APLICACIÓN DE LA LEY ORGÁNICA

Como ya se expuso con anterioridad, la aplicación de la normativa de protección de datos iniciada prácticamente durante el segundo semestre del año 1994 ha puesto de manifiesto una serie de problemas respecto a la interpretación de determinados preceptos de la Ley, en relación a situaciones de hecho concretas, que a continuación pasamos a exponer:

FICHEROS DE TITULARIDAD PÚBLICA

La determinación de lo que debe entenderse por Administración Pública a efectos de la aplicación o no de los artículos 18 y 19 de la Ley Orgánica ha planteado grandes dudas en el momento de llevar a cabo la inscripción de los ficheros de aquella naturaleza. El concepto de Administración Pública, al que hace referencia en concreto el artículo 18 de la Ley Orgánica, ha planteado el problema de si todo fichero perteneciente a la misma debe ser objeto de la aplicación del precepto, o, por el contrario, el contenido del mismo solamente se aplicará a aquellos ficheros que correspondan a las Administraciones Públicas siempre que tengan capacidad normativa propia. Dicho de otra manera, si los ficheros pertenecientes a los Colegios Profesionales y a las Sociedades Estatales, que, conforme a los artículos 1 de la Ley de Colegios Profesionales, Ley 2/74, de 13 de febrero, y 6.1. a) de la Ley General Presupuestaria, Texto Refundido aprobado por Real Decreto Legislativo 1091/88, de 23 de septiembre, aparecen definidos como corporaciones de derecho público o como sociedades mercantiles en cuyo capital sea mayoría la participación, directa o indirecta, de la Administración del Estado o de sus organismos autónomos y demás entidades estatales de Derecho Público, tienen la consideración de ficheros públicos, o, por no tener capacidad normativa propia, deben adoptar la configuración de ficheros de titularidad privada como forma de salvaguardar su independencia y lograr la agilidad de gestión propia de las sociedades regidas por las normas de Derecho mercantil, civil o laboral.

La solución, en principio, del problema sería la de otorgar a sus ficheros la consideración o la naturaleza de privados sin perjuicio de que en reforma legislativa posterior se decida sobre la existencia o no de la división entre la titularidad pública o privada de los ficheros, máxime cuando la posición común del Consejo de la Unión Europea con vista a la adopción de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos no establece ninguna diferencia de tratamiento entre ficheros de una y otra naturaleza.

La interpretación del artículo 19 de la Ley Orgánica no ha dejado de plantear igualmente problemas en lo referente a qué debe entenderse por Administraciones Públicas cuando de cesión de datos personales se trate. Es decir, si debe aplicarse un concepto unitario de Administración Pública, (actuación con personalidad jurídica única conforme a lo establecido en el artículo 1 de la Ley de Régimen Jurídico de la Administración del Estado de 26 de julio de 1957), de forma que solamente coexistan la estatal, la autonómica, la local, la corporativa o la institucional, o, por el contrario, debe entenderse que el criterio diferenciador ha de situarse en otros elementos que permitan determinar en que caso se pueden ceder datos entre distintas Administraciones Públicas como si de una misma se tratara, y en cuales no pueden llevarse a cabo las mismas incluso entre ficheros pertenecientes a un mismo Departamento ministerial,

Consejería autonómica o Concejalía. Planteado así el problema, ha de señalarse que la interpretación primera, al ser formulada de manera tan amplia, desconoce criterios de coincidencia en las competencias atribuidas a los órganos de los ficheros, o de similitud de las materias por ellos tratadas, lo que permitiría la posibilidad de cesiones de datos entre todos los ficheros pertenecientes a una Administración sin someterse a ninguna de las precisiones que establece el artículo 19. Debe por ello, adoptarse la segunda postura, ya que parece ser la mas acorde con el contenido del precepto, que permite la posibilidad de cesión para el ejercicio de competencias idénticas o que versen sobre materias similares, y desde luego es más respetuosa con la prohibición de usar el dato personal para una finalidad distinta de aquella para la que fue recogido como dispone el artículo 4.2 de la Ley Orgánica.

De todos modos, sería deseable que la ley matizara más, a efectos de la interpretación del artículo 19, el concepto de Administración Pública en materia tan relevante como es la cesión de datos personales entre las Administraciones Públicas.

Igualmente debe ser objeto de análisis la cuestión de la incidencia o no en lo que respecta a la aplicación de la Ley Orgánica a aquellas conductas que, pudiendo ser incluidas en algunas de las infracciones previstas en el artículo 43 de la misma, tienen su origen en materias que conforme a lo dispuesto con su artículo 2.3 se rigen por unas disposiciones específicas. En concreto, si la utilización del censo electoral con fines de captación de futuros clientes que han venido efectuando algunas empresas supone la comisión de alguna infracción de las previstas en el artículo 43 de la Ley Orgánica. Es claro que la realización de dichas conductas encierra en sí misma una cesión, en principio no consentida por parte del titular del dato personal, ya que el mismo se utiliza por un tercero que no tenía la condición legal de destinatario y para una finalidad diferente a la propiamente electoral. Por ello, parece lógico que deba predicarse la plena aplicación de la normativa contenida en la Ley Orgánica para tratar de restablecer la pérdida de la intimidad que puedan sufrir los ciudadanos como consecuencia de dichas prácticas. Además, la tesis de la aplicación de la normativa de protección de datos, queda reforzada por la propia interpretación del artículo 2 de la Ley Orgánica en donde se distingue entre ficheros a los que no puede aplicarse la misma, (artículo 2.2), y ficheros que aun rigiéndose por sus disposiciones específicas, (artículo 2.3), se encuentran dentro de su ámbito protector en lo referente a la realización de actividades posteriores y distintas de aquellas previstas como propias en la específica legislación de que se trate. Una interpretación distinta a la que se viene sustentando supondría, además de ser a nuestro juicio no conforme a los criterios normales de análisis jurídico, dejar desprotegido un amplio campo de datos personales con gran incidencia en el plano de la intimidad.

En otro orden de cosas, llama poderosamente la atención la falta de previsión legal, cuando de la materia de sanciones se trata, respecto del destino que haya de darse al fichero o ficheros de datos personales a través del cual se hubiera cometido la infracción. Es cierto que la Ley Orgánica, a través de su articulado, regula la cancelación pero como derecho personalísimo del afectado, (artículo 15.3 de la Ley Orgánica y artículos 11 y 15.3 del Reglamento), e igualmente la modificación y cancelación de la inscripción, (artículo 8 del Reglamento). Ahora bien, la potestad de cancelar ficheros, como consecuencia directa de la infracción cometida a través de su uso, no parece regulada en los tipos de sanciones del artículo 44 de la Ley Orgánica, ni se prevé medida de esta naturaleza, aunque sí se admite la potestad de inmovilizar ficheros, (conforme al artículo 48 de la Ley Orgánica), y el bloqueo de datos (artículo 16 del Reglamento). En esta materia no puede desconocerse que el artículo 36. f) de la Ley Orgánica al enumerar las funciones de la Agencia de Protección de Datos alude genéricamente a "...la cancelación de los ficheros cuando no se ajusten a las disposiciones de la presente ley"; ahora bien, lo que venimos afirmando es que dicha facultad, genéricamente definida en dicho precepto, no aparece desarrollada en el resto del articulado, lo que no deja de producir inconvenientes graves a la hora de determinar si tal medida, de poder llevarse a efecto, se aplica a todo tipo de infracción, leve, grave o muy grave, o, por ejemplo, solamente a las muy graves, o si la misma se aplica conjuntamente con las sanciones pecuniarias o en algún caso cabría imponerse en sustitución de aquellas. Quizá, lo más lógico sería dar al fichero de datos personales la consideración de instrumento necesario e imprescindible para la comisión de la infracción y como tal aplicar la solución que el Código Penal establece para el mismo, (artículo 48), con las salvedades y destino que en el mismo se establece.

La aplicabilidad del precepto penal al derecho administrativo sancionador se efectuaría teniendo en cuenta la doctrina recogida por las resoluciones del Tribunal Supremo y del Tribunal Constitucional que señalan que los principios inspiradores del orden penal son de aplicación, con ciertos matices, al citado derecho dado que ambos son manifestaciones del ordenamiento punitivo del Estado tal y como se refleja en la propia Constitución.

Las competencias atribuidas a la Agencia en el campo de la elaboración y aplicación de las normas que incidan en materia propia de la Ley Orgánica no han sido, desde un punto de vista puramente interpretativo, comprendidas y consecuentemente aceptadas por los órganos competentes en materia de desarrollo normativo. El artículo 36.h) de la Ley señala, entre otras, como funciones de la Agencia la de informar, con carácter preceptivo, los proyectos de disposiciones generales que la desarrollen. Precepto que ha de ser complementado con lo previsto en el n) del mismo artículo, por el que se asigna con carácter residual a la Agencia, cualquier otra materia que le sea atribuida por normas legales o reglamentarias. En este sentido, debe señalarse que el artículo 5 de su Estatuto, en sus apartados a) y b), establece el informe preceptivo no sólo de los proyectos de disposiciones generales de **desarrollo** de la Ley Orgánica, sino también de cualesquiera proyectos de ley o reglamento que incidan **en la materia propia de aquélla**. El contenido de los citados apartados es claro: dentro de las misiones que por el artículo 36 de la Ley Orgánica se confían a la Agencia se encuentra la de informar cualquier disposición legislativa que desarrolle la misma o que afecte a materias reguladas por ella. El comportamiento de las Administraciones Públicas en el cumplimiento de esta obligación ha sido desigual, más por desconocimiento del contenido de las normas que venimos comentando que por reticencias a cumplir con lo establecido. La actuación de la Agencia en esta materia ha ido dirigida tanto a dar a conocer a los órganos encargados de promover el desarrollo normativo estatal y autonómico la necesidad del informe preceptivo en los términos antes señalados como a solicitar la colaboración de los poderes propiamente legislativos para evitar que pudiera tramitarse

cualquier proyecto de disposición legislativa que no contara con el previo informe de la Agencia.

El problema que venimos tratando se complica aun más cuando de desarrollo normativo de carácter autonómico se trata: el artículo 40 de la Ley Orgánica, al desarrollar los órganos idénticos a la Agencia dentro de las Comunidades Autónomas, atribuye a los mismos, entre otras, las competencias contenidas en los apartados h) y n) del artículo 36. La redacción, en principio, de ambos apartados no presenta problemas: las normas y disposiciones reglamentarias que desarrollan la Ley Orgánica se refieren a materias con incidencia en la misma que, cuando tengan carácter autonómico, deberían ser informados por los órganos competentes de cada Comunidad. Ahora bien, determinar quién es el que debe cumplir con ese precepto en los supuestos en que todavía no se haya creado el órgano autonómico es cuestión fundamental que, sin ánimo de invadir competencias autonómicas, debe resolverse atribuyendo residualmente a la Agencia las mismas con carácter transitorio. Lo contrario supondría incumplir sistemáticamente con la obligación de dictaminar, bien por inexistencia transitoria del órgano competente, bien por que exista voluntad de eludir dicho trámite y cualquier otra función que tenga atribuida el órgano autonómico correspondiente a través de la no creación del mismo. Sí, a nuestro juicio, está claro que las funciones reservadas a la Agencia autonómica no podrán ser encomendadas a otro órgano de la Comunidad ya que le faltaría la nota de la independencia que respecto de las Administraciones se establece en el artículo 34.2 de la Ley Orgánica. En el anexo I se acompaña relación de proyectos de disposiciones legales sometidas a informe de la Agencia. Por último las consideraciones anteriormente efectuadas fueron confirmadas en informe emitido por la Dirección General del Servicio Jurídico del Estado al señalar como conclusiones que, por un lado, no se aprecian motivos de ilegalidad en el artículo 5.
b) del Estatuto de la Agencia y, por otro, que el informe previsto en el referido precepto obliga a los órganos a los que corresponda la elaboración de Proyectos de leyes o Reglamentos que incidan en la materia propia de la Ley Orgánica.

La interpretación del contenido del apartado c) del artículo 36 plantea igualmente problemas y puede afectar de forma importante al papel que en el futuro tiene que desarrollar la Agencia. El mencionado apartado otorga a la Agencia la facultad 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, planteando el problema de lo que debe entenderse por instrucción, es decir, si es o no un acto administrativo al que se le atribuye carácter normativo.

Planteado así el problema de interpretación del citado apartado, deben igualmente tenerse en cuenta una serie de consideraciones: primera, que no debe equipararse el término instrucción con la instrucción de servicio ya que en ningún caso la instrucción a la que se refiere el apartado c) del artículo 36 de la Ley Orgánica puede ser considerada como una orden general impartida por un órgano a aquellos que de él dependen, señalándoles el sentido de su actuación; segunda, que aquella tiene por finalidad la de adecuar los tratamientos automatizados, cualquiera que sean estos, y no resolver un aspecto concreto y determinado; tercera, que el artículo 5, apartado c) del Estatuto coloca, junto a las instrucciones, las **recomendaciones precisas** con lo que parece diferenciar el carácter normativo de las primeras a diferencia de las segundas; cuarta, que la instrucción va dirigida a un colectivo indeterminado de personas, bien sean todos aquellos que son responsables de ficheros automatizados de datos personales, bien los que lo sean de una serie de ficheros correspondientes a una determinada finalidad y, por último, que cuando el Estatuto ha querido **limitar** la competencia de la Agencia de Protección de Datos lo ha dispuesto de manera expresa. Así, en materia de seguridad de los datos y control de acceso a los ficheros, como establece el apartado c) del artículo 5 del Estatuto, solamente podrá dictar recomendaciones y nunca instrucciones. Debe añadirse que la nota de la independencia de la Agencia de Protección de Datos respecto del resto de las Administraciones Públicas precisamente refuerza la línea interpretativa que venimos manteniendo ya que, lo contrario, le privaría de la capacidad de adecuar los tratamientos automatizados a los principios de la Ley Orgánica o eliminaría su nota de independencia pues tendría que recurrir para lograr tal fin a otros órganos administrativos dotados de potestad normativa.

A estos efectos debe igualmente señalarse que conforme al artículo 47.2 las resoluciones de la Agencia ponen fin a la vía administrativa pudiendo interponerse contra las mismas el correspondiente recurso contencioso-administrativo.

Igualmente ha de ser objeto de tratamiento en esta parte de la Memoria el problema de qué deba entenderse por ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general, según la redacción contenida en el artículo 2.2.a) de la Ley Orgánica. Es claro que en esta materia existen una serie de ficheros destinados a fines de publicidad que no presentan ningún problema interpretativo por estar clara que esa es la finalidad perseguida por los mismos. Así, los ficheros de los Registros de la propiedad y mercantiles participan plenamente de esa idea y consecuentemente por aplicación del artículo 2.1 de la Ley se hallan fuera del ámbito de la misma como señala igualmente la Exposición de Motivos. El problema ciertamente se complica cuando, sin ser ficheros dirigidos a la publicidad con carácter general, se exponen públicamente con el fin de lograr una finalidad diferente como puede ser alcanzar la certeza y veracidad de sus asientos mediante la corrección de sus errores. El problema es importante tanto por el volumen de datos que suelen contener los ficheros a los que nos referimos como por el deseo de la incorporación de sus datos a ficheros de titularidad privada. Estamos aludiendo al padrón municipal y al censo electoral que, de conformidad con su legislación específica, (artículo 15.2 del Texto Refundido en materia de Régimen Local y el 39.2 de la Ley Orgánica 3/1995, de 23 de febrero), son objeto de exposición pública para la formulación de reclamaciones.

En esta materia no puede nunca equipararse, por tratarse de términos de significado diferente, la publicidad con la exposición pública de un determinado dato, por lo que ni el padrón municipal ni el censo electoral tendrán la consideración de ficheros en los que se almacenan datos para su publicidad con carácter general sino que siempre serán ficheros de titularidad pública sometidos a una legislación específica sin que en ningún caso puedan utilizarse los datos personales sin el consentimiento del interesado ya que ni lo prestó por tratarse, dada la finalidad de los ficheros, de datos obligatorios, ni mucho menos podrán ser utilizados para finalidades distintas de las estrictamente perseguidas por el padrón municipal y el censo electoral.

Dentro del estudio de los problemas de aplicación de la Ley Orgánica a los ficheros de titularidad pública, debe hacerse especial referencia a los denominados Ficheros Judiciales. Ante el silencio que de los mismos guarda la Ley, debe en primer lugar determinarse si tales ficheros pueden regularse conforme a las prescripciones de la misma. En este aspecto debe señalarse que la disposición adicional 1ª de la Ley Orgánica excluye de la aplicación de los Títulos VI y VII a los ficheros automatizados de los que son titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional. El artículo 2 de la Ley Orgánica, por otra parte, no incluye a los ficheros judiciales entre aquellos que están excluidos del ámbito de aplicación de la Ley o se rigen por sus disposiciones específicas.

Podría llegarse a afirmar, alternativamente, que o la Ley Orgánica ha dejado fuera de su regulación, voluntaria o involuntariamente, a los ficheros judiciales o que los ha incluido dentro de la denominación genérica de ficheros del Consejo General del Poder Judicial confundiendo aquellos que sirven al órgano de gobierno de los jueces y tribunales con los que directamente van dirigidos a la realización de tareas propiamente jurisdiccionales.

La cuestión es grave y compleja máxime si se tiene en cuenta el extraordinario volumen de ficheros judiciales referidos a todos los ámbitos de actuación de las funciones jurisdiccionales, con tratamiento en la mayoría de circunstancias de datos especialmente protegidos, y la regulación que la Ley Orgánica 6/1985, del Poder Judicial, ha efectuado, de los ficheros informáticos para el desarrollo de su actividad y el ejercicio de sus funciones a través del artículo 230 de la misma. A través de este precepto se ha resuelto uno de los problemas más importantes, cual es el del sometimiento de los ficheros personales de datos automatizados a las prescripciones de la Ley Orgánica, pues así expresamente se dispone en el punto 5 del citado precepto. No obstante, quedan sin resolver dudas -mientras no se lleve a cabo el desarrollo reglamentario previsto en dicho apartado- relativas tanto a quién debe ser el responsable del fichero como a problemas de aplicación de medidas sancionadoras en caso de incumplimientos graves de los principios rectores de la Ley de Protección de Datos, sanciones que, en principio, parece lógico deberían ser impuestas por los órganos competentes sancionadores de aquellos que ejerzan la actividad jurisdiccional.

Por otra parte, tenerse debe en cuenta, para una mejor regulación de los ficheros judiciales en el tratamiento de datos personales, que los mismos se hallan relacionados con otros tipos de ficheros -normalmente los policiales- y que será necesaria la interrelación entre ellos a fin de poder concretar conceptos jurídicos indeterminados que aparecen en la regulación de los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado.

FICHEROS DE TITULARIDAD PRIVADA

También respecto de este tipo de ficheros han surgido varios problemas interpretativos que afectan a preceptos específicos de la Ley Orgánica. De entre ellos, merece la pena destacar:

El artículo 28 de la Ley, al regular los denominados ficheros sobre prestación de información sobre solvencia patrimonial y crédito, engloba dentro del mismo dos clases de ficheros totalmente distintos en su tratamiento y contenido: por un lado, los propiamente denominados "de información sobre solvencia patrimonial y de crédito", para los que se exige que sus datos se hayan recogido de fuentes accesibles al público o que procedan de informaciones facilitadas por el afectado o con su consentimiento, y, por otro, los que se refieren al "cumplimiento o incumplimiento de obligaciones dinerarias", para los que no es necesario en el tratamiento del dato el previo consentimiento del afectado ya que basta con que el mismo sea facilitado por el acreedor o por quien actúe por su cuenta o interés. A esta última clase de ficheros no le son ajenos determinados problemas jurídicos relativos a la notificación posterior que debe efectuarse al afectado, a la forma de garantizar el cumplimiento de lo establecido en el artículo 4.3 de la Ley Orgánica referente a la exactitud y puesta al día de los datos de manera que respondan con veracidad a la situación real del afectado, y, por último, a la forma de computar el plazo de seis años que para los antecedentes desfavorables establece el último apartado del artículo 28.

La quiebra del principio del consentimiento del afectado en la recogida y tratamiento de sus datos personales, cuando se trata de un fichero sobre cumplimiento o incumplimiento de obligaciones dinerarias, se justifica en el hecho de que, al tratarse de un fichero que produce valoraciones negativas respecto de las personas que en él se incluyen, sería muy difícil obtener el consentimiento de dicha persona. Es precisamente esta característica de juicio o valor negativo sobre el comportamiento económico de la persona afectada la que debe hacer extremar las precauciones para tratar de evitar inclusiones no justificadas y desde luego inclusiones que no respondan a una situación real de deuda o del importe o cuantía de la misma. Por ello, se hace así mismo necesario el cumplimiento de la obligación de notificación del alta en el fichero como forma igualmente necesaria para garantizar la certeza de dicha inclusión y por ello también es preciso que los plazos de permanencia en el mismo sean interpretados de forma restrictiva de manera que no se concedan, de hecho, ampliaciones en el cumplimiento del establecido con una duración de seis años.

Es evidente que la Ley Orgánica no distingue, por lo que tampoco puede hacerlo la Agencia de Protección de Datos, entre incumplidores y morosos a fin de darles un trato diferente. La diferenciación entre uno y otro supuesto podría lograrse a través de la autorregulación efectuada por los códigos tipo una vez que pudiera ponerse de acuerdo a todas las partes implicadas en este tipo de ficheros. La incidencia que tienen en la vida económica, así como la transcendencia que para el ciudadano produce su inclusión hacen necesaria una especial vigilancia de los mismos tendente a lograr su correcto funcionamiento.

También debe mencionarse el problema surgido respecto de las condiciones que se exigen por parte de las entidades de crédito para la concesión de préstamos con garantía hipotecaria y personal y su vinculación a la celebración de un

contrato de seguro de vida, anejo al mismo. Está claro que los problemas que puedan plantearse como consecuencia de la licitud o no de dichas operaciones, de la posible o no vulneración de la Ley para la Defensa de los Consumidores y Usuarios y de la aplicación de la Ley Reguladora de la Mediación en el Seguro Privado, son ajenos a la competencia de la Agencia de Protección de Datos. Este organismo solamente tiene competencia para decidir sobre la naturaleza de los datos, sobre las condiciones en su recogida, tratamiento y destino, y sobre la cesión de los mismos, velando en todo caso para que los datos de salud sigan necesariamente, en su tratamiento automatizado, al contrato de seguro de vida y en ningún caso queden en poder de la entidad de crédito que de alguna forma actuó de mediadora en dicho contrato.

Igualmente debe afirmarse que presentan problemas de aplicación de las normas de la Ley Orgánica los ficheros que tienen por finalidad restringir, o, si se prefiere, controlar el acceso de las personas a determinados edificios, públicos o privados, cuando tal control sea llevado a cabo por empresas de seguridad privada. Parece conveniente que en estos casos se efectúe una regulación unitaria de dicha actividad en la que se tenga siempre presente la necesidad de una cierta vinculación con normas de seguridad pública y en la que se defina, entre otras cosas, quién sea el que haya de figurar como responsable del fichero, esto es, si lo ha de ser el órgano que sea objeto de vigilancia privada o la empresa que en concreto realiza dicha actividad; el tiempo que, por razones de seguridad pública, se considera necesario deben guardarse los datos contenidos en los ficheros de acceso correspondientes, las cesiones que de los mismos puedan efectuarse y dado que, por último, no puede hablarse en principio de un carácter voluntario en la recogida del dato, ya que sin comunicar el mismo no parece posible el acceso al edificio, si pueden utilizarse cualquier tipo de dato personal, y entre ellos la fotografía.

ANÁLISIS Y VALORACIÓN DE LOS PROBLEMAS

El conjunto de problemas anteriormente enunciados y los que puedan ir apareciendo en el transcurso de los años venideros evidencia una realidad que se hace preciso comentar y que se refiere a la necesidad de encontrar dentro de la sociedad el espacio necesario para que la Ley Orgánica pueda cumplir con la finalidad de protección de la intimidad y, en definitiva, dar cumplimiento a lo establecido en el artículo 18.4 de la Constitución Española.

El problema reside, no sólo en el hecho de que la normativa de protección ha surgido tardíamente, prácticamente quince años después de la aprobación de la Constitución, sino también en que ha sido durante ese periodo cuando se ha producido el desarrollo informático tanto en los medios técnicos como en la aceptación del uso de los mismos por parte de los ciudadanos. La existencia de una pluralidad de bases de datos personales, e incluso sensibles, nacidas sin el control de una regulación legal, limitativa de los abusos y protectora de los derechos de los ciudadanos, supone un plus de dificultad en la aplicación de aquélla.

La expresión partir de cero no es en este caso ni exagerada ni desorbitada si se tiene en cuenta el hecho añadido de que desde la entrada en vigor de la Ley Orgánica y hasta la creación de facto de la Agencia de Protección de Datos transcurrió aún un año más con lo que la existencia de esta normativa de protección y del órgano encargado de ponerla en funcionamiento desapareció de la conciencia social, salvo en muy contadas excepciones de personas que, bien por una especial sensibilidad a este tipo de problemas, bien por dedicar sus actividades de investigación al contenido de esta materia, vinieron manteniendo una mínima noticia de ella.

Por ello, el análisis y la valoración de los problemas que se han planteado, o que en el futuro se planteen, deberán necesariamente pasar por un primer requisito: la necesidad del conocimiento de la existencia de la Ley Orgánica y consecuentemente la necesidad del cumplimiento de las obligaciones y del ejercicio de los derechos que la misma impone. La publicidad de la normativa reguladora de la materia a la que nos estamos refiriendo debe lograrse, en primer lugar, a través de las campañas de difusión que sean necesarias para lograr dicho fin. Así, durante 1994 se efectuó una primera, dirigida fundamentalmente a los responsables de la obligación de inscripción de ficheros y se tiene prevista para 1995 la realización de otra o de otras para lograr que los derechos que la Ley Orgánica tutela sean conocidos por los ciudadanos y consecuentemente puedan ejercitar los derechos en ella reconocidos.

Debe destacarse en esta materia la configuración que efectúa el Reglamento de desarrollo de la Ley Orgánica, al tratar el ejercicio y tutela de los derechos en ella reconocidos, fundamentada en el carácter personalísimo de los mismos, de forma que no pueden ser ejercidos frente al responsable del fichero, salvo en los supuestos de representación legal, sino por el propio afectado o titular de los mismos. Ello conduce a un planteamiento nuevo, si no original, de la materia de protección de la intimidad que podría formularse en los términos siguientes: solamente la persona interesada en la protección de su intimidad podrá alcanzar una defensa eficaz de la misma, o, lo que es igual, es necesaria la colaboración activa del ciudadano para lograr una mejor implantación de la normativa vigente en esta materia, ya que aquí no existe la posibilidad de encomendar o delegar dichas tareas a un tercero, ni siquiera a la Agencia de Protección de Datos cuya actuación, siempre importante, no deja de ser complementaria respecto de la fundamental que tiene encomendada el titular de los derechos.

Dentro de los ficheros de titularidad pública, las Administraciones correspondientes han actuado de forma en principio correcta en el grado de cumplimiento de la Ley Orgánica, tanto en lo referente a la obligación de inscripción de los ficheros como en el resto de las obligaciones que la normativa de protección de datos impone a las mismas.

Ahora bien, si los incumplimientos que se detectan en materia de inscripción son en su mayoría debidos a la falta de conocimiento de la existencia y vigencia de la ley Orgánica y las disposiciones complementarias, las omisiones en cuanto a las demás obligaciones legales presentan a veces una nota de exclusión voluntaria de trámites quizá debida a una diferente interpretación jurídica del precepto en concreto de que se trata.

Los ficheros privados ofrecen, junto a la misma causa de desconocimiento de la existencia de la normativa vigente, una serie de peculiaridades que creemos necesario resaltar. Así, es curioso observar que las finalidades de los ficheros inscritos en el Registro General de Protección de Datos colocan en primer lugar, con una amplia diferencia respecto del resto, a los que se dedican a la gestión contable, fiscal y administrativa, (69,74%), a la gestión de cobros y pagos, (45, 41%) y a la gestión de clientes, (32,74%), pudiendo a la vista de ello afirmar que los más numerosos no son los más importantes desde el punto de vista de la protección del honor y la intimidad, debiendo tener en cuenta dicha circunstancia en una posterior reforma legislativa a fin de tratarlos bien, bajo la forma de una inscripción simplificada, (como establece la legislación francesa), de forma que se tenga un control sobre ellos, si bien no tan intenso que el que se ejerce sobre el resto, bien acordando su no inscripción, (como permite la legislación portuguesa), cuando se trate de ficheros que cumplen una finalidad determinada. En este sentido puede calificarse en principio de excesivo el tratamiento que efectúa nuestra propia legislación que obliga, fuera de las excepciones contenidas en el artículo 2 de la Ley Orgánica, a la inscripción de todo fichero de datos personales con independencia del número de datos y del conjunto pequeño o grande de ciudadanos afectados, olvidando que el peligro de fuga de datos o conocimiento de los mismos sin consentimiento de su titular prácticamente radica en los grandes ficheros. El problema, en todo caso, estaría en determinar la formula a desarrollar y los criterios que deban imponerse a efectos de distinguir entre los ficheros en los que se hace precisa la inscripción, de aquellos otros en que la misma no es necesaria.

Sería igualmente importante a efectos de lograr una perfecta correlación entre los ficheros inscritos en el Registro General y la realidad social que, al igual que se regula en la legislación inglesa, las inscripciones en el citado organismo se actualicen a través de la obligación de renovar las inscripciones en el Registro cada cierto periodo de tiempo. Ello conduciría a una casi permanente actualización del Registro General evitando de esta forma que se pudiera incurrir en el incumplimiento de lo establecido en el artículo 4.2. de la Ley Orgánica.

El tema de la seguridad física y lógica de determinados ficheros, y con ello la posibilidad de evitar que se produzcan fugas de datos que pudiesen desvirtuar la finalidad de los mismos, además de evitar un ataque a la intimidad de las personas en ellos incluidas, presenta problemas importantes en cuanto a su funcionamiento. Bien es cierto que los denominados ficheros de cumplimiento o incumplimiento de obligaciones dinerarias presentan una serie de especialidades que ya se han comentado con anterioridad. Ahora nos estamos refiriendo, ya que así se ha detectado en los pocos meses de actuación de la Inspección de Datos en 1994, a la utilización indebida de datos de esta naturaleza por parte de personas o entidades que o se dedican a emitir informes comerciales o pretenden conocer la situación de incumplimiento de la obligación de pago con la finalidad de ofrecer sus servicios de mediación en la cancelación del dato personal del fichero correspondiente. Una y otra actividad tienen como elemento común el que son totalmente ajenas a la actividad de crédito que caracteriza y debería ser requisito indispensable para poder participar del uso del citado fichero. En este sentido la expresión contenida en el artículo 28.1 de la Ley Orgánica de **datos facilitados por el acreedor o quien actúe por su cuenta o interés** debe ser el único instrumento interpretativo válido de forma que solamente pueden participar en dichos ficheros aquellas personas que detenten la posición real de acreedor en el cumplimiento de una obligación dineraria. Dicho de otra forma, nadie que no tenga dicha condición puede acceder al contenido del fichero por muy lícita que sea la actividad que desempeñe, ya que la ausencia del consentimiento previo por parte del afectado se justifica exclusivamente por la condición de acreedor y no por ninguna más.

Pues bien, establecido el funcionamiento de estos ficheros de la forma anteriormente expuesta toda falta de seguridad en el tratamiento de los datos que produzca un conocimiento indebido por parte de quien no ostente la condición de acreedor deberá ser severamente investigada y sancionada ya que de por sí encierra todos y cada uno de los peligros que la Ley Orgánica trata de reprimir: tráfico ilegal del dato, no actualización del mismo y posibilidad de almacenar datos que por hallarse fuera de los canales de actualización del mismo sean inexactos desde el inicio del tratamiento con posibilidad de mantenerse en esa situación de irregularidad durante un periodo dilatado de tiempo con los consiguientes perjuicios que puede sufrir el ciudadano en concreto como consecuencia de dicha situación.

MEMORIA DE 1994 - ANEXOS

ANEXO I

PROYECTOS DE DISPOSICIONES LEGALES SOMETIDOS A INFORME DE LA AGENCIA DE PROTECCIÓN DE DATOS

PROYECTO DE DISPOSICIÓN/SOLICITADO POR/FECHA SOLICITUD

- Proyecto de Real Decreto por el que se aprueban las normas de acceso que han de regir en la distribución pública de información catastral cartográfica y alfanumérica por la Dirección General del Centro de Gestión Catastral y Coopera - ción Tributaria.
Solicitado por : Subsecretario del **Ministerio de Economía y Hacienda.**
Fecha solicitud: 20-10-1993

- Anteproyecto de Ley Orgánica de reforma de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
Solicitado por : Subsecretaria del **Ministerio de Justicia.**
Fecha solicitud: 3-11-1993

- Proyecto de Orden Ministerial sobre creación del fichero automatizado de datos de carácter personal (sistema de información sobre los usuarios de servicios sociales: S.I.U.S.S.).
Solicitado por : Secretario General Técnico del **Ministerio de Asuntos Sociales.**
Fecha solicitud: 4-11-1993

- Anteproyecto de Real Decreto-Ley por el que se prorroga la entrada en vigor de la disposición adicional segunda de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
Solicitado por : Secretario General Técnico del **Ministerio de Justicia.**
Fecha solicitud: 8-11-1993

- Proyecto de Orden de la Consejería de Sanidad de la Junta de Comunidades de Castilla-La Mancha por la que se pretende autorizar la sustitución de libro foliado por sistema informático en el Registro de Ingresos y Altas Hospitalarias.
Solicitado por : Secretario General Técnico de la **Junta de Comunidades de Castilla-La Mancha.**
Fecha solicitud: 25-1-1994

- Proyecto de Real Decreto por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automa-tizado de los datos de carácter personal.
Solicitado por : Subsecretaria del **Ministerio de Justicia.**
Fecha solicitud: 7-3-1994

- Proyecto de Ley de reforma parcial de la Ley General Tributaria.
Solicitado por : Secretario General Técnico del **Ministerio de Justicia e Interior.**
Fecha solicitud: 7-9-1994

- Proyecto de Orden de regulación de los ficheros automatizados del Instituto Nacional de Estadística que caen en el ámbito de la Ley de regulación del tratamiento automatizado de datos de carácter personal.
Solicitado por : Presidente del **Instituto Nacional De Estadística, Del Ministerio De Economía Y Hacienda.**
Fecha solicitud: 8-7-1994

- Proyecto de Orden Ministerial de regulación de las bases de datos y ficheros automatizados de la Agencia Estatal de Administración Tributaria.
Solicitado por : Director del Servicio Jurídico de la **Agencia Estatal de Administración Tributaria, del Ministerio de Econo-mía y Hacienda.**
Fecha solicitud: 12-7-1994

- Anteproyecto de Ley de Incompatibilidades de los Miembros del Gobierno de la Nación y de los Altos Cargos de la Administración del Estado.
Solicitado por : Secretario General Técnico del **Ministerio de Justicia e Interior.**
Fecha solicitud: 19-10-1994

- Proyecto de Ley de medidas fiscales, administrativas y del orden social.
Solicitado por : Ministro de la **Presidencia.**
Fecha solicitud: 31-10-1994

- Anteproyecto de Ley de tratamiento automatizado de datos de la Comunidad Autónoma de Aragón.
Solicitado por : Consejero de Presidencia y Rela-ciones Institucionales del **Gobierno de Aragón.**
Fecha solicitud: 17-11-1994

- Proyecto de Ley de modificación parcial de la Ley General Tributaria.

Solicitado por : Director General de Tributos del **Ministerio de Economía y Hacienda.**
Fecha solicitud: 5-12-1994

ANEXO II

CÓDIGO TIPO "APLICACIÓN EN TELEFÓNICA DE LA LEY ORGÁNICA REGULADORA DEL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL"

1. INTRODUCCIÓN

La Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de datos de carácter personal, que entró en vigor el 31 de Enero de 1993, ha venido a desarrollar el art. 18.4 de la Constitución, estableciendo las garantías que deben adoptar los titulares de ficheros automatizados con datos de carácter personal para que el uso generalizado de la informática no atente contra el honor y la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Como titular de ficheros automatizados de titularidad privada que contienen datos de carácter personal, Telefónica de España S.A. se encuentra afectada por la aplicación de esta Ley. Además, tiene suscritos gran número de contratos de entrega de datos de personas físicas para su tratamiento automatizado, así como publicados repertorios de servicios de telecomunicación, derivándose de estas actividades diversas obligaciones para la Compañía, establecidas en la referida Ley.

Telefónica, con el fin de ceñirse en su gestión a la más estricta legalidad, ha adoptado, mediante decisión de empresa, el **código deontológico** previsto en el art. 31 de la Ley, el cual establece:

a) Las condiciones de integridad y seguridad que deben tener los ficheros de Telefónica que contienen datos personales, así como los centros de tratamiento, equipos, sistemas y locales en que se ubiquen aquéllos.

b) Los responsables operativos internos de los ficheros.

c) Las condiciones y requisitos para la creación de nuevos ficheros.

d) Las medidas a adoptar en los supuestos de entrega o cesión de datos a un tercero, con especial tratamiento de las solicitudes de datos recibidas de organismos judiciales y administrativos.

e) El procedimiento para dar cumplimiento a las obligaciones que corresponden a Telefónica en relación con la Agencia de Protección de Datos y el Registro General de Protección de Datos.

f) La atención al ejercicio de los derechos que corresponden a los afectados por esta Ley, cuyos datos personales obren en los ficheros de la empresa: abonados, empleados, contratistas, proveedores, suministradores, o profesionales colaboradores.

El presente Código-tipo ha sido objeto de desarrollo por medio de una normativa interna, que articula las prescripciones de la Ley Orgánica en los diversos procesos de gestión empresarial de forma unitaria y homogénea.

2. UNIDADES AFECTADAS

Este Código-tipo es de obligado cumplimiento para todas las Unidades de la Empresa, y en particular para aquéllas que intervienen en la recogida, tratamiento y entrega de 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.

3. DEFINICIONES

A efectos del presente Código-tipo, se considera fichero automatizado todo conjunto organizado de datos de carácter personal, centralizado o repartido en diversos emplazamientos, que sea objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Por **tratamiento automatizado** se entienden las operaciones y procedimientos técnicos que permiten la recogida, grabación, conservación, elaboración, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, cotejo o interconexión, así como su bloqueo o cancelación.

Por **datos de carácter personal** se entiende toda información numérica, alfabética, gráfica, fotográfica, acústica o de

cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión, concerniente a personas físicas identificadas o identificables (nombre, apellidos, estado civil, D.N.I., sexo, edad, domicilio, número de afiliación a la Seguridad Social, número de matrícula del empleado...).

Por **responsable operativo interno** del fichero se entiende la persona física que decide acerca de la finalidad, contenido y uso del tratamiento, garantizando la integridad y confidencialidad del fichero, y determinando los controles que deben aplicarse para proteger la información.

Por **depositario** del fichero se entiende el área autorizada para mantener y procesar la información (normalmente el área informática), que tiene la responsabilidad de aplicar controles técnicos y organizativos que aseguran el tratamiento y residencia de la información contenida en los ficheros.

Por **afectado** se entiende: empleados, abonados, proveedores, suministradores, profesionales y contratistas que sean personas físicas.

Las presentes definiciones no contradicen a las efectuadas, en su caso, en el artículo 3 de la propia Ley Orgánica y en el artículo 1 del Reglamento de desarrollo de la misma.

4. RESPONSABLES DE LOS FICHEROS AUTOMATIZADOS CON DATOS DE CARÁCTER PERSONAL

Telefónica, a efectos internos de gestión y organización empresariales, ha designado un **responsable operativo interno** de cada fichero, cuyas obligaciones son las siguientes:

- Vigilar el contenido y el uso del tratamiento automatizado.
- Autorizar las personas y Unidades que, de acuerdo con las necesidades de gestión, puedan acceder a la información.
- Vigilar el cumplimiento de las medidas de seguridad establecidas.
- Guardar el secreto profesional respecto de los datos del fichero.
- Informar a las Unidades competentes de la creación, modificación y cancelación, en su caso, del fichero.

5. SEGURIDAD DE LOS DATOS Y FICHEROS

Los locales, equipos, sistemas y ficheros titularidad de Telefónica con datos afectados por la Ley 5/1992 deberán cumplir las condiciones de seguridad e integridad establecidas en la Plan de Seguridad de la Información de Telefónica.

Para una mayor garantía de cumplimiento de las exigencias de confidencialidad y seguridad de los datos obrantes en los ficheros titularidad de Telefónica, se establecen unas medidas organizativas de carácter general consistentes en:

- Clasificación de la Información Personal en el Grado de Confidencial.
- Identificación del Responsable, Depositario y Usuario de los Ficheros con datos personales.
- Mantenimiento del Inventario de ficheros con datos de carácter personal.
- Procedimiento formal para solicitud de Autorizaciones de Acceso, dirigidas al Responsable.
- Instrucción técnica de "Estándares de Seguridad para tratamiento de Información Confidencial".
- Formación y concienciación del personal de Telefónica en las exigencias de la LORTAD.
- Auditoría periódica de la confidencialidad de Ficheros con datos de carácter personal y persecución de infracciones.

5.1. DEBER DE SECRETO DE LOS EMPLEADOS QUE INTERVIENEN EN CUALQUIER FASE DEL TRATAMIENTO

Aquellos empleados que intervengan en cualquier fase del tratamiento de datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, subsistiendo estas obligaciones aún después de haber finalizado su relación con Telefónica, o haber cambiado de función o acoplamiento en la misma, todo ello además de acuerdo con lo previsto en el Convenio Colectivo.

La violación de este deber de secreto tendrá la consideración de falta laboral muy grave dando lugar a la aplicación de la Normativa sobre Régimen Disciplinario, sin perjuicio de otras responsabilidades a que hubiera lugar.

5.2. ACCESO DE LOS EMPLEADOS A LOS FICHEROS AUTOMATIZADOS DE DATOS RESERVADOS DE CARÁCTER PERSONAL

Únicamente podrán acceder a estos ficheros y obtener datos de carácter personal obrantes en los mismos las personas especialmente autorizadas para ello por la Alta Dirección de la Compañía o por el responsable operativo interno del fichero.

6. CONDICIONES PARA LA CREACIÓN DE NUEVOS FICHEROS

Podrán crearse ficheros automatizados que contengan datos de carácter personal cuando resulte necesario para la

actividad de la Unidad correspondiente y siempre que no se efectúe con finalidad distinta de la que constituye el objeto social de Telefónica.

En todo caso, la creación de nuevos ficheros de esta naturaleza deberá ser autorizada en el momento de la aprobación del Sistema Informático en el que residan por la Alta Dirección o por los directivos de Telefónica competentes para ello.

Los ficheros creados por empleados con fines personales (agendas de trabajo, etc...) estarán sujetos a la obligación de garantía de la confidencialidad de la información de carácter personal que contengan.

En cualquier caso, queda terminantemente prohibida la creación de ficheros automatizados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual. La infracción de esta prohibición es constitutiva de falta laboral muy grave.

7. RECOGIDA, UTILIZACIÓN, CONSERVACIÓN Y CANCELACIÓN DE LOS DATOS

La recogida de los datos de carácter personal, así como su uso, tratamiento automatizado, conservación y cancelación se realizará conforme a lo que se dispone en los apartados siguientes.

7.1. RECOGIDA DE LOS DATOS

Los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y los fines para los que se han obtenido, no pudiendo recogerse por medios fraudulentos, desleales o ilícitos.

Se requerirá el consentimiento del afectado para la recogida y el tratamiento automatizado de sus datos personales, excepto cuando los datos se recojan de fuentes accesibles al público, o cuando se requieran por motivo de una relación negocial, laboral o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento de un contrato.

El consentimiento podrá ser revocado por el afectado cuando exista causa justificada para ello, sin que tenga efectos retroactivos.

No obstante no será necesario el consentimiento del afectado cuando sus datos de carácter personal se recojan y traten con la finalidad de dar cumplimiento a mandamientos judiciales (observaciones legales de las telecomunicaciones, etc...).

Asimismo los datos deberán ser exactos, y actualizarse cuando sea necesario, de forma que respondan con veracidad a la situación real del afectado.

Si los datos de carácter personal registrados resultaran inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos por los correspondientes datos rectificados o completados.

Los datos de carácter personal que hagan referencia a la salud sólo podrán ser recabados y tratados automatizadamente cuando por razones de interés general así lo disponga una Ley, el afectado consienta expresamente, o bien cuando su obtención y tratamiento se realice para el correcto cumplimiento de la función de Telefónica como empresa colaboradora en la gestión del Régimen General de la Seguridad Social.

Los profesionales de Telefónica directamente relacionados con la salud de los empleados pueden tratar automatizadamente los datos de carácter personal relativos a la salud de las personas que a ellos acudan, de acuerdo con lo dispuesto en las Leyes sanitarias.

7.2. UTILIZACIÓN DE LOS DATOS

Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquéllas para las que hubieran sido recogidos.

Sólo se utilizarán de forma automatizada datos de carácter personal en las encuestas de opinión, trabajos de prospección de mercados, investigación científica o similares, si hubieran sido previamente sometidos a un procedimiento de disociación que los prive de su nexo con una persona concreta; o si el afectado hubiera prestado libremente su consentimiento previo, en cuyo caso podrá utilizarse el fichero original no disociado, no pudiéndose utilizar en ningún caso los datos con finalidad distinta a aquélla para la que se recabaron.

7.3. CONSERVACIÓN Y CANCELACIÓN DE LOS DATOS

Los datos serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

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. No obstante, el plazo de conservación

dependerá de la relación contractual existente entre Telefónica y el afectado, manteniéndose conservados, con carácter general, como mínimo mientras subsiste aquélla, y como máximo por los plazos siguientes:

- Quince años para los datos de abonados o clientes (artículo 1.964 del Código Civil).
- Seis años para los datos de proveedores o suministradores (artículo 30 del Código de Comercio).
- Permanentemente para los datos de empleados o ex-empleados, a fin de no causarles perjuicios en el supuesto de futuras solicitudes de prestaciones a la Seguridad Social.

La cancelación de los datos se realizará de oficio por el responsable del fichero por haber finalizado el plazo de conservación, o a instancia del afectado en ejercicio de su derecho de cancelación, tal como dispone el apartado 8 de este Código-tipo.

La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros, o cuando existiese obligación de conservarlos, según se establece en el artículo 15.4 de la LORTAD.

8. EJERCICIO DE LOS DERECHOS POR LOS AFECTADOS

Cuando las personas físicas titulares de los datos que son objeto del tratamiento automatizado (abonados, empleados, contratistas, proveedores, suministradores y profesionales colaboradores) ejerciten los derechos que les corresponden se actuará de acuerdo con el procedimiento establecido en el apartado 8.2 de este Código-tipo.

8.1. DERECHOS DE LOS AFECTADOS

a) Derecho de información en la recogida de datos

El afectado tiene derecho a ser informado de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección laboral del responsable del fichero.

Asimismo se le informará del carácter obligatorio o facultativo de su respuesta, de las consecuencias de la obtención de sus datos, de su negativa a suministrarlos, así como de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación. No obstante no será necesaria esta información, cuando el contenido de la misma se deduzca claramente de la naturaleza de los datos personales que se solicitan en el momento de la contratación.

b) Derecho de acceso

El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados, excepto en los casos en que la confidencialidad de la información sea necesaria para la salvaguardia de actuaciones judiciales de carácter personal.

c) Derecho de rectificación y cancelación

El afectado tiene derecho a solicitar la rectificación de sus datos personales inexactos, incompletos, inadecuados o excesivos, o la cancelación de los mismos, en su caso.

d) Derecho de exclusión de los repertorios de servicios de telecomunicación

Los abonados pueden solicitar que se excluyan en los repertorios de abonados de acceso al público los datos sobre su número de abono y demás datos complementarios.

8.2. PROCEDIMIENTO DE EJERCICIO

Como regla general, y tratándose de derechos personalísimos, únicamente el afectado puede ejercerlos. Podrá, no obstante actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le impida el ejercicio personal de los mismos. En relación con los ficheros titularidad de Telefónica, se facilitará este ejercicio de acuerdo con el procedimiento que se establece a continuación.

a) b) y c) Derechos de acceso, rectificación y cancelación

El ejercicio del derecho de acceso tendrá carácter gratuito y se permitirá mediante petición o solicitud del afectado por cualquier medio que garantice la identificación del mismo, en la que conste el fichero a consultar. Se informará al afectado que no podrá volver a hacer uso de este derecho hasta transcurridos doce meses. No obstante, excepcionalmente, cuando se acredite un interés legítimo para ello, se podrá ejercitar nuevamente el derecho de acceso antes de que transcurra el referido período de doce meses. A efectos de control de este plazo, la Unidad correspondiente deberá

dejar constancia de la fecha de ejercicio de este derecho.

La petición de acceso se resolverá, por el responsable operativo interno del fichero o mando en el que haya delegado este trámite, en el plazo máximo de un mes, a contar desde la recepción de la solicitud, y si la resolución fuera estimatoria, el acceso a los datos se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla. Si la petición fuese desestimada o hubiese transcurrido el plazo de un mes citado sin respuesta, el afectado puede reclamar ante la Agencia de Protección de Datos.

Como regla general, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado, o la información se refiera a actuaciones penales (observación de las comunicaciones) y hasta tanto dure la intervención de las comunicaciones o, en su caso, el secreto sumarial.

El acceso a los datos se realizará, a voluntad del afectado y siempre que la configuración del fichero lo permita, mediante: visualización en pantalla, entrega de escrito, copia o fotocopia en que se reflejen los mismos remitida por correo, o mediante telecopia.

En los supuestos de petición de duplicado de facturación detallada por el titular del abono se le entregará a éste personalmente en la Oficina de Abonados correspondiente. Cuando los datos sean solicitados por persona autorizada distinta del titular, debidamente acreditada, la petición se realizará por escrito, y se enviará la información por correo al titular.

La información comprenderá los datos de base del abonado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación del uso o finalidad para los que se almacenaron los datos.

El ejercicio de los derechos de **rectificación y cancelación** de datos erróneos, inexactos, incompletos, inadecuados o excesivos, será gratuito y requerirá siempre **escrito** del afectado en el que solicite la rectificación o cancelación de sus datos y en el que también debe constar su D.N.I.

Para atender y tramitar las solicitudes de ejercicio de estos derechos por los afectados serán competentes:

- Si se ejercitan por los abonados: las Oficinas Comerciales correspondientes.
- Si se ejercitan por empleados: las Unidades de Relaciones Laborales.
- Si se ejercitan por los contratistas, proveedores, suministradores o profesionales colaboradores: las Unidades Provinciales de Intervención correspondientes, o el Dpto. de Intervención General, en su caso.
- Si se ejercitan por titulares de activos financieros: el Dpto. de Tesorería.

La rectificación o cancelación se hará efectiva dentro de los cinco días siguientes al de la recepción de la solicitud. En igual plazo se comunicará motivadamente la denegación de la solicitud al afectado, cuando así proceda.

Si los datos, rectificados o cancelados hubieran sido cedidos a un tercero, deberá notificarse a éste último la rectificación o cancelación efectuada en el plazo señalado de cinco días desde que se recibió la solicitud de aquéllas.

En el caso de que las Unidades señaladas no tuvieran acceso al fichero en que se encuentran los datos del afectado, se canalizará la solicitud de ejercicio al directivo responsable operativo interno del fichero.

d) Derecho de exclusión de los repertorios de servicios de telecomunicación

El ejercicio de este derecho de exclusión de los repertorios de servicios de telecomunicación por los abonados, se tramitará en la Oficina Comercial correspondiente, de forma gratuita, según el procedimiento establecido en la normativa interna.

9. ENTREGA DE DATOS DE CARÁCTER PERSONAL A TERCEROS PARA LA PRESTACIÓN DE SERVICIOS DE TRATAMIENTO AUTOMATIZADO

La entrega de datos de carácter personal a terceros para su tratamiento automatizado se realizará siempre en virtud de una relación contractual entre Telefónica y el tercero, sin que los datos se puedan aplicar o utilizar con finalidad distinta a la que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas.

Para garantizar la confidencialidad de los datos personales entregados, se incorporarán en todo contrato a este fin cláusulas-tipo específicas que garanticen la confidencialidad.

Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos. No obstante, si Telefónica presume la posibilidad de ulteriores encargos al tercero prestador del servicio, podría admitir el almacenamiento de los datos, por este último, con las debidas garantías de seguridad, por un período máximo de cinco años.

Con carácter general no se permitirá la subcontratación en los contratos que conllevan entrega de datos de carácter personal a un tercero, salvo en los casos en que sea absolutamente necesario.

10. CESIÓN DE DATOS

Se entiende por cesión de datos: 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 datos realizada por una persona distinta de la afectada.

Con carácter general, Telefónica no cederá datos personales a terceros, excepto en los casos siguientes:

a) La cesión realizada a organismos judiciales y administrativos, de conformidad con las diferentes leyes aplicables (Ley IRPF, Ley Seguridad Social, etc.), pero siempre en el ejercicio de las funciones que tienen atribuidas dichos organismos y en los supuestos y condiciones establecidos en el apartado 11 de esta norma.

b) La cesión de datos personales de empleados realizada a los representantes sindicales en cumplimiento de la Ley Orgánica 11/1985, de 2 de Agosto, de Libertad Sindical; y de la Ley 2/1991 de 7 de Enero, sobre derecho de información de los representantes de los trabajadores en materia de contratación.

c) La cesión de datos de carácter personal de los empleados adheridos al Plan de Pensiones que la Comisión de Control realice a la Entidad Gestora del Plan de Pensiones, para su utilización por ésta exclusivamente a los fines previstos en la Ley 8/87, de 8 de Junio, de regulación de los Planes y Fondos de Pensiones.

d) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado, o para realizar los estudios epidemiológicos en los términos establecidos en la Ley 14/1986, de 25 de Abril, General de Sanidad y disposiciones complementarias.

e) Cuando la cesión se efectúe previo procedimiento de disociación, es decir, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

En todos los casos se requerirá que la cesión sea autorizada por el responsable operativo interno del fichero.

Cualquier otra cesión distinta de las mencionadas deberá ser autorizada por la Alta Dirección, siendo preciso, además, obtener previamente el consentimiento del afectado y notificarle la cesión efectuada. El consentimiento del afectado deberá recaer siempre sobre un cesionario determinado o determinable.

Si el consentimiento otorgado por el afectado para la cesión de sus datos fuera revocado, se tomarán las medidas oportunas, para que no se efectúen cesiones de sus datos en el futuro. Se exigirá en todo caso que la revocación conste por escrito.

La cesión deberá notificarse a la Agencia de Protección de Datos, en los impresos oficiales existentes al efecto.

11. SOLICITUD DE INFORMACIÓN DE DATOS DE CARÁCTER PERSONAL POR AUTORIDADES JUDICIALES Y ADMINISTRATIVAS

La información sobre datos de carácter personal obrantes en ficheros automatizados de Telefónica, que puede afectar, tanto a abonados, como a empleados o a contratistas y proveedores, será comunicada a autoridades judiciales y administrativas, dentro del procedimiento legalmente establecido con sujeción a las reglas que se exponen a continuación.

No se atenderán peticiones de información sobre datos de carácter personal formuladas genéricamente o de forma indiscriminada, cualquiera que sea el procedimiento en que se acuerde o el órgano que lo solicitase.

Las informaciones solicitadas por órganos gubernativos directamente relacionados con actuaciones preparatorias o complementarias de procesos judiciales, sólo podrán ser facilitadas cuando conste claramente la intervención de órgano judicial concreto.

a) Organismos Judiciales

Tratándose de jurisdicción penal, se facilitarán los datos solicitados en cualquier caso.

Tratándose de cualquier otra jurisdicción distinta, se informará en todo caso de los datos de abonados, en la medida en que los datos interesados figuren en repertorios de los abonados a servicios de telecomunicación (nombre, domicilio, número de abono y actividad). No se informará de los datos que no figuren en los repertorios antes mencionados, salvo que proceda lo contrario con arreglo a derecho (Diligencias para mejor proveer, resolución expresa de ser fundamental para dictar sentencia y supuestos en que se pida el dato a instancia de la parte a quien se refiere lo interesado).

b) Organismos administrativos

Se informará de los datos personales de abonados en la medida en que estos datos figuren en los repertorios de

abonados a servicios de telecomunicación.

En cuanto a los datos que no figuran en los repertorios, sólo se facilitarán en los siguientes supuestos:

- Cuando la solicitud haya sido presentada por la Inspección Tributaria, la Agencia Estatal Tributaria o las oficinas recaudatorias de las Haciendas Locales, en virtud de lo establecido en los arts. 111 y 112 de la Ley General Tributaria, y el art. 37 del Reglamento General de Inspección de Tributos, y siempre que la información solicitada tenga trascendencia tributaria.

- Cuando la solicitud sea presentada por el Instituto Nacional de la Seguridad Social o cualquiera de sus Agencias, en el ejercicio de su potestad recaudatoria.

- Cuando la solicitud de datos se presente basada en la Ley 12/1989, de 12 de Mayo, sobre función estadística pública para la elaboración de estudios de este carácter.

12. MOVIMIENTO INTERNACIONAL DE DATOS

Se entiende por transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

No podrán realizarse transferencias temporales o 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 al que presta la Ley Orgánica 5/1992, de 29 de Octubre en España, sin perjuicio de lo dispuesto en el apartado 10 de este Código-tipo.

No será de aplicación lo dispuesto en el párrafo anterior en los casos siguientes:

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

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

c) Cuando la 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.

El acceso por las operadoras telefónicas de otros países a la Base de Datos del Servicio de Información 003 de Telefónica, no tiene la consideración de movimiento internacional de datos, al realizarse exclusivamente abonado a abonado.

Si en el futuro se realizase una transferencia de datos personales a un país que no tenga el nivel de protección adecuado, se solicitará la autorización previa del Director de la Agencia de Protección de Datos, con posterior notificación a la misma en el impreso oficial correspondiente.

13. NOTIFICACIÓN E INSCRIPCIÓN REGISTRAL DE LOS FICHEROS

Telefónica, a través de la Unidad competente, ha tramitado antes del 31 de Julio de 1994 ante la Agencia de Protección de Datos la inscripción de los ficheros automatizados de datos de carácter personal existentes en la Empresa en el Registro General de Protección de Datos, mediante la presentación de modelos normalizados en soporte informático.

Asimismo tramitará la inscripción de los que se creen en el futuro y comunicará igualmente las modificaciones que se produzcan en los ficheros, la supresión de alguno de ellos o las cesiones o transferencias de datos, en su caso, a la Agencia de Protección de Datos en los modelos oficiales correspondientes.

14. RELACIONES CON LA AGENCIA DE PROTECCIÓN DE DATOS

Las relaciones de Telefónica con la Agencia de Protección de Datos se llevarán de forma centralizada por el Dpto. de Ordenación y Gestión Jurídico-Administrativa, sin perjuicio de la colaboración de los Departamentos que proceda.

En este sentido, la Unidad de Telefónica que reciba aviso de inspección o solicitud de información de la Agencia de Protección de Datos, lo comunicará inmediatamente al Dpto. de Ordenación y Gestión Jdco.-Admva., enviándole copia del escrito recibido de la Agencia, así como información sobre los extremos solicitados por esta última. El citado Departamento, remitirá la contestación que proceda a este Organismo a la mayor brevedad.

15. EFECTIVIDAD

El presente Código-tipo será de aplicación en Telefónica a partir de la fecha de su inscripción en la Agencia de Protección de Datos.

La adaptación de las condiciones de seguridad de los locales, equipos, sistemas y ficheros con datos personales, dado

que requiere la adopción de medidas técnicas complejas, se llevará a cabo paulatinamente dentro del Plan de Seguridad de la Información de Telefónica y, en todo caso, antes de que transcurra el plazo marcado en la disposición transitoria única de dicha Ley.

En Madrid, a 31 de Octubre de 1994

ANEXO III

TEXTO DE LA POSICIÓN COMÚN DEL CONSEJO DE LA UNIÓN EUROPEA SOBRE LA PROPUESTA MODIFICADA DE DIRECTIVA MARCO DE PROTECCIÓN DE DATOS, APROBADA POR EL CONSEJO EL 20 DE FEBRERO DE 1995 (INCLUIDO TEXTO A DOBLE COLUMNA DE LA DIRECTIVA Y LA LEY ORGÁNICA 5/1992)

DIRECTIVA 95/ / CEE DEL PARLAMENTO EUROPEO Y DEL CONSEJO
de
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

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, su artículo 100 A,
Vista la propuesta de la Comisión (1)
Visto el dictamen del Comité Económico y Social (2)
De conformidad con el procedimiento establecido en el artículo 189 B del Tratado (3)

(1) DO nº C 277 de 5.11.1990, p. 3. y DO nº C 311 de 27.11.92, p. 38
(2) DO nº 159 de 17.6.1991, p.38
(3) Dictamen del Parlamento Europeo de (no publicado aún en el Diario Oficial)
Posición común del Consejo de (no publicada aún en el Diario Oficial) y
Decisión del Parlamento Europeo de (no publicada aún en el Diario Oficial)

(1º) Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el proceso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de estos pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;

(2º) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;

(3º) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas;

(4º) Considerando que, en los diferentes sectores de actividad económica y social, se recurre cada vez más en la Comunidad al tratamiento de datos personales; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos;

(5º) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones en nombre de las administraciones de otros Estados miembros, en el contexto del espacio sin fronteras que supone el mercado interior;

(6º) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;

(7º) Considerando que la diferencia entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, puede impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, esta

diferencia puede constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia y dificultar la misión de las administraciones que intervienen en el ámbito de aplicación del Derecho comunitario; que este diferencia en los niveles de protección se debe a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;

(8º) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta en particular las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

(9º) Considerando que, en razón de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos de carácter personal por motivos de protección de los derechos y libertades de las personas físicas, y en particular del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que estos podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de los datos; que, al actuar así, los Estados miembros se procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la Directiva, y que ello podrá tener repercusiones en la circulación de los datos tanto en el interior de un Estado miembro como en la Comunidad;

(10º) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho a la intimidad reconocido en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

(11º) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;

(12º) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por un persona física en el ejercicio de actividades exclusivamente personales o domésticas, por ejemplo a la correspondencia y a la llevanza de un repertorio de direcciones;

[Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión consideran que con miras a una aplicación coherente y homogénea de las normas de protección dentro de la Unión, los tratamientos efectuados por las Instituciones y Organismos de la Unión Europea, deberían estar sometidos a los mismos principios de protección previstos por la presente Directiva. - Francia considera que la declaración adicional al Considerando 12º, referente a los tratamientos efectuados por las Instituciones y Organismos de la Unión Europea no se refiere a los tratamientos instaurados en aplicación del Título IV del Tratado de la Unión Europea"]

(13º) Considerando que las actividades a que se refieren los Títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no son materia del ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado;

(14º) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos de sonido e imagen relativos a las personas físicas constituidas por sonidos e imágenes, la presente Directiva debe aplicarse a los tratamientos que afectan a dichos datos;

(15º) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un registro estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;

(16º) Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no son materia del ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no son materia del ámbito de aplicación del Derecho

comunitario;

(17º) Considerando que en lo que respecta a los tratamientos de sonido e imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en el artículo 9;

(18º) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter los tratamientos efectuados por cualquier persona que trabaje bajo la autoridad del responsable del tratamiento en un Estado miembro a la aplicación de la legislación de tal Estado;

(19º) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante la instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un solo responsable se establezca en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;

(20º) Considerando que el hecho de que el responsable del tratamiento está establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos los tratamientos deben regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;

(21º) Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal;

(22º) Considerando que los Estados miembros precisarán en su legislación o en la aplicación de las disposiciones adoptadas en virtud de la presente Directiva las condiciones generales de licitud de los tratamientos; que, en particular, junto a los artículos 7 y 8, el artículo 5 ofrece a los Estados miembros la posibilidad de prever, independientemente de las normas generales, condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos contemplados en el artículo 8;

(23º) Considerando que los Estados miembros están facultados a garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas contra el tratamiento de los datos de carácter personal como mediante leyes sectoriales como las relativas a los institutos estadísticos;

(24º) Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;

(25º) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos - obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de tales datos, de poder acceder a ellos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias;

(26º) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente aplicados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales pueden hacerse anónimos y conservarse en forma que no haga posible identificar ya al interesado;

(27º) Considerando que la protección de los individuos debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular , el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a los individuos, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjunto de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no pertenecen en ningún caso al ámbito de aplicación de la presente Directiva;

(28º) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse en particular a datos pertinentes y no excesivos en relación con los objetivos perseguidos; estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos, que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados;

(29º) Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos, no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros otorguen las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones relativas a cualquier individuo concreto;

(30º) Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en cuestión, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;

(31º) Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;

(32º) Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;

(33º) Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales;

(34º) Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a garantía de la calidad y a la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;

[Declaración a incluir en el Acta del Consejo:" El Consejo y la Comisión manifiestan que los elementos que se recogen en el Considerando 34 de la Directiva, y que principalmente tienen por objeto aclarar la noción de interés público que figura en los artículos 7 y 8 de la Directiva, están vinculados a la motivación de esta y, en tal sentido, son parte integrante de este acto jurídico; de ello resulta que tales elementos deberán ser tomados en consideración por los Estados miembros cuando adoptaren las disposiciones legislativas, reglamentarias y administrativas necesarias para ajustarse a la Directiva en cuestión"]

(35º) Considerando que, además, el tratamiento de datos personales por parte de las autoridades públicas con fines establecidos en el Derecho Constitucional o el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;

(36º) Considerando que si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;

(37º) Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar información, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control. Esto no debería inducir, sin embargo, a los Estados miembros a prever excepciones de las medidas que garanticen la seguridad del tratamiento. Igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales;

(38º) Considerando que el tratamiento leal de datos supone que los interesados deban estar en condiciones de conocer la existencia de los tratamientos y beneficiarse de los mismos cuando los datos se obtengan de ellos a partir de una

información precisa y completa respecto a las circunstancias de dicha obtención;

(39º) Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente de la persona afectada; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos ante la persona afectada; que en todos estos supuestos, debe informarse a la persona afectada en el momento del registro los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero;

(40º) Considerando que además esta obligación no está prevista si la persona afectada ya está informada, si el registro o la comunicación están expresamente previstos por ley o si resulta imposible informarle, o implicara esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de personas afectadas, la antigüedad de los datos, y las posibles medidas compensatorias;

(41º) Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse en particular de su exactitud y de la licitud de su tratamiento; considerando que por las mismas razones cualquier persona debe tener además el derecho a conocer la lógica que subyace al tratamiento automatizado de los datos que le conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este último derecho no debe menoscabar la propiedad intelectual y en particular el derecho de autor que proteja el "software"; que no obstante esto no debe suponer que se deniegue cualquier información de la persona afectada;

(42º) Considerando que, en interés de la persona de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán , por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda ejercerse a través de un profesional de la medicina;

(43º) Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la seguridad pública, el orden público o intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como investigaciones y acciones penales y violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa;

(44º) Considerando que los Estados miembros podrán verse obligados, en virtud de las disposiciones del Derecho comunitario, a establecer excepciones a las disposiciones de la presente Directiva relativas al derecho de acceso, la información de personas y la calidad de los datos para garantizar algunas de las finalidades contempladas más arriba;

(45º) Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias;

(46º) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y del coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;

(47º) Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de este tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;

(48º) Considerando que los procedimientos de notificación tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(49º) Considerando que para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que se precisen los límites; que se puede igualmente disponer la exención o la simplificación cuando un encargado, nombrado por el responsable del tratamiento, se cerciore de que los tratamientos efectuados no pueden atentar contra los derechos y libertades de los interesados; que dicho encargado, sea o no empleado del responsable del tratamiento

de datos, deberá ejercer sus funciones con una independencia total;

(50º) Considerando que se podrá disponer la exención o la simplificación para los tratamientos cuya única finalidad sea el mantenimiento de registros destinados, según el Derecho nacional, a la información del público y que sean accesibles para la consulta del público o de toda persona que justifique un legítimo interés;

(51º) Considerando que, no obstante, el beneficio de la simplificación o de la exención de la obligación de notificación no dispensa al responsable del tratamiento de ninguna de las demás obligaciones derivadas de la presente Directiva;

(52º) Considerando que, en este contexto, el control a posteriori por parte de las autoridades competentes debe considerarse, en general, una medida suficiente;

(53º) Considerando que, no obstante, determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, o por el uso particular de una tecnología nueva; que es competencia de los Estados miembros, si así lo desean, precisar tales riesgos en su legislación;

(54º) Considerando que, con respecto a todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquella, que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga el Derecho nacional, podrá emitir un dictamen o autorizar el tratamiento; que este examen previo podrá realizarse también como parte de la preparación de una medida legislativa aprobada por el Parlamento nacional o sobre la base de una iniciativa de ese género, en la que se defina la naturaleza del tratamiento y se especifiquen las garantías adecuadas;

(55º) Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en que el responsable del tratamiento no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento, el cual sólo podrá ser eximido de responsabilidad si demuestra que no se lo puede imputar el hecho perjudicial, principalmente si alega la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a cualquier persona, tanto de Derecho privado como de Derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(56º) Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

(57º) Considerando, por otra parte, que cuando un país tercero no ofrece un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

(58º) Considerando que han de establecerse excepciones a esta prohibición en determinadas circunstancias, cuando el interesado haya dado su consentimiento, cuando la transferencia se necesaria en relación con un contrato o una reclamación legal, cuando así lo exige la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en asuntos de seguridad social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo; que dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro; que, cuando la finalidad de un registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia solo debería poder efectuarse a petición de dichas personas o cuando éstas sean las destinatarias;

(59º) Considerando que pueden adoptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, en caso de que el responsable del tratamiento ofrezca garantías adecuadas; que, por lo demás, deben preverse procedimientos de negociación entre la Comunidad y terceros países de que se trate;

(60º) Considerando que, en cualquier caso, las transferencias hacia terceros países sólo podrán ejecutarse si se respetan plenamente las disposiciones tomadas por los Estados miembros en aplicación de la presente Directiva, y en particular en su artículo 8;

(61º) Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar, tomando en consideración el carácter específico de los tratamientos efectuados en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación;

(62º) Considerando que la creación de una autoridad de control independiente en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;

(63º) Considerando que dicha autoridad debe ser dotada de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de quejas presentadas a la autoridad o de poderes para incoar procedimientos legales; que tal autoridad ha de contribuir a la transparencia de los tratamientos efectuados en el Estado miembro del que depende;

(64º) Considerando que las autoridades de los distintos Estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones, de forma que se garantice el adecuado respeto de las normas de protección en toda la Unión Europea;

(65º) Considerando que se debe crear, en el ámbito comunitario, un Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, teniendo en cuenta este carácter específico, el Grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva;

(66º) Considerando que por lo que respecta a la transferencia de datos hacia terceros países, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo al procedimiento establecido en la Decisión 87/373/CEE del Consejo; (1)

(1) DO nº L 197 de 18.7.1987, p. 33

(67º) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, el respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios;

(68º) Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste-eficacia, se concederá a los Estados miembros un periodo que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese periodo transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento;

(69º) Considerando que no es procedente que el interesado tenga que dar de nuevo su consentimiento a fin de que el responsable pueda seguir efectuando, tras la entrada en vigor de las disposiciones nacionales adoptadas virtud de la presente Directiva, tratamientos de datos sensibles necesarios para la ejecución de contratos celebrados previo consentimiento libre e informado antes de la entrada en vigor de las disposiciones mencionadas;

(70º) Considerando que la presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a los tratamientos de datos personales;

(71º) Considerando que la Directiva autoriza que se tenga en cuenta el principio de acceso del público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva;

Han adoptado la presente directiva:

SYN 287 (Texto de la posición común del Consejo de la Unión Europea doc. 12003/94)

CAPITULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto de la Directiva.

1. Los Estados miembros garantizarán con arreglo a las disposiciones de la Presente Directiva, la protección de las libertades y los derechos fundamentales de las personas físicas, y en particular del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
[*Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión declaran que la protección de los derechos y las libertades, en particular de la vida privada, con respecto al tratamiento de datos de carácter personal, incluye la protección de la identidad personal"]*

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Artículo 2. Definiciones.

A efectos de la presente Directiva, se entenderá por:

(a) "datos personales": toda información sobre una persona física identificada o identificable ("el interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
[Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión confirman que corresponde a los Estados miembros determinar si, y en que medida, la presente Directiva puede ser aplicable a las personas fallecidas. - El Consejo y la Comisión confían que los tratamientos de datos de sonido e imagen efectuados con fines de seguridad pública quedarán excluidos del ámbito de aplicación de la Directiva, cualesquiera que fueren las transformaciones de la tecnología de la información"]
[Cfr . Considerandos 14º a 16º]

(b) "tratamiento de datos personales" ("tratamiento"): cualquier operación o cualquier conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso de los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

(c) "Fichero de datos personales" ("fichero"): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sean centralizados, descentralizados o repartidos de forma funcional o geográfica;
[Declaración a incluir en el Acta del Consejo: " El Consejo y la Comisión reconocen que: - de conformidad con la definición actual del artículo 2, c), la Directiva sólo se aplicará a ficheros y no a expedientes; - los criterios que permitan determinar los elementos que constituyen un conjunto estructurado de datos de carácter personal, así como los criterios en virtud de los cuales tal conjunto deba ser accesible, podrán ser precisados por cada uno de los Estados miembros; - los expedientes y los conjuntos de expedientes, incluidas las carátulas, no estarán cubiertos por la definición a que se refiere el primer guión si su contenido no estuviera estructurado a la manera de un fichero". " El Consejo y la Comisión reconocen que los documentos de papel impresos mediante un aparato de telefax están sujetos a las reglas aplicables a los datos manuales y que en consecuencia no estarán cubiertos por el ámbito de aplicación de la presente Directiva si no estuvieran destinados a figurar en un fichero"]

(d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que determine los fines y los medios de tratamiento de datos personales;

(e) "subencargado": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

(f) "tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo con excepción del interesado, del responsable del tratamiento, del subencargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del subencargado.

(g) "destinatario": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante las autoridades que puedan recibir una comunicación de datos durante un trabajo de investigación particular no se considerarán destinatarios;

(h) "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento datos personales que le conciernan.

Artículo 3. Ámbito de aplicación.

1. Las disposiciones de la presente Directiva se aplicarán al tratamiento de datos personales, automatizado completamente o en parte, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en ficheros.

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:
- efectuado en el ejercicio de actividades que no entren en el ámbito de aplicación del Derecho comunitario, como aquellas a las que se aplican las disposiciones de los Títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado) y las actividades del Estado en materia penal;
- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
[Declaración a incluir en el acta del Consejo: " El Consejo y la Comisión consideran que la expresión « actividades exclusivamente personales o domésticas» no debe permitir excluir de la Directiva los tratamientos de datos de carácter personal efectuados por una persona física cuando tales datos fueren comunicados, no a una o varias personas, sino a un número indeterminado de personas]

Artículo 4. Derecho nacional aplicable.

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

(a) el tratamiento sea efectuado en el contexto de las actividades de un establecimiento en el territorio del Estado miembro del responsable. Cuando el mismo responsable está establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

(b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica la legislación nacional en virtud del Derecho internacional público;

(c) 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;

2. En el caso mencionado en la letra c) del apartado 1, 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.

CAPITULO II

CONDICIONES GENERALES PARA LA LICITUD DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 5.

Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en las que son lícitos los tratamientos de datos personales.

Sección I

Principios relativos a la calidad de los datos

Artículo 6.

1. Los Estados dispondrán que los datos personales sean:

(a) tratados de manera leal y lícita;

(b) recogidos con fines determinados, explícitos y legítimos y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros tomen las garantías oportunas;

(c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben o para los que se traten posteriormente;

(d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

(e) conservados en una forma que permita la identificación del interesado durante un período no superior al necesario para los fines para los que fueron recogidos los datos o para los que se traten ulteriormente. Los Estados miembros estipularán las garantías apropiadas para los datos personales archivados por un periodo más largo del mencionado, por motivos históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento del apartado 1.

Sección II

Principios relativos a la legitimación del tratamiento de datos

Artículo 7.

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

(a) el interesado ha dado su consentimiento de forma inequívoca, o

(b) es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales adoptadas en respuesta a una solicitud del interesado, o

(c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

(d) es necesario para proteger el interés vital del interesado, o

(e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferida al responsable del tratamiento o a un tercero a quien se comunican los datos, o

(f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comunican los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que invoque una protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.
[Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión reconocen que el interés legítimo del responsable o del tercero al que se comunican los datos puede responder a una misión de interés general"]

Sección III

Categorías especiales de tratamientos.

Artículo 8. Tratamientos de categorías especiales de datos.

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
[Declaración a incluir en el acta del Consejo: "El Consejo y la Comisión consideran que los Estados miembros pueden, de conformidad con el artículo 5, precisar las categorías de datos sensibles que figuran en el artículo 8, apartado 1, habida cuenta de las características jurídicas y sociológicas del país, por ejemplo en lo que respecta a la identidad genética, a la afiliación política, a la condición física, a las convicciones o hábitos personales, etc."]

2. El apartado 1 no se aplicará cuando:

(a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado; o

(b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea unas garantías adecuadas, o;
[Declaración a incluir en el Acta del Consejo : "El Consejo y la Comisión consideran que los términos «obligaciones en materia de Derecho del trabajo» comprenden igualmente todo acuerdo entre los interlocutores sociales"]

(c) el tratamiento sea necesario para salvaguardar el interés vital de la persona en cuestión o de otra persona, en el supuesto de que la persona en cuestión no esté en condiciones de dar un consentimiento, o

(d) el tratamiento lo efectúe una fundación, una asociación o cualquier otro organismo sin finalidad lucrativa, cuyo objeto tenga carácter político, filosófico, religioso o sindical, en el curso de sus actividades legítimas y con las debidas garantías, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan regularmente relaciones con la fundación, la asociación o el organismo en razón de su objeto y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o

(e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el fundamento, ejercicio o defensa de demandas judiciales, (1)

[Declaración a incluir en el Acta del Consejo : "Austria parte del principio de que el tratamiento de datos para el reconocimiento, el ejercicio o la defensa en juicio de un derecho engloba la correspondiente utilización de los datos en procedimientos sustanciados ante otros organismos estatales, en la medida en que tales procedimientos precedan a la instancia judicial"]

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médico, la prestación de atención sanitaria o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por organismos nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto,

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de la autoridad pública.

6. Las excepciones a las disposiciones del apartado 1, que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro de identificación de carácter general podrá ser objeto de un tratamiento.

Artículo 9. Tratamiento de datos personales y libertad de expresión.

En lo correspondiente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, las excepciones que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

[Declaración a incluir en el Acta del Consejo: " 1. En su informe periódico sobre la aplicación de la presente Directiva, la Comisión examinará con especial atención la aplicación del artículo 9 por los Estados miembros, al objeto de formu - lar las propuestas necesarias. - 2. El consejo y la Comisión declaran que: - la protección por el derecho de autor de las obras artísticas o literarias no interfiere con la presente Directiva; - la expresión literaria y artística es una forma de expresión cuya libertad está garantizada por el artículo 10 del Convenio Europeo de los Derechos del Hombre. - 3. Francia declara que hará uso de las excepciones previstas en el artículo 9 para el conjunto de las actividades del sector audiovisual cubiertas por la Directiva. - 4. El Reino de Suecia considera que la noción de expresión artística y literaria hace referencia a los medios de expresión más que al contenido de la comunicación o a su calidad."]

Sección IV

Información del interesado

Artículo 10. Información en caso de obtención de datos facilitados por el interesado.

Los Estados miembros dispondrán que el responsable del tratamiento o su representante comuniquen a la persona de la que se obtengan datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

(a) la identidad del responsable del tratamiento y, en su caso, de su representante,

(b) los fines del tratamiento de que van a ser objeto los datos,

(c) cualquier otra información tal como:

- los destinatarios o las categorías de destinatarios de los datos,

- el carácter obligatorio o no de la respuesta y las consecuencias que tendrá para la persona interesada una negativa a responder,

- la existencia de derechos de acceso y rectificación de los datos que la conciernen.

Habida cuenta de las circunstancias específicas en que se obtengan los datos resulte necesaria para garantizar un tratamiento de datos de manera leal respecto a la persona interesada.

Artículo 11. Información cuando los datos no han sido recabados del interesado.

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar a la persona interesada por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

(a) la identidad del responsable del tratamiento y, en su caso, de su representante,

(b) los fines del tratamiento de que van a ser objeto los datos,

(c) cualquier otra información tal como:

- las categorías de los datos de que se trate
- los destinatarios o categorías de destinatarios de los datos,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen.

habida cuenta de las circunstancias específicas en que se hayan obtenidos los datos, resulte necesaria para garantizar un tratamiento de datos de buena fe respecto a la persona interesada.

[Declaración a incluir en el Acta del Consejo: "El Reino Unido considera, en lo que respecta a la aplicación del artículo 11 a situaciones, en especial comprendidas en el ámbito de la propaganda electoral, en las cuales los datos no fueren recogidos directamente del interesado, que la obligación del responsable del tratamiento de facilitar informaciones no precisa un contacto directo con la persona interesada, sino que las informaciones pueden ser facilitadas, por ejemplo, bajo la forma de una comunicación por medio de la persona del domicilio de la persona interesada de la cual fueren recabados los datos.- El Consejo y la Comisión consideran que para decidir sobre la cuestión de saber si la dación de información implica un esfuerzo desproporcionado en el sentido del artículo 11, apartado 2, debe tenerse en cuenta la importancia del interés público en virtud del cual fueren tratados los datos"]

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

Sección V

Derecho de acceso del interesado a los datos

Artículo 12. Derecho de acceso.

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

1. libremente, sin coacción y con una frecuencia razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como de la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado al menos en los casos de las decisiones automatizadas a las que se refiere el apartado 1 del artículo 15;

2. la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

3. la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el apartado 2, si no resulta imposible o supone un esfuerzo desproporcionado.

Sección VI

Excepciones y limitaciones

Artículo 13. Excepciones y restricciones.

1. Los Estados miembros podrán tomar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, en el artículo 12 y en el artículo 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

(a) la seguridad del Estado;

(b) la defensa;

(c) la seguridad pública;

(d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la ética en las profesiones reglamentadas;

(e) un interés económico y financiero importante del Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

(f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejerci-

cio de la autoridad pública en los casos a que hacen referencia (c), (d) y (e);

(g) la protección del interesado o de los derechos y libertades de otras personas.

[Declaración a incluir en el Acta del Consejo: "El Reino Unido, apoyado por España, declara que las disposiciones del artículo 13, apartado 1, puntos (d), (e) y (f) tienen por objeto concretamente que el derecho de acceso previsto en el artículo 12 puede ser sometido a restricciones o a condiciones especiales cuando así fuere necesario para el ejercicio del control financiero previsto en las Directivas 77/780/ CEE, 85/611/CEE, 92/49/CEE, 92/96/CEE y 93/22/CEE, que corresponden respectivamente a la primera Directiva de coordinación bancaria modificada por la segunda Directiva de coordinación bancaria; la Directiva OPCVM; la tercera Directiva de seguros distintos del de vida; la tercera Directiva de seguros de vida; y la Directiva de Servicios de inversión.- La Comisión comparte la interpretación dada por las declaraciones relativas a la propaganda electoral y al control de los servicios financieros.- El Consejo y la Comisión declaran que la excepción que figura en la letra (g) del artículo 13 no contempla derechos como el de realizar tratamientos de datos."]

2. Sin perjuicio de las garantías legales apropiadas, que excluyen en particular que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán limitar mediante una disposición legislativa los derechos contemplados en el artículo 13 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un periodo que no supere el tiempo necesario para la única finalidad de la elaboración estadística.

Sección VII

Derecho de oposición del interesado

Artículo 14. Derecho de oposición del interesado.

Los Estados miembros reconocerán al interesado el derecho a:

(a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

(b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal respecto de los cuales responsable prevea un tratamiento destinado a la prospección; o

ser informado 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 le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que las personas interesadas conozcan la existencia del derecho al que se refiere el primer párrafo de la letra (b).

Artículo 15. Decisiones individuales automatizadas.

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que las afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, credibilidad, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

(a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que se haya satisfecho la petición del interesado o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o

(b) esté autorizada por una ley que contenga medidas para la salvaguardia del interés legítimo del interesado.

Sección VIII

Confidencialidad y seguridad del tratamiento

Artículo 16. Confidencialidad del tratamiento.

Ninguna persona que actúe bajo la autoridad del responsable o del subencargado del tratamiento, incluido este último, tratará datos personales a los que tenga acceso, a menos que se lo encargue el responsable del tratamiento y salvo que se lo exija un imperativo legal.

Artículo 17. Seguridad del tratamiento.

1. Los Estados miembros dispondrán la obligatoriedad por parte del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, necesarias para la protección contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los progresos técnicos y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros dispondrán que el responsable del tratamiento, en caso de tratamiento por cuenta propia, elija a un encargado del tratamiento que reúna garantías suficientes sobre las medidas de seguridad técnica de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por cuenta de un encargado deberá estar regulada por un contrato u otro acto jurídico que le vincule con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento actúa sólo siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a este.

4. A efectos de conservación de la prueba, las partes del contrato o acto jurídico relativas a la protección de los datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

Sección IX

Notificación

Artículo 18. Obligación de notificación a la autoridad de control.

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, se precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los se comuniquen los datos y el periodo de conservación de los datos, y/o

- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de datos personales que se hará cargo, en particular,

* de hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

* de llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21,

garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

[Declaración a incluir en el Acta del Consejo: " En la medida en que un Estado miembro aplique simultáneamente las dos disposiciones del artículo 18 apartado 2, primero y segundo guión, podrá prever que el comisionado de protección de datos no esté obligado a incluir en su registro la información referente a los tratamientos comprendidos en el primer guión del artículo 18, apartado 2, primer guión."]

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya por única fina-

lidad sea la de llevar registros que, con arreglo al derecho nacional, estén destinados a facilitar información y estén abiertos a la consulta por el público en general o de toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación a los tratamientos a que se refiere la letra d) del apartado 2 del artículo 8, o disponer una simplificación de la notificación.

5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal sean notificados en general o en casos concretos, o contemplar medidas de simplificación para la notificación de dichos tratamientos.

[Declaración a incluir en el Acta del Consejo: " La República de Austria estima que sólo los tratamientos no atentatorios contra los derechos y libertades de los interesados podrán ser eximidos de la obligación de notificar"]

Artículo 19. Contenido de la notificación.

1. Los Estados miembros definirán los datos que deben figurar en la notificación, que serán como mínimo:

(a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;

(b) el o los objetivos del tratamiento,

(c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;

(d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;

(e) las transferencias previstas de datos a terceros países;

(f) una descripción general que permita evaluar sin resultan adecuadas las medidas adoptadas para garantizar la seguridad del tratamiento, en aplicación del artículo 17.

2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modifi - caciones que afecten a las informaciones contempladas en el apartado 1.

Artículo 20. Controles previos.

1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades individuales y velarán por que sean examinados antes del comienzo del tratamiento.

2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos que, quien en caso de duda deberá consultar a la autoridad de control.

3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21. Publicidad de los tratamientos.

1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.

2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se incluirán, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.

[Declaración a incluir en el Acta del Consejo:" El Consejo y la Comisión precisan que los derechos contemplados en el artículo 21, apartado 3, no deberán ser ejercidos de manera abusiva e indican especialmente, como ejemplo de abuso, el caso de una petición que fuera hecha cuando fuere público y notorio que el tratamiento de datos no concierne al peticionario"].

3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables de los tratamientos u otro órgano designado por los Estados miembros comuniquen en las formas adecuadas al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19 a toda persona que lo pida.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea

disponer de un registro que, en virtud de leyes o de reglamentos, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

CAPÍTULO III

RECURSOS JUDICIALES, RESPONSABILIDAD Y SANCIONES

Artículo 22. Recursos.

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28 y antes de acudir a la autoridad judicial, los Estados miembros dispondrán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. Responsabilidad.

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

[Declaración a incluir en el Acta del Consejo: "Austria declara que en lo que respecta a la cuestión del Derecho nacional aplicable a la cuestiones de responsabilidad, parte del principio de que en el caso de la responsabilidad de los empleados se aplicará en todo caso el Derecho austríaco cuando se tratare de un contrato de trabajo que se rigiere por el Derecho austríaco"]

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24. Sanciones.

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular , las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

CAPÍTULO IV

TRANSFERENCIA DE DATOS PERSONALES A PAÍSES TERCEROS

Artículo 25. Principios.

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del 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; en particular, se tomará en consideración la naturaleza de los datos, el fin o los fines y la duración del tratamiento o tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el tercer país de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. 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 con arreglo del apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos del mismo carácter al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho, en aplicación del apartado 4.

6. La Comisión podrá comprobar, según el procedimiento mencionado en el apartado 2 del artículo 31, que un tercer país garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su

legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 4 bis, con fines de protección de la vida privada o de las libertades o derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. Excepciones.

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que rija los casos particulares, los Estados miembros dispondrán que una transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, puede efectuarse siempre y cuando:

1) el interesado haya dado su consentimiento inequívocamente, o

2) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas preliminares al contrato tomadas en respuesta a una petición del interesado, o

3) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado en interés del interesado, entre el responsable del tratamiento y un tercero, o

4) la transferencia sea necesaria para la salvaguardia de un interés público importante, o para el fundamento, el ejercicio o defensa de demandas judiciales, o

5) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

6) la transferencia tenga lugar desde un registro que, en virtud de disposiciones legislativas o reglamentarias, esté concebido para facilitar la información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en el caso particular, las condiciones que establece el Derecho para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento aduzca 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 derechos con ello relacionados, dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que conceden con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente los motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

CAPÍTULO V

CÓDIGOS DE CONDUCTA

Artículo 27.

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a una aplicación adecuada de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, así como otros organismos representativos de otras categorías de responsables de tratamientos, que elaboren proyectos de códigos nacionales o que tengan la intención de modificar o de prorrogar códigos nacionales existentes puedan presentarlos a las autoridades para su dictamen.

Los Estados miembros establecerán que dicha autoridad vele, en particular, por la conformidad de los proyectos que se presenten con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conve-

niente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

[Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión consideran que esta Directiva no altera la obligación de secreto profesional impuesta a las autoridades competentes por las directivas comunitarias relativas a las instituciones financieras, dado que el artículo 28 habilita a las Autoridades de control en materia de protección de datos para acceder a las informaciones en poder de las autoridades competentes de manera que dicho acceso no implique la divulgación de la información cubierta por una obligación de secreto profesional"]

CAPÍTULO VI

AUTORIDAD DE CONTROL Y GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Artículo 28. Autoridad de control.

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20 y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; **Artículo 48. Potestad de inmovilización de ficheros.**

- el poder de litigar en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las demandas que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su demanda.

Toda autoridad de control entenderá, en particular, de las demandas de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Esa persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de Control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Cualquier autoridad de otro Estado miembro podrá pedir a dicha autoridad que ejerza sus poderes a petición de una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular, mediante el intercambio de información.

7. Los Estados miembros dispondrán que los miembros y la plantilla de las autoridades de control deban estar sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

Artículo 29. Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.

1. Se crea un Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado "el Grupo".

Dicho Grupo, tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro y por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, así como por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión desempeñará la secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de este, bien previa solicitud motivada de un representante de las autoridades de control, bien a solicitud de la Comisión.

Artículo 30.

1. El Grupo tendrá la misión de:

(a) estudiar toda cuestión relativa a la ejecución de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

(b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los terceros países;

(c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

(d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación o la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.

3. El grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de los datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité previsto en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe se publicará.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los terceros países, y lo comunicará a la Comisión, al Parlamento Europeo y al Consejo. Dicho informe se publicará.

CAPÍTULO VII

MEDIDAS DE EJECUCIÓN COMUNITARIAS

Artículo 31. El Comité.

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El representante de la Comisión presentará al Comité un proyecto de las medidas. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Con motivo de la vota-

ción en el Comité, los votos de los representantes de los Estados miembros se ponderarán de la manera definida en el artículo anteriormente citado. El Presidente no tomará parte en la votación.

La Comisión adoptará las medidas previstas cuando sean conformes al dictamen del Comité.

Cuando las medidas no sean conformes con el dictamen del Comité o en caso de ausencia de dictamen, la Comisión someterá sin demora al Consejo una propuesta relativa a las medidas que daban tomarse. El Consejo se pronunciará por mayoría cualificada.

Si, transcurrido un plazo de tres meses a partir del momento en que la propuesta se haya sometido al Consejo, este no se hubiere pronunciado, la Comisión adoptará las medidas propuestas.

DISPOSICIONES FINALES

Artículo 32.

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar, al final de un período de tres años a partir de la adopción de la Directiva.

Cuando los Estados miembros adopten dichas disposiciones, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia .

2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.

No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de los datos que se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. Los Estados miembros otorgarán no obstante a la persona interesada, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a rectificar, suprimir o bloquear los datos que no estén completos o inexactos o hayan sido almacenados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.

[Declaración a incluir en el Acta del Consejo: "El Consejo y la Comisión consideran que, en lo que respecta a las circunstancias específicas en las cuales los datos personales contenidos en ficheros manuales que no fueren objeto de tratamiento activo después de la entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, pero que estén validamente conservados con miras a un previsible uso futuro, el artículo 32 contiene una obligación para los responsables del tratamiento, de adoptar, antes de expirar el plazo de 12 años que en el mismo se contempla, todas las medidas razonables previstas en los artículos 6, 7 y 8 que no resulten imposibles o que no impliquen un esfuerzo financiero desproporcionado teniendo siempre la necesidad de garantizar la protección de los derechos y libertades de las personas físicas y dentro de la observancia de las prerrogativas de la Autoridad de Control a que se refiere el artículo 28 de la Directiva.- Bélgica y Luxemburgo consideran que la declaración del Consejo y de la Comisión que antecede no afecta para nada a la aplicabilidad de la Directiva, en especial de sus artículos 6, 7, 8, y 32, a los datos manuales y no confiere al responsable del tratamiento discrecionalidad en cuanto a la decisión de aplicar las disposiciones de la Directiva a los datos manuales; consideran que en todo caso los tratamientos de datos manuales deberán efectuarse en condiciones que no atenten contra los derechos y libertades de las personas físicas"].

3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las salvaguardas oportunas, que los datos conservados con el único fin de la investigación histórica no se ajusten a los artículos 6, 7 y 8 de la presente Directiva.

4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones del Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 33.

La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe se publicará.

La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de sonidos e imágenes personales y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información de la situación.

Artículo 34.

Los destinatarios de la presente Directiva son los Estados miembros.

(1) Cf. doc. 11369/94, punto B. ll, iv) b)

Ley Orgánica 5/1992; Real Decreto 428/1993; Real Decreto 1332/1994

Artículo 1. Objeto.

1. La presente Ley Orgánica, 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.

Artículo 3. Definiciones.

A los efectos de la presente Ley se entenderá por:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.
Real Decreto 1332/1994. Artículo 1. A efectos de lo dispuesto en el presente Real Decreto se entenderá por : 4. Datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identifica - ble. 5. Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

e) Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo

c) Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la reco - gida, grabación, conservación, elaboración modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Real Decreto 1332/1994. Artículo 1.: A efectos de lo dispuesto en el presente Real Decreto se entenderá por :1. Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento. - 2. Cesión de datos: 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 datos realizada por una persona distinta de la afectada. - 6. Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

b) 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.

d) Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se tenga no pueda asociarse a persona determinada o determinable.

Artículo 2. Ámbito de aplicación.

1. La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

Disposición final segunda. Extensión de la aplicación de la Ley a ficheros convencionales.

El Gobierno, previo informe del Director de la Agencia de Protección de Datos, podrá extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan los datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

(Art. 2). 2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

(Art. 2). 3. Se regirán por sus disposiciones específicas:

c) Los derivados del (...) Registro Central de Penados y Rebeldes

(Art. 2). 2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley no serán de aplicación:

b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales.

(Art. 2.) 2. El régimen de protección de los Datos de carácter personal que se establece en la presente Ley no será de aplicación:

a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.

d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.

e) 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.

(Art. 2.) 3. Se regirán por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los sometidos a la normativa sobre protección de materias clasificadas.

c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.

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.

e) 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.

[Cfr. Real Decreto 1332/1994, artículo 2.1]

Artículo 4. Calidad de los datos.

7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos

1.(...) En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

2. 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.(Cfr., infra, art. 4.5)

1. 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 legítimas para las que se hubieran obtenido.

3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facul - tades que a los afectados reconoce el artículo 15.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la fina - lidad 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 deter-minará 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.

6. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

(Cfr. articulo 42 a 48)

Artículo 6. Consentimiento del afectado.

1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

3. El consentimiento (...) podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.

Artículo 11. Cesión de datos.

1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando una Ley prevea otra cosa.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.

(Art. 6) 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público (...) ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

(Art. 11). 2. El consentimiento (...) no será preciso:
c) Cuando el establecimiento del fichero automatizados responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

(Cfr. artículo 8)

(Art. 6). 2. No será preciso el consentimiento cuando los datos de carácter personal (...) se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias (...)

(Art. 11). 2. El consentimiento (...) 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.
e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

Artículo 7. Datos especialmente protegidos.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente.

(Cfr. artículo 8)

(Cfr. artículo 2 - 2 e)

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96

y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública y demás leyes sanitarias.

(Cfr. artículos 7, 21-1, 21-21-2)

5. El tratamiento de los datos relativos a infracciones, condenas penales o medidas de seguridad sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse una recopilación completa de condenas penales bajo el control de la autoridad pública.

(Artículo 7). 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

(Cfr. artículo 2-3 c)

[Cfr. Decreto 196/1976, de 6 de febrero, modificado por Real Decreto 1245/1985, de 17 de julio, y Orden de 12 de julio de 1990, del Ministerio del Interior. Cfr. asimismo, Real Decreto 1119/1986, de 26 de mayo, por el que se aprueba el Reglamento de ejecución de la Ley Orgánica 7/1985, de 1 de julio sobre derechos y libertades de los extranjeros en España (art. 67: número personal de extranjero). Cf. asimismo Real Decreto 338/1990, de 9 de marzo, por el que se regula la composición y la forma de utilización del Número de Identificación Fiscal.]

Artículo 5. Derecho de información en la recogida de datos.

1. Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

e) De la identidad y dirección del responsable del fichero.

a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Artículo 25. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d) y e), y 6 del artículo 11 ni cuando la cesión venga impuesta por Ley.

(Art. 11) 1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando una Ley prevea otra cosa.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

6. Si la cesión se efectúa previo procedimiento de disociación no será aplicable lo establecido en los apartado anteriores.

Real Decreto 1332/1994, artículo 11: los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto. - Podrá, no obstante, actuar el representante legal del afectado cuando este se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos

Artículo 14. Derecho de acceso.

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 el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 15. 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.[**Cfr. Real Decreto 1332/1994,** artículos 12 a 15]

2. Los datos de carácter personal que resulte inexacto 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.

Real Decreto 1332/1994, artículo 16: 1. En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización. - Se exceptúa, no obstante, el supuesto en que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquellos figuren. -2. Contra la resolución por la que el responsable del fichero acuerde el bloqueo de los datos procederá reclamación ante el Director de la Agencia de Protección de Datos.

(Art. 22). 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad Pública o a la persecución de infracciones penales o administrativas.

Artículo 21. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3, y 4 del artículo anterior podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la Seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar, el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

(Art. 15). 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.

(Art. .22) 2. Lo dispuesto en el artículo 14 y en 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 o, en su caso, del órgano equivalente de las Comunidades Autónomas.

(Art. 21). 3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores, podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros automatizados mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Ley 12/89, de 9 de mayo, de la FunciónEstadística Pública Artículo 16:

4. Los interesados tendrán derecho de acceso a los datos personales que figuren en los directorios estadísticos no amparados por el secreto estadístico y a obtener la rectificación de los errores que contengan. 5. Las normas de desarrollo de la presente Ley establecerán los requisitos necesarios para el ejercicio del derecho de acceso y rectificación a que se refiere el apartado anterior de este artículo (...)]

Artículo 29. Ficheros con fines de publicidad.(...)

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.

Artículo 12. Impugnación de valoraciones basadas exclusivamente en datos automatizados.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Artículo 10. Deber de secreto.

El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

(Cfr. artículo 27.2 in fine)

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados, y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 24. Notificación e inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificarán previamente a la Agencia de Protección de Datos.

4. El registro General de Protección de Datos inscribirá el fichero automatizado si la notificación se ajusta a los requisitos exigibles. - En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

Artículo 13. Derecho de información.

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

(Cfr. Real Decreto 428/1993, Artículo 23. El Registro General de Protección de Datos.

El Registro General de Protección de Datos es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 13 a 15 de la Ley Orgánica 5/1992, de 29 de octubre.)

Artículo 38. El Registro General de Protección de Datos.

1. Se crea el Registro General de Protección de datos como órgano integrado en la Agencia de Protección de Datos.

Real Decreto 428/1993. Artículos 11 y 23.

Real Decreto 1332/1994. Artículo 7. 2. El director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará la inscripción de los ficheros de titularidad privada si la notificación contuviera la información preceptiva y se cumplen las restantes exigencias legales, requiriendo, en caso contrario, al responsable del fichero para que la complete o subsane en el plazo de diez días, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, archivándose sin más trámite. 3. La inscripción contendrá, en el supuesto de ficheros de titularidad pública, las indicaciones previstas en el artículo 18.2 de la Ley Orgánica 5/1992, con especificación de la disposición general de creación y del diario oficial de su publicación, y, en el supuesto de ficheros de titularidad privada, los extremos relacionados en el artículo 6 del presente Real Decreto, con excepción de las medidas de seguridad. 4. La inscripción será notificada al responsable del fichero por el Registro General de Protección de Datos.

(Art. 13) (...) El Registro General será de consulta pública y gratuita.

(Cfr. art. 24).

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros automatizados de que sean titulares las Administración Públicas.

b) Los ficheros automatizados de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 31 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contras las resoluciones correspondientes y demás extremos pertinentes.

[Cfr. Real Decreto 1332/1994, artículo 7 y 8]

Artículo 17. Tutela de los derechos y derecho de indemnización.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos en la forma que reglamentariamente se determine.

2. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Real Decreto 428/1993. Artículos 2-3 y 2-4

Real Decreto 1332/1994. Artículos 10, 15-4, 16-2, 17

3. Los afectados que, como consecuencia del incumplimiento de los dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Real Decreto 1332/1994. Artículo 17.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirán de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

Real Decreto 429/1993, de 26 de marzo.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Artículo 42. Responsables.

1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45, apartado 2 (medidas disciplinarias)

(Cfr. artículos 43, 44, 45, 46, 47 y 48).

Real Decreto 1332/1994, Artículos 18 y 19.

Real Decreto 428/1994, Artículo 29.

Artículo 32. Norma general.

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 al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

(Cfr. art. 32, segundo inciso)

Artículo 33. Excepciones.

Lo dispuesto en el articulo anterior no será de aplicación:

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

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

c) Cuando la 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 bretes epidémicos.

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

Artículo 31. Códigos tipo.

1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo.

Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buen a práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

Artículo 34.

1. Se crea la Agencia de Protección de Datos.

(Cfr. artículo 40)

2. La Agencia de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. (...)

Artículo 36. Funciones.

Son funciones de la Agencia de Protección de Datos:

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

Real Decreto 428/1993. Artículo 5.b) Informará preceptivamente cualesquiera proyectos de ley o reglamento que incidan en la materia propia de la Ley Orgánica. - c) Dictará instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica. - d) Dictará recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

(Art. 36 i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

Artículo 39. Potestad de inspección.

1. La Agencia de Protección de Datos podrá inspeccionar los ficheros a que hace referencia la presente Ley recabando cuantas informaciones precise para el cumplimiento de sus cometidos. - A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se aténte de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesión en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas.

(Cfr. artículo 45).

(Art. 41).2. Si la administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración (C.C.A.A.)

Artículo 17. Tutela de los derechos y derecho de indemnización.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

Real Decreto 428/1993. Artículo 2-4. Los actos dictados por el Director en el ejercicio de las acciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recurso contenciosos-administrativos que resulte procedentes.

(Art. 36) d) Atender las peticiones y reclamaciones formuladas por personas afectadas.

(Art. 36 k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

Real Decreto 428/1993. Artículo 8. 2. La memoria anual será remitida por el Director al Ministro de Justicia, para su ulterior envío a las Cortes Generales.

(Art. 36 l) (...) desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

(Art. 39). 2. Los funcionarios que ejerzan la inspección (....) tendrán la consideración de autoridad pública en el desempeño de sus cometidos. - Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.