AGENCIA DE PROTECCIÓN DE DATOS

MEMORIA 2001

MEMORIA DE 2001 - PRESENTACIÓN

A través de la presente Memoria se pasa revista a las principales actividades llevadas a cabo por la Agencia de Protección de Datos (APD) durante el año 2.001, con el fin no solo de cumplir con la obligación que establece el artículo 37 k) de la Ley, sino también de informar a todos de los principales desarrollos que, en materia de protección de datos, han tenido lugar tanto a nivel nacional como internacional durante el período al que la misma se refiere y los criterios sustentados por la APD sobre diversos temas en el mismo período.

La entrada en vigor de la nueva Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) así como la STC 292/2000 determinaron, como ya se refería en la Memoria del año anterior, el incremento de acciones por parte de la APD para dar a conocer tanto la nueva normativa como la interpretación que debía darse a la misma a la luz de la trascendental STC por la que se viene a definir el derecho a la protección de datos personales como un derecho fundamental independiente, lo que ha constituido una prioridad también en el pasado año. Así durante el año 2.001, como Director de la APD, he estado presente en diversos cursos, seminarios y títulos de masters, organizados por diversas instituciones públicas y privadas y en todos aquellos lugares de nuestra geografía en los que se ha requerido la colaboración de la APD. El total de conferencias o ponencias impartidas ha alcanzado la cifra de 55.

En el mismo orden de actuaciones, hemos coorganizado con el Consejo de Gobierno de la Rioja unas jornadas dedicadas a “La protección de Datos por las Administraciones Públicas” en las que se pasaba revista, por diversos expertos y desde distintas posiciones, a las obligaciones que para las administraciones comporta la LOPD y las restricciones que para la cesión de datos entre las mismas viene a concretar la antes mencionada STC. La posterior publicación de todas las ponencias contribuirá sin duda a la mejor difusión de los temas tratados.

Hemos continuado acogiendo alumnos en prácticas procedentes de diversos masters universitarios para contribuir también a la formación de las nuevas generaciones en la defensa del derecho a la protección de datos personales en donde la APD tiene una de sus principales funciones.

Para incentivar el estudio en profundidad de la diversa problemática que suscita la legislación de protección de datos continuamos convocando el Premio Protección de Datos, con carácter anual, y que en el anterior ejercicio se otorgó al trabajo “El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones”, presentado por María de los Reyes Corripio Gil-Delgado y Lorenzo Marroig Pol, concediéndose un accesit al trabajo titulado “La Protección de los Datos en la Unión Europea: Divergencias Normativas y Anhelos Unificadores”, del que es autor D. Abel Tellez Aguilera.

La calidad y cantidad de los trabajos presentados al premio es un exponente más de la concienciación e interés que esta legislación está alcanzando en España.

También para velar por el cumplimiento de la legislación en la materia que nos concierne, dar a conocer mejor el marco legislativo, y buscar soluciones a los problemas que a responsables de ficheros y encargados de tratamientos se les plantean en la práctica en distintos sectores, la APD ha continuado realizando planes de inspección sectoriales y trasladando posteriormente sus recomendaciones tanto a los directamente inspeccionados como a los organismos representantes del sector. Así en el año 2.001 se han producido las recomendaciones respecto de inspecciones anteriores al Consorcio de Compensación de Seguros, sector del comercio electrónico, gestión de tarjetas en grandes superficies comerciales y operadores de telefonía móvil. En este año se han llevado a cabo inspecciones sobre el Censo de Población y Viviendas 2.001, el fichero histórico de seguros del automóvil, Europol, el sector de la banca a distancia, el fichero RAI y otro fichero sobre solvencia patrimonial.

Como ya es habitual en el año 2.001 he comparecido ante ambas Cámaras Legislativas en mi condición de Director de la APD. Se afianza así el control parlamentario como una garantía más de la independencia que debe presidir todas las actuaciones de la Agencia tal y como exige la Ley. La comparecencia ante la Comisión Constitucional del Congreso de los Diputados tuvo lugar a petición propia, para dar cuenta de la anterior memoria al propio tiempo que para responder a diversas interpelaciones de los Grupos Parlamentarios. Ante el Senado las comparecencias fueron dos. La primera ante la Comisión de la Sociedad de la Información y del Conocimiento y la segunda ante la Ponencia de estudio de los derechos de concursantes y audiencia en relación con concursos, juegos y apuestas.

Todas las actividades de la APD han continuado en el 2.001 la tendencia creciente que ya tuvo especial significación en el 2.000 según se constataba en la anterior Memoria. El área de atención al ciudadano ha dado respuesta a consultas varias que por diversos medios –presenciales, telefónicos, telemáticos y escritos- han planteado los ciudadanos con un total de 19.940, cifras similares a las del año anterior. Esta información se ha visto completada mediante la que se proporciona a través de la página web de la APD en Internet. El número de accesos a nuestra web ha pasado de 1.000.000 registrado en el 2.000 a 1.572.738 en el pasado ejercicio, lo que evidencia la utilidad de la información que en la misma se facilita.

Por lo que respecta a la inscripción de ficheros debe significarse un aumento del 35% respecto del año 2.000. También se continúan notificando a la APD transferencias internacionales de datos por un total de 644, en cifra superior al anterior ejercicio.

Las actuaciones inspectoras, sancionadoras, por supuestas infracciones a la legislación en materia de protección de datos y las demandas de tutela de derechos ante la APD, también crecieron en el período que examinamos. Así se

iniciaron 405 actuaciones de inspección, instruyéndose 218 procedimientos sancionadores y 363 tutelas de derechos frente a 319, 171 y 193 iniciados, respectivamente, el año anterior. El importe total de sanciones impuestas, alcanzó la cifra de 1.601.000.000 de pesetas, casi 400.000.000 de pesetas menos que el año anterior. Por primera vez, afortunadamente, se ha producido un descenso en el importe de las sanciones.

Las actividades internacionales cada año experimentan notables incrementos debido al mayor número de asuntos que se tratan en los distintos foros así como por el aumento de aquellos en los que debe participar la APD.

En particular, merece destacarse la celebración del Segundo Encuentro Ibérico de Autoridades de Protección de Datos, que reunió a las autoridades española y portuguesa en Cáceres durante dos días de cordiales e intensos debates, la puesta en marcha definitiva de un Proyecto de Hermanamiento de un año de duración con la Autoridad de Protección de Datos de la República Checa, la continuada colaboración con la Inspección General de Protección de Datos de Polonia o la impartición por parte de la Agencia de Protección de Datos de un seminario sobre la legislación española y europea en el Ministerior del Interior de Bulgaria.

Asimismo, la Agencia también participó activamente en los trabajos de las dos Conferencias Internacionales más importantes celebradas a lo largo del año pasado: la de Autoridades de Control europeas, celebrada en Atenas y la mundial celebrada en París, de cuyos resultados encontrarán cumplida relación en las páginas que siguen, así como las actividades llevadas a cabo en los foros habituales: Grupo del artículo 29, Autoridad de Control de Schengen, Autoridad de Control de Europol y Grupo de Protección de datos en el sector de las telecomunicaciones (Grupo Berlín).

La presente Memoria aún respetando la configuración que viene marcada por la Ley y el Estatuto, incorpora como novedad una mejor sistematización de las diversas áreas y un detalle más explícito de su índice con el fin de facilitar consultas concretas. Esperamos que resulte de utilidad para todos y conlleve a una mejor información para los ciudadanos a los que, quienes trabajamos en la APD, nos esforzamos día a día en velar por su derecho a la protección de sus datos personales. También deseamos que la Memoria sea útil para los responsables de ficheros y encargados de tratamientos a quienes tratamos de ayudar en el mejor conocimiento y cumplimiento de la LOPD.

Madrid, Abril 2002

Juan Manuel Fernández López
Director de la Agencia de Protección de Datos

MEMORIA DE 2001 - FUNCIONAMIENTO DE LA AGENCIA

I. CONSEJO CONSULTIVO

El Consejo Consultivo, previsto en el artículo 38 de la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal, y en los artículos 18 a 22 del Real Decreto 428/93, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, se configura como órgano colegiado de asesoramiento del Director del Ente Público, cuyos cometidos se centran en emitir informe en todas las cuestiones que le someta el Director de la Agencia y formular propuestas en temas relacionados con las materias de competencia de ésta.

En su composición, está integrado por los siguientes miembros:

* Presidente:

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

* Vocales:

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

Dª Rosa Vindel López, Senadora propuesta por el Senado.

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

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

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

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

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

Dª Rosa García Ontoso, Directora de la Agencia de Protección de Datos de la Comunidad de Madrid, en representación de esta Comunidad Autónoma.

* Secretario:

D. Carlos Corbacho Pérez, Secretario General de la Agencia de Protección de Datos.

La única variación producida en la composición del Consejo Consultivo en el transcurso del 2001 ha sido la baja de Dª Rosa García Ontoso por haber cesado como Directora de la Agencia de Protección de Datos de la Comunidad de Madrid (Decreto 41/2001, de 21 de noviembre, del Presidente de la Comunidad de Madrid) de acuerdo con el artículo 16.5 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

Han tenido lugar cuatro reuniones del Consejo en el año, entre los temas tratados pueden destacarse:

* Análisis evolutivo de la aplicación de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

* Consideraciones de la Sentencia 292/2000 del Tribunal Constitucional y de la Carta de Derechos Fundamentales de la Unión Europea, en las que se define el derecho a la protección de datos como un derecho independiente.

* Exposición de los Planes Sectoriales de inspección para 2001.

* Criterios judiciales en la aplicación de la Ley Orgánica de Protección de Datos.

* Presentación de la Memoria del año 2000.

* Informe del desarrollo de las Jornadas de Protección de Datos celebradas en Logroño (La Rioja) los días 5 y 6 de julio.

* Presentación del libro que recoge las Jornadas de Protección de la Privacidad celebradas en Pamplona (Navarra) en junio del 2000.

* Constitución del Consejo como Jurado para emitir los fallos de los Premios "Protección de Datos Personales" y Premio de Periodismo "Protección de Datos Personales" Convocatoria 2001.

* Informe y análisis de los principales problemas que afronta la Agencia en el momento actual.

* Deliberación sobre tareas y objetivos de la Agencia en el año 2002.

II SUBDIRECCIÓN GENERAL DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS.

1. OPERACIONES REALIZADAS EN EL RGPD DURANTE EL AÑO 2001

Durante el año 2001, se ha puesto de manifiesto que el gran incremento de solicitudes que se produjo a partir del año 1999 no fue un hecho puntual sino que obedece a una dinámica que parece consolidarse a lo largo del tiempo.

En efecto, durante 2001 se ha iniciado la tramitación de 15.078 solicitudes relativas a la inscripción de ficheros, lo que ha supuesto la realización de 34.713 operaciones de inscripción, de las que el 75% han sido expedientes de alta de inscripción (26.113), un 15% de modificación (5.161) y el 10% restante de supresiones de la inscripción (3.439). A comienzos del año 2002 se encontraban pendientes de tramitar 577 expedientes de inscripción de ficheros, cuyas entradas en la Agencia fueron registradas en los últimos días del año 2001.

Las operaciones anteriormente citadas, han sido realizadas a solicitud del responsable del fichero, habiéndose realizado, además, un total de 2.255 operaciones de oficio, fundamentalmente con el fin de subsanar errores materiales y normalizar algunos apartados de la declaración.

Estos datos suponen un aumento del 35% respecto a las operaciones realizadas durante el año 2000. Este incremento se une a los ya significativos aumentos, producidos durante los años anteriores, en especial durante los años 1999 y 2000, lo que parece poner de manifiesto que dichos incrementos obedecen a una dinámica que parece consolidarse a lo largo de los sucesivos años.

Es importante señalar que el número de operaciones de modificación y supresión, como consecuencia de solicitudes de los responsables de ficheros, no han experimentado variación entre las realizadas durante el año 2000 y el 2001, es decir, que la práctica totalidad del aumento de las operaciones entre este año y el anterior, se refieren a nuevas inscripciones de ficheros.

Las citadas operaciones han dado como resultado que, a 31 de diciembre de 2001, consten inscritos un total de 271.875 ficheros, siendo 31.805 de titularidad pública y 240.070 de titularidad privada. Esta cifra supone que, a la fecha anteriormente citada, se encuentran registrados 22.666 ficheros más que al finalizar el año 2000.

En el RGPD consta la historia de todas las operaciones de inscripción que se han realizado a lo largo del ciclo de vida de un fichero, desde que se inscribe inicialmente, hasta que, en su caso, se suprime, quedando constancia de cada una de las modificaciones que se han realizado a dicha inscripción. Al finalizar el año 2001, se han contabilizado aproximadamente 390.000 operaciones realizadas desde 1994, fecha en la que se creó el RGPD.

Durante el año 2001 se ha consolidado la notificación de solicitudes de inscripción mediante el programa de ayuda que fue puesto a disposición de los responsables de los ficheros a mediados del año 2000. Este programa, disponible en la dirección web de la Agencia, se ha convertido en una herramienta de gran utilidad para facilitar y agilizar el procedimiento de notificación e inscripción de ficheros.

La declaración por Internet, además de facilitar notablemente la solicitud de inscripciones, ha reducido a la mitad el número de subsanaciones de errores que ha sido necesario requerir a los responsables de los ficheros durante el año 2001 (2.378 frente a las 4.685 remitidas durante el año 2000).

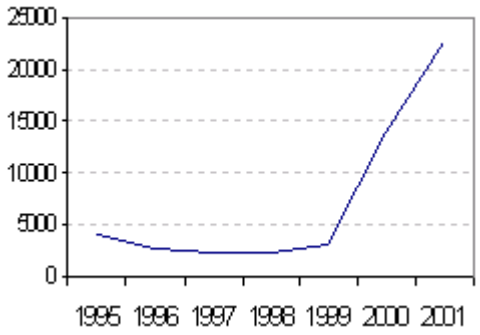
Las operaciones de inscripción notificadas mediante el programa de ayuda, ya sean a través de Internet o mediante soporte magnético, han representado el 68% del total de las mismas, mientras que han utilizado el formulario en soporte en papel en el restante 32%.

La mayor difusión y conocimiento de la obligación de notificar los tratamientos de datos de carácter personal, junto con la entrada en vigor del Reglamento de Medidas de Seguridad y de la LOPD, han implicado un incremento en las solicitudes de inscripción, que comenzó durante el año 1999, teniendo una especial incidencia en el año 2000 y que ha continuado durante el 2001.

Durante la inscripción inicial que se realizó entre 1994 y primer trimestre de 1995, se inscribieron aproximadamente 221.000 ficheros. Finalizada la inscripción inicial, durante el resto del año 1995 y los años 1996 y 1997, se incrementó esta cifra en 8.800 ficheros registrados, con un promedio de 3.000 nuevas inscripciones al año, constando, al final de 1997, un total de 229.804 ficheros de titularidad pública y privada.

A finales del año 2001, constan inscritos 271.875 ficheros de ambas titularidades, 42.071 ficheros más que al final del año 1997, lo que supone haber quintuplicado las inscripciones durante este período.

En el siguiente gráfico, se puede ver la evolución del número de nuevas inscripciones de ficheros que se han realizado desde marzo de 1995, fecha en que finalizó la inscripción inicial masiva, pudiéndose apreciar el incremento de nuevas inscripciones producido desde 1999.



2. DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

Cualquier persona puede conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, mediante una consulta pública y gratuita al RGPD según establece el art. 14 de la LOPD.

Estas consultas se corresponden con las solicitadas por los ciudadanos que desean conocer esta información al objeto de obtener la dirección del responsable del fichero ante el que desean ejercer sus derechos de acceso, oposición, rectificación o cancelación. Por otra parte, existe otro tipo de solicitudes bien diferenciado, que se corresponde con el del responsable del fichero, o de un tercero con interés legítimo, que en un momento determinado desea conocer la situación y el contenido de la inscripción de un fichero.

2.1. Publicación del catálogo de ficheros

Al objeto de facilitar el derecho de consulta al que hace referencia el artículo 14 de la LOPD, anualmente se publica el Catálogo de Ficheros inscritos en el RGPD en soporte CD-ROM, y mensualmente se actualiza este mismo Catálogo en la página web de la Agencia.

Con esta publicación se da cumplimiento al artículo 37j) de la Ley en el que se determina que es función de la Agencia velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto deberá publicar periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

En el Catálogo de ficheros 2001, publicado en CD-ROM, se incluyeron todos los ficheros que figuraban inscritos en el Registro a día 31 de mayo de 2001.

Asimismo, en este CD-ROM, correspondiente al Catálogo de ficheros 2001 se han incluido las informaciones que vienen siendo ya habituales en el mismo:

* Estadísticas del Registro General de Protección de Datos
* Memorias de la Agencia de los años anteriores desde 1994 hasta 2000.
* Publicaciones correspondientes a las Jornadas y Conferencias organizadas por la Agencia de Protección de Datos
* Premios de Protección de Datos correspondientes a 1997, 1998 y 2000
* Legislación actualizada sobre Protección de Datos
* Manual de Protección de Datos
* Programa de ayuda para la notificación de ficheros en soporte magnético o a través de Internet
* Modelos de notificación en soporte papel

Mediante esta publicación, distribuida a través de 1.500 ejemplares se ha facilitado el derecho de consulta de los ciudadanos. A lo largo de 2001, y sólo a través de la publicación del Catálogo en la página web de la Agencia se practicaron mas de 700.000 consultas, además de las atendidas telefónicamente a través de Atención al Ciudadano.

También, la consulta relativa al artículo 14 se ofrece a través de Internet, en este caso únicamente se publica información relativa a la identidad del responsable, la existencia de tratamientos citando la finalidad de los mismos y la dirección dónde se pueden ejercitar los derechos reconocidos en la Ley.

2.2. Información al responsable

Durante el año 2001, se han tramitado alrededor de 430 solicitudes, relativas a la copia del contenido de la inscripción de ficheros. Esta información ha sido solicitada, entre otros, con el fin de, posteriormente, proceder a notificar las modificaciones de las inscripciones correspondientes. Teniendo en cuenta que cada solicitud ha implicado una media de 3

copias de contenido, en total se han remitido cerca de 1300 copias de inscripción.

El principal motivo que ocasiona estas solicitudes es la necesidad de actualizar la inscripción del Registro. Ésta puede derivar de:

* Una adaptación de los sistemas de información.
* La práctica de una auditoría en aplicación del Reglamento de Medidas de Seguridad, con el fin de anexar al documento de seguridad de la entidad una copia de los ficheros inscritos en el Registro.
* La necesidad de actualizar la inscripción, bien porque haya transcurrido mucho tiempo desde la anterior comunicación o por cambios en el responsable, o en cualquier otro apartado de la notificación, o bien, para adecuar la inscripción a la LOPD, comunicando el nivel de medidas de seguridad aplicables al fichero y, en su caso, las transferencias internacionales de datos.

Por último, también se solicitan desde los órganos judiciales copias y certificaciones de la situación registral.

En todos estos casos, se facilita una copia completa de la inscripción siempre que se acredite un interés legítimo al respecto, excepto el apartado de medidas de seguridad, que únicamente se facilita al responsable del fichero.

Se está estudiando en el Registro la posibilidad de enviar copias de inscripción de ficheros a través de Internet.

En relación con la copia de inscripción sería necesario identificar al solicitante de la información, toda vez que únicamente a personas con interés suficiente se les podría dar copia completa de la inscripción.

Dado que se está estudiando la posibilidad de implementar la firma electrónica en el procedimiento de notificación de ficheros, mediante esta acreditación también se podría identificar al solicitante a los efectos de remitir electrónicamente la copia completa de inscripción.

3. INSCRIPCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA

3.1. Evolución y práctica de la inscripción de ficheros de titularidad pública

Cuando ya han transcurrido casi ocho años desde la puesta en marcha del Registro se puede hacer un balance acerca de la inscripción de ficheros de titularidad pública, que como puede desprenderse tanto de la lectura de esta memoria como de la de años anteriores, ha tenido una trayectoria bastante diferente de la de ficheros de titularidad privada.

En este sentido, debe recordarse que a diferencia de los ficheros de titularidad privada, que requieren de notificación e inscripción en el Registro, la creación, modificación o supresión de ficheros de titularidad pública requiere, además, la adopción de una disposición general publicada en el BOE o diario oficial correspondiente.

El balance puede considerarse positivo toda vez que la mayoría de los ficheros de esta titularidad han sido notificados para su inscripción en el Registro, al menos, todos aquellos ficheros que dan soporte a los sistemas de información más importantes de las Administraciones Públicas. Sin embargo, si hacemos un estudio cualitativo de estas inscripciones ya no se obtiene una visión tan satisfactoria.

En el transcurso del año 2001 se han reflejado en el Registro un total de 3.886 operaciones relativas a ficheros de titularidad pública. De estos movimientos, a instancia de parte se han practicado 1.193 inscripciones de creación de ficheros, 1.487 modificaciones y 536 cancelaciones de inscripción. Asimismo, se realizaron 670 rectificaciones de oficio y de subsanación de errores, debido a la necesidad de normalización y adecuación de los datos consignados en la notificación de ficheros, en relación con las disposiciones de regulación de los mismos que se publican en los boletines oficiales.

Al finalizar el ejercicio, el número de ficheros de titularidad pública que constaban inscritos en el RGPD es de 31.805. De ellos, el porcentaje más alto, con 23.757 ficheros, equivalente al 75% aproximadamente, corresponde a ficheros de la Administración Local.

La inscripción de ficheros públicos se va incrementando cada año aproximadamente en un 5%, que corresponde con nuevos sistemas de información que se ponen en marcha en la Administración General, la adecuación de determinadas Comunidades Autónomas, que en el momento inicial no declararon todos los ficheros existentes, y por último, con las declaraciones de Entidades de la Administración Local.

La Administración Local en este año, ha solicitado la inscripción de 407 nuevos ficheros, lo que representa un 34,32% del total de ficheros inscritos en 2001. Debe hacerse constar que en España existen más de 8.000 Ayuntamientos, el 95% de la población está censada en Ayuntamientos de más de 4.000 habitantes, de los cuales el 95% han inscrito sus ficheros en el RGPD. De este modo, los ficheros de los Ayuntamientos inscritos en el RGPD implican el 91% de la población total del país.

Los Ayuntamientos comprendidos en el tramo de menos de 1.000 habitantes son los que representan un porcentaje más alto de Ayuntamientos sin inscribir, sin embargo, también es cierto que el colectivo de población que incluye sus ficheros es únicamente de un 2,65% respecto del total de la población del territorio español.

En muchas de estas pequeñas corporaciones locales, que carecen de medios tecnológicos, puede darse la circunstancia de que la correspondiente Diputación tenga encomendada la gestión informática del padrón municipal de habitantes.

No obstante, es necesario aclarar que en estos casos el responsable del fichero es el Ayuntamiento, y por lo tanto, debería constar en el Registro como titular del fichero, y la correspondiente Diputación como encargada del tratamiento.

Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o diario oficial correspondiente constituye una infracción grave, según establece el art. 44.3.a) de la LOPD. Asimismo, el art. 44.2.c) califica de infracción leve, el hecho de no solicitar la inscripción del fichero de datos de carácter personal en el Registro, cuando no sea constitutivo de infracción grave. Este caso se produciría si no se cumple la previsión del artículo 44.3 i) *"No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos".*

3.2. Cambios de estructuras orgánicas y modificación del responsable de ficheros de titularidad pública

Como ya se cita anteriormente, una de las funciones más importantes que la LOPD atribuye al Registro, es la de velar por la publicidad de la existencia de ficheros de datos de carácter personal para facilitar al ciudadano la información relativa a la finalidad de los ficheros y sus tratamientos, la identidad del responsable y la dirección a la que se puede dirigir para ejercitar los derechos de oposición, acceso, rectificación y cancelación que la Ley le reconoce.

El cumplimiento de esta función tiene una estrechísima relación con la obligación de que cada órgano responsable de ficheros notifique, a los efectos de inscripción, la creación, modificación o supresión de los mismos.

El artículo 20.2 de la LOPD enumera los apartados obligatorios que debe contener la disposición general de creación de un fichero: finalidad y usos previstos, personas o colectivos, procedimiento de recogida, estructura y tipos de datos del fichero, cesiones y/o transferencias internacionales, órganos de las Administraciones responsables del fichero, servicios o unidades ante los que pudiesen ejercitarse los derechos y el nivel de medidas de seguridad. Asimismo, es obligatorio comunicar para su inscripción cualquier variación o modificación que se produzca en cualquiera de sus apartados. Esta previsión está establecida en el artículo 20 de la LOPD y en el artículo 8.1 del Real Decreto 1332/1994, *"la modificación o, en su caso, cancelación de la inscripción de los ficheros de titularidad pública se producirá de oficio por la Agencia de Protección de Datos, previo traslado por el órgano de la Administración responsable del fichero de una copia de la disposición general que modifique o suprima aquél".*

Las consecuencias de no actualizar las inscripciones en consonancia con las variaciones que se hayan producido, suponen en la práctica, un menoscabo en el ejercicio del derecho del ciudadano. La Agencia periódicamente requiere a los órganos responsables de las Administraciones Públicas y solicita que se actualice la inscripción de sus ficheros, en el caso de que se hubieran producido variaciones desde su inscripción. Asimismo, se realizan actuaciones de oficio en aquellos casos en los que la inscripción se puede subsanar.

En este sentido, en el último trimestre de 2000, se requirió a los Departamentos ministeriales y otros organismos públicos, para que notificasen los cambios derivados de reestructuraciones orgánicas. Estos requerimientos han sido uno de los factores que han influido en el aumento de los informes de proyectos de disposiciones generales presentados al Gabinete Jurídico durante el año 2001. A modo de ejemplo, se puede mencionar, por el número de ficheros a los que ha implicado, la modificación notificada por el Ministerio de Asuntos Exteriores en el mes de marzo de 2001, que afectaba a todos los ficheros de la anterior Dirección General de Asuntos Jurídicos y Consulares, que tras la publicación del Real Decreto 687/2000, quedó bajo la denominación de Dirección General de Asuntos Consulares y Protección de los Españoles en el Extranjero. Este cambio de centro directivo trajo consigo la modificación de 489 inscripciones de ficheros de Embajadas, Consulados y Secciones Consulares.

Como ya se exponía en memorias anteriores, también fueron requeridos los órganos titulares de ficheros de la Administración Autonómica. Durante el ejercicio 2001, han completado las modificaciones derivadas de reestructuraciones las Comunidades Autónomas de Galicia, Castilla León, La Rioja, Región de Murcia y la Comunidad Valenciana. En relación con Castilla La Mancha, ha de indicarse que no se han notificado aún las actualizaciones debido a que están elaborando sus propios programas informáticos de gestión de ficheros de datos de carácter personal, y se encuentran solventando algunos problemas técnicos que le impiden la notificación a este Registro. No obstante, es necesario citar que esta justificación no es suficiente para que no se haya cumplido con las previsiones que la Ley tiene en relación con las notificaciones de modificación que deben realizar obligatoriamente los titulares de ficheros.

Otro supuesto que implica notificar una modificación del órgano responsable, se produce cuando varía la estructura orgánica de un departamento, cuando se crea un nuevo centro directivo y se le atribuyen las competencias correspondientes a otros centros directivos en materias de gestión interna. Esta situación provoca que los ficheros que ya constan inscritos con finalidades relativas a la gestión de cada organismo se refundan en un único fichero, dando lugar en estos casos a la necesidad de supresión de las anteriores inscripciones.

Otros casos que pueden dar lugar a supresiones son los que se producen con ocasión de un traspaso de competencias de una Administración a otra, fundamentalmente entre la Administración Central y las Comunidades Autónomas. Esta situación implica la creación de un nuevo fichero por cada una de las administraciones autonómicas que han recibido la nueva competencia y la supresión del fichero de la Administración central, o en su caso, de la modificación de las finalidades.

Cuando se suprime la función de un órgano administrativo relacionado con un fichero creado e inscrito en el RGPD, la cancelación del fichero no podrá ser efectiva de forma inmediata. Puede ser necesario conservar los datos para las finalidades relacionadas con la atención de posibles responsabilidades a solicitud de las Administraciones Públicas, Jueces y Tribunales, así como la previsión del mantenimiento de datos de carácter personal con el objeto de tratar los datos para fines históricos, estadísticos o científicos. Sin embargo, en éstos casos, será necesaria una disposición de modificación del fichero en la que, al menos, se modifique el apartado relativo a la finalidad del fichero artículo 20.2.a) y los órganos de la Administración responsable del fichero.

3.3. Repercusión de la sentencia 292/2000 del Tribunal Constitucional en la inscripción de ficheros de titularidad pública

En el fallo de esta sentencia se declara contrario a la Constitución y nulo el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del art. 21.1 de la LOPD.

La comunicación de datos a terceros está regulada, con carácter general, en el art. 11.1 de la LOPD que dispone que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y del cesionario con el previo consentimiento del interesado". No obstante, el apartado 2 del mismo artículo determina que no será preciso dicho consentimiento, entre otros casos, "cuando la cesión está autorizada por una Ley".

En este sentido, en el mes de julio el Director de la Agencia remitió un escrito a cada uno de los departamentos ministeriales, a cada comunidad autónoma, a los ayuntamientos de todas las capitales de provincia y a todos aquellos responsables de ficheros que habían notificado al Registro, que realizaban cesiones amparadas en la norma de creación. Junto con esta actuación informativa se comunicó al órgano responsable la prohibición de realizar una cesión, por el mero hecho de ampararse en la norma de creación del fichero, solicitándoles que procedieran a revisar la inscripción de sus ficheros, en particular, el apartado de cesiones y especificar las normas con rango de ley en las que puede estar amparada la comunicación de los datos de carácter personal. Para facilitar la tarea de revisión a los responsables, se remitía la relación de todos los ficheros que constaban inscritos, en los que se habían declarado cesiones de datos.

Por otro lado, se hacía una especial mención, y se relacionaban independientemente los ficheros en los que se habían declarado cesiones amparándose únicamente en la disposición general de creación del fichero.

A su vez, se indicaba que en el caso de que las cesiones no estén amparadas en ninguno de los supuestos previstos por la Ley en los arts. 11 y 21 deberían proceder a notificar las correspondientes supresiones a los efectos de su cancelación en el Registro General de Protección de Datos.

Este requerimiento se realizó a 119 responsables de ficheros de titularidad pública.

En el mes de diciembre, se reiteraron los requerimientos, informando además de las posibles infracciones a las que podría dar lugar la práctica de estas cesiones o la falta de notificación al Registro.

3.4. Adecuación de la norma de creación de ficheros a la LOPD, según la Disposición Adicional Primera.

Los ficheros y tratamientos automatizados deberán adecuarse a la LOPD dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

Como se citaba en memorias anteriores, esta disposición establece el periodo de adecuación de tres años, refiriéndose, exclusivamente, a los ficheros que ya se encontraban sometidos al ámbito de aplicación de la LORTAD, a los deberes meramente formales, entre los que se encuentra la adaptación de la disposición general de regulación del fichero.

Dado que este plazo finaliza al inicio del año 2003, y teniendo en cuenta el tiempo que se precisa para tramitar la publicación de una disposición general, los responsables de ficheros de titularidad pública deberán preparar estas normas con antelación suficiente.

Se puede constatar por los informes presentados en la Agencia, que la actuación informativa realizada durante este año, ha influido en los órganos titulares de los datos en orden a adaptar las disposiciones de creación de ficheros o la modificación de las disposiciones ya existentes.

Para adaptar la disposición de creación de ficheros existentes a las previsiones del artículo 20 de la LOPD, se deberá publicar por cada fichero, las medidas de seguridad con indicación del nivel básico, medio o alto exigible y, en su caso, las transferencias de datos que se prevean a países terceros, así como, cualquier modificación que se hubiera produ-

cido en el resto de las previsiones del artículo 20.2 desde la publicación inicial de la disposición general publicada con anterioridad.

Asimismo, se podrían actualizar las denominaciones de los diferentes responsables de ficheros según sus estructuras actuales, obligaciones previstas en el artículo 20.

En este sentido, debe informarse que al finalizar 2001, el Ministerio de la Presidencia ya ha publicado la disposición general de adaptación a la Ley, mediante la Orden Ministerial de 23 de noviembre de 2001 (BOE nº 291, de 5 de diciembre de 2001).

También se ha publicado la Resolución de 27 de julio de 2001 de la Agencia de Protección de Datos por la que se ha adaptado la regulación de los ficheros de este Organismo (BOE nº 197, de 17 de agosto de 2001). Se da cuenta de ello en el epígrafe siguiente.

3.5. Norma de regulación de los ficheros de la Agencia de Protección de Datos

La Agencia de Protección de Datos tenía que aprobar la pertinente disposición de regulación de ficheros para la adecuación de los mismos a la LOPD, en los términos que establece el artículo 20.2 de la LOPD.

A fin de facilitar el conocimiento público de los ficheros de la Agencia en una sola disposición, la Resolución de 27 de julio de 2001 de la Agencia de Protección de Datos por la que se regula la adecuación de los ficheros de este Organismo (BOE nº 197, de 17 de agosto de 2001), deroga las anteriores disposiciones publicadas por esta Agencia de 18 de julio de 1994 y 7 de febrero de 1995, incorporando en un Anexo los ficheros ya regulados por aquéllas, con las modificaciones que la Ley o el transcurso del tiempo recomiendan. Además, se ha incluido la creación de dos nuevos ficheros ("Agenda de Comunicaciones" y "Gestión de consultas"), que no existían cuando se publicaron las anteriores Resoluciones.

Asimismo, se adaptan los ficheros contenidos en las anteriores Resoluciones a lo dispuesto en el artículo 20.2 de la LOPD indicando el nivel de medidas de seguridad básico, medio o alto correspondiente a cada uno de estos ficheros, en aplicación del Real Decreto 994/1999, de 25 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, las transferencias internacionales previstas y las normas con rango de Ley que habilitan las comunicaciones o cesiones de datos.

La aprobación de esta Resolución no ha supuesto la supresión de ningún fichero de datos de carácter personal, por lo que no ha sido necesaria la aplicación de lo dispuesto en el artículo 20.3 de la LOPD.

El texto completo de esta Resolución se puede consultar en los Anexos de esta Memoria.

3.6. Actualización de inscripciones de ficheros públicos

Los requerimientos y los escritos que se han tramitado desde el Registro a los diferentes responsables de titularidad pública, solicitando la actualización de las inscripciones, y que han tenido una especial repercusión durante 2001 han sido los correspondientes a las Comunidades Autónomas de Galicia, Andalucía, Castilla León, Madrid, La Rioja y Comunidad Valenciana.

En volumen, las notificaciones de la Junta de Galicia han sido las que han producido un mayor incremento en el número de inscripciones en el Registro. En particular, hay que citar por su importancia la regularización de la inscripción de los ficheros de la Consejería de Sanidad, incluyendo todos los Hospitales dependientes del Servicio Gallego de Salud (SERGAS).

Esta notificación ha producido también un aumento considerable en la cifra de inscripciones de ficheros con datos especialmente protegidos durante este año como puede comprobarse en el epígrafe "Registro en cifras".

Dado el tipo de datos declarados y las finalidades de los tratamientos, estas declaraciones han sido objeto de un análisis singular. Las notificaciones de los ficheros de Historias Clínicas, se han declarado con datos de religión amparados en la aplicación del art. 7.2 de la Ley, en relación con el art. 7.6. Este artículo excepciona la necesidad del consentimiento expreso y por escrito del afectado en la recogida de este tipo de datos, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

La Agencia ha procedido a la inscripción de esta notificación dado el carácter meramente declarativo, si bien el Director, en la Resolución, indicaba los términos en que debe aplicarse la excepción prevista en el artículo 7.6 de la Ley.

"Estos ficheros han sido inscritos con datos especialmente protegidos de religión, salud y vida sexual, amparándose en el art. 7.6 de la Ley Orgánica 15/1999, según manifiesta en la declaración el responsable del fichero. El régimen excepcional del citado artículo requiere la concurrencia de dos requisitos: a) que el tratamiento de dichos datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, y b) que el tratamiento de datos se realice por un profesional o por otra persona

obligada a equivalente secreto".

Respecto al resto de Comunidades Autónomas que han notificado actualizaciones de ficheros, cabe destacar que Andalucía ya había iniciado esta adecuación en 2000, finalizándola durante este año. La Comunidad Valenciana y la Comunidad Autónoma de Madrid, al tener, en el caso de Valencia, un órgano administrativo encargado de coordinar la creación de ficheros, y Madrid, su propia Agencia de Protección de Datos, son las Comunidades que mantienen con un índice mas alto de actualización su inscripción de ficheros.

En otro orden de cosas, se ha producido un impulso considerable en relación con las inscripciones de titulares de ficheros públicos en la Comunidad de La Rioja. Analizando este dato, puede considerarse que este incremento es debido al interés y concienciación que se produjo con las Jornadas sobre Administraciones Públicas y Protección de Datos que se impartieron en La Rioja.

Por último, a finales de 2001 se notificó la actualización de encuadramientos administrativos de los ficheros de la Comunidad Autónoma de la Región de Murcia.

3.6.1. *Disposiciones generales de la Administración General del Estado publicadas en el Boletín Oficial del Estado en 2001*

Ministerio de Economía.
* Resolución de 5 de diciembre de 2000, de la Comisión Nacional de Energía, por la que se crean y modifican ficheros automatizados de datos de carácter personal en este organismo. (BOE nº 34, 8-2-2001).
* Resolución de 22 de enero de 2001, de la Presidencia de la Comisión del Mercado de las Telecomunicaciones, por la que se crea el fichero automatizado de suscriptores al servicio de noticias de la Comisión del Mercado de las Telecomunicaciones. (BOE nº 50, 27-2-2001).
* Orden de 11 de diciembre de 2001 por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda. (BOE nº 311, 28-12-2001).

Ministerio de la Presidencia.
* Orden de 23 de noviembre de 2001 por la que se regulan los ficheros automatizados que contienen datos de carácter personal gestionados por el Ministerio de la Presidencia y Organismos Autónomos adscritos al mismo. (BOE nº 291, 5-12-2001).

Ministerio del Interior.
* Orden de 5 de febrero de 2001 por la que se crean en la Delegación del Gobierno para el Plan Nacional sobre Drogas diversos ficheros automatizados de datos de carácter personal. (BOE nº 41, 16-2-2001).
* Orden de 30 de julio de 2001 por la que se crea en la Delegación del Gobierno para el Plan Nacional sobre Drogas el fichero automatizado de datos de carácter personal denominado "Folleto". (BOE nº 190, 9-8-2001).
* Orden de 4 de octubre de 2001 por la que se regula el fichero automatizado de terceros de la aplicación SOROLLA en la Dirección General de la Guardia Civil. (BOE nº 250, 18-10-2001).

Ministerio de Sanidad y Consumo.
* Orden de 18 de diciembre de 2000 por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH). (BOE nº 11, 12-1-2001).
* Orden de 28 de marzo de 2001 por la que se amplía la de 21 de julio de 1994 por la que se regulan los ficheros con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo. (BOE nº 93, 18-4-2001)
* Orden de 18 de julio de 2001 por la que se crea un fichero con datos de carácter personal, gestionado por el Instituto de Salud "Carlos III", del Ministerio de Sanidad y Consumo, relativo al proyecto Itínere.
(BOE nº 188, 7-8-2001).
* Orden de 10 de septiembre de 2001 por la que se crea y regula un nuevo Fichero de Investigadores del Sistema Nacional de Salud con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo. (BOE nº 226, 20-9-2001).

Ministerio de Trabajo y Asuntos Sociales.
* Orden de 25 de junio de 2001, por la que se crean, modifican y suprimen ficheros automatizados de datos de carácter personal gestionados por el Ministerio de Trabajo y Asuntos Sociales. (BOE nº 165, 11-7-2001).

Ministerio de Fomento.
* Orden de 13 febrero 2001, por la que se amplía la relación de ficheros automatizados de datos de carácter personal del Ministerio de Fomento. (BOE nº 51, 28-2-2001).
* Orden de 11 de abril de 2001 por la que se amplía la relación de ficheros automatizados de datos de carácter personal en el Ministerio de Fomento. (BOE nº 102, 28-4-2001).

Ministerio de Defensa.
* Orden 69/2001, de 29 de marzo, por la que se amplía la Orden 75/1994, de 26 de julio, por la que se regulan los ficheros de tratamiento automatizado de datos de carácter personal existentes en el Ministerio de Defensa. (BOE nº 85, 9-4-2001).

Agencia de Protección de Datos.
* Resolución de 27 de julio de 2001, de la Agencia de Protección de Datos, por la que se crean y modifican ficheros de datos de carácter personal de la Agencia. (BOE nº 197, 17-8-2001).

3.6.2. *Disposiciones generales de la Administración Autonómica publicadas en 2001*

Junta de Andalucía.
* Resolución de 08 de febrero de 2001 del Instituto de Fomento BOJA 25 de 01/03/01.
* Orden de 24 de julio de 2001 de la Consejería de Salud BOJA 95 de 18/06/01.

Comunidad Autónoma de Aragón.
* Orden de 20 de abril de 2001 de la Departamento de Medio Ambiente BOA 55 de 11/05/01.

Comunidad Autónoma de Canarias.
* Orden de 25 de enero de 2001 de la Consejería de Presidencia BOC 18 de 07/02/01.
* Orden de 12 de septiembre de 2001 de la Consejería de Sanidad y Consumo BOC 146 de 09/11/01.

Comunidad Autónoma de Cantabria.
* Orden de 19 de junio de 2001 de la Consejería de Sanidad, Consumo y Servicios Sociales BOC 132 de 10/07/01.

Comunidad Autónoma de Castilla La Mancha.
* Orden de 22 de marzo de 2001 de la Consejería de Administraciones Públicas DOCM 59 de 18/05/01.
* Orden de 20 de julio de 2001 de la Consejería de Agricultura y Medio Ambiente DOCM 84 de 27/07/01

Comunidad Autónoma de Castilla León.
* Orden de 6 de julio de 2001 de la Consejería de Industria, Comercio y Turismo BOC y L 160 de 17/08/01.
* Orden de 31 de agosto de 2001 de la Consejería de Industria, Comercio y Turismo BOC y L 196 de 08/10/01.

Comunidad Autónoma de Cataluña.
* Decreto 418 de 5 de diciembre de 2000 del Departamento de Sanidad y Seguridad Social DOGC 3305 de 15/01/01.
* Decreto 87 de 20 de marzo de 2001 del Departamento de Política Territorial y Obras Públicas DOGC 3360 de 02/04/01.

Comunidad Autónoma de Extremadura.
* Orden de 9 de mayo de 2001 de la Consejería de Cultura DOE 66 de 09/06/01.

Comunidad Autónoma de Galicia.
* Orden de 02 de febrero de 2001 de la Consejería de Sanidad y Servicios Sociales DOGA 40 de 26/02/01.
* Orden de 20 de abril de 2001 de la Consejería de Familia y Promoción del Empleo, Mujer y Juventud DOGA 89 de 09/05/01.
* Orden de 30 de mayo de 2001 de la Consejería de Familia y Promoción del Empleo, Mujer y Juventud DOGA 113 de 12/06/01.
* Orden de 21 de junio de 2001 de la Consejería de Presidencia y Administración Pública DOGA 130 de 05/07/01.
* Orden de 3 de octubre de 2001 de la Consejería de Sanidad y Servicios Sociales DOGA 207 de 25/10/01.

Comunidad Autónoma de Madrid.
* Ordenes 1725/01 y 1726/01, corrección del Decreto 76/01 y Decretos 76/01 y 78/01 respectivamente de la Consejería de la Presidencia. BOCM 288/01, 200/01, 145/01, y 145/01.
* Orden 3318/01 de la Consejería de Economía e Innovación Tecnológica. BOCM 296/01.
* Decretos 135/01, 125/01, 95/01, 84/01, y 29/01 respectivamente de la Consejería de Economía y Empleo. BOCM 213/01, BOCM 164/01, BOCM 156/01, y BOCM 60/01.
* Orden de 16 de octubre de 2001 de la Consejería de Hacienda. BOCM 267/01.
* Orden 2285/01 de la Justicia y Administraciones Públicas. BOCM 289/01.
* Órdenes 5181/01, 3820/01, 3819/01 y 3738/01, corrección del Decreto 117/01, y Decretos 117/01, 71/01, 69/01, 52/01 respectivamente de la Consejería de Educación. BOCM 281/01, 233/01, 228/01, 216/01, 173/01, 134/01, 107/01.
* Orden de 249 de 13 de noviembre de 2001 de la Consejería de Trabajo. BOCM 279/01.
* Orden 5552 de 6 de noviembre de 2001 de la Consejería de Medio Ambiente. BOCM 275/01.
* Ordenes 672/01 y 614/01, y Decreto 10/01 respectivamente de la Consejería de Sanidad. BOCM 248/01, 230/01, 32/01.
* Orden 1670/01, y Decretos 71/01, 49/01, y 38/01 respectivamente de la Consejería de Servicios Sociales BOCM 134/01, 99/01, y 70/01.
* Decretos 70/01, 56/01, y 43/01 respectivamente de la Consejería de Cultura BOCM 134/01, 111/01, y 75/01.
* Decretos 127/01, 54/01, 21/01, y 14/01 respectivamente de la Consejería de Obras Públicas, Urbanismo y Transportes BOCM 198/01, 110/01, 52/01, y 36/01.

Comunidad Autónoma de la Región de Murcia.
* Ordenes 25 y 26 de enero de 2001 de la Consejería de Economía y Hacienda BORM 35 de 12/02/01.
* Orden de 15 de febrero de 2001 de la Consejería de Economía y Hacienda BORM 48 de 27/02/01.Ordenes de 9 y 12 de marzo de 2001 de la Consejería de Economía y Hacienda BORM 70 de 26/03/01.

Comunidad Autónoma de Navarra.
* Orden Foral 77 de 12 de marzo de 2001 del Departamento de Educación y Cultura BON 47 de 16/04/01.
* Decreto Foral 58 de 28 de marzo de 2001 de la Comunidad Foral de Navarra BON 60 de 16/05/01.
* Orden Foral 142 de 11 de abril de 2001 del Departamento de Educación y Cultura BON 65 de 28/05/01.
* Orden Foral 136 de 4 de abril de 2001 del Departamento de Educación y Cultura BON 55 de 4 de mayo de 2001.
* Orden Foral 226 de 15 de junio de 2001 del Departamento de Educación y Cultura BON 88 de 20/07/01.
* Orden Foral 345 de 10 de septiembre de 2001 del Departamento de Educación y Cultura BON 119 de 01/10/01.

Comunidad Autónoma de la Rioja.
* Orden 51 de 9 de mayo de 2001 de la Consejería de Desarrollo Autonómico y Administraciones Públicas BOLR 59 de 17/05/01.

Comunidad Valenciana.
* Resolución de 7 de febrero de 2001 de Presidencia DOGV 3945 DE 22/02/01.
* Orden de 8 de febrero de 2001 de la Consejería de Justicia y Administraciones Públicas DOGV 3951 de 02/03/01.
* Orden de 12 de febrero de 2001 del Portavoz del Gobierno DOGV 3951 de 12/02/01.
* Orden de 27 de marzo de 2001 del Portavoz del Gobierno DOGV 3979 de 12/04/01.
* Orden de 28 de marzo de 2001 del Portavoz del Gobierno DOGV 3989 de 30/04/01.
* Orden de 20 de abril de 2001 de la Consejería de Bienestar Social DOGV 3991 de 03/05/01.
* Orden de 3 de mayo de 2001 de la Consejería de Sanidad DOGV 4038 de 09/07/01.
* Resolución de 7 de mayo de 2001 de la Consejería de la Presidencia DOGV 4000 de 16/05/01.
* Orden de 7 de mayo de 2001 de la Consejería de Economía, Hacienda y Empleo DOGV 4013 de 04/06/01.
* Resolución de 31 de mayo de 2001 de la Consejería de la Presidencia DOGV 4019 de 12/06/01.
* Orden de 20 de junio de 2001 de la Consejería de Economía, Hacienda y Empleo DOGV 4036 de 05/07/01.
* Orden de 6 de agosto de 2001 de la Consejería de Medio Ambiente DOGV 4067 de 20/08/01.
* Resolución de 7 de agosto de 2001 de la Consejería de Bienestar Social DOGV 4074 de 29/08/01.
* Orden de 24 de octubre de 2001 de la Consejería de Economía, Hacienda y Empleo DOGV 4125 de 12/11/01.

3.7. Agencia de Protección de Datos de la Comunidad de Madrid

La LOPD ha ampliado las competencias de las Agencias Autonómicas regulando en su art. 41.1 que las funciones de su competencia "serán ejercidas cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido."

La nueva Ley de Protección de Datos de la Comunidad de Madrid, publicada en el mes de julio de 2001, ha regulado las competencias de la Agencia autonómica habiéndose ampliado el ámbito de aplicación en previsión al art. 41.1 de la LOPD a los ficheros de la Administración Local de su ámbito territorial y corporaciones de derecho público representativas de intereses económicos y profesionales del ámbito territorial de la Comunidad de Madrid.

Dado que hasta este momento, los ficheros de esas entidades dependían plenamente de la Agencia, y con el objeto de facilitar la nueva tarea a la Agencia de Madrid, en el marco de colaboración que se ha venido manteniendo entre ambas, desde su creación, el Registro General de Protección de Datos remitió una copia en el mes de octubre del contenido de la inscripción de ficheros correspondientes a estas entidades.

3.8. Actuaciones relacionadas con la Inspección de Datos

* Ayuntamientos

Tras los reiterados requerimientos citados en memorias anteriores y en particular los que se realizaron a finales de 2000, se reiteró el requerimiento a 92 Ayuntamientos de poblaciones superiores a 4000 habitantes que no habían notificado hasta ese momento ningún fichero al Registro para su inscripción.

Como contestación a ese requerimiento en el mes de junio de 2001 habían notificado para su inscripción los ficheros de los Ayuntamientos de 11 municipios, otros 17 Ayuntamientos se encontraban tramitando las correspondientes disposiciones de creación de ficheros y cuatro se encontraban en el ámbito territorial de la Comunidad de Madrid.

En relación con los cuatro Ayuntamientos de la provincia de Madrid, se remitió la comunicación correspondiente a la Agencia de Protección de Datos de Madrid, ya que en ese momento estaba asumiendo las competencias sobre las entidades locales.

Con los 60 Ayuntamientos restantes que no habían contestado al requerimiento, se dio traslado a la Inspección de Datos a los efectos de que se iniciaran los correspondientes expedientes sancionadores en los términos del art. 46 de la Ley.

A partir de ese momento, se ha recibido la solicitud de inscripción de doce de los Ayuntamientos. No obstante, la Inspección ha continuado la tramitación de los correspondientes expedientes.

* Consorcio de Compensación de Seguros

A partir de las actuaciones llevadas a cabo por la Inspección de Datos, dentro de los planes de oficio del año 2000, al Consorcio de Compensación de Seguros se habían detectado algunos aspectos relacionados con la inscripción en el Registro que no se correspondían con la situación real.

Estas variaciones se producían en los apartados de *Estructura básica y tipo de datos* y en el de *Medidas de Seguridad*. En el año 2001 el Consorcio procedió a notificar las modificaciones correspondientes quedando debidamente inscritos sus ficheros.

4. INSCRIPCIÓN DE FICHEROS DE TITULARIDAD PRIVADA

La inscripción de ficheros de titularidad privada durante este año, ha estado condicionada por varios motivos. Uno de ellos ha sido la revisión que los responsables de los ficheros han realizado, durante los últimos años, en sus sistemas de información, para su adaptación al efecto 2000 y a la moneda única.

Por otra parte, en algunos sectores empresariales, como el bancario, asegurador y el farmacéutico, entre otros, han continuado las operaciones de fusión y absorción, ya señaladas en memorias anteriores. Algunos de estos cambios de la estructura organizativa del responsable del fichero, han tenido una repercusión reseñable en la inscripción en el RGPD durante el año 2001.

Otro de los motivos, quizás de más importancia que los anteriores, a los efectos de inscripción, ha sido la adaptación de los tratamientos al Reglamento de Medidas de Seguridad y a las nuevas previsiones de la Ley 15/1999.

Por un lado, los sistemas de información que deben cumplir las medidas calificadas de nivel medio y alto, están obligados a realizar auditorías internas o externas para verificar la adecuación de las medidas de seguridad, de conformidad con el artículo 17 del Reglamento. Esta obligación ha supuesto que se hayan detectado situaciones en las que las inscripciones de los ficheros en el RGPD, no reflejaban la situación real de los sistemas de información del responsable.

Además, la finalización del plazo para la adopción de las medidas de seguridad de nivel alto el día 26 junio de 2001, ha traído consigo una cantidad importante de solicitudes de inscripción durante estas fechas, situación que se puede comprobar en la tabla correspondiente. No obstante, mediante resolución del Ministerio de Justicia de 22 de junio de 2001 por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información, se estableció que este plazo se ampliaba hasta el 26 de junio de 2002.

Como ya se ha señalado anteriormente, también ha influido el fin del plazo transitorio (14 de enero de 2003) establecido en la Disposición Adicional Primera de la LOPD para adecuar los ficheros preexistentes a la entrada en vigor de la Ley. Esta adecuación de los ficheros preexistentes, únicamente se traduce en la necesidad de completar las inscripciones de ficheros con el nivel de seguridad.

Por otro lado, este período transitorio también se aplica a los ficheros que la LORTAD consideraba fuera del ámbito de aplicación en su artículo 2.21, sin embargo, la LOPD no los cita en las previsiones de excepciones establecidas en el ámbito de aplicación en su artículo 2.2.

4.1. Evolución y criterios en la inscripción de ficheros de titularidad privada

Durante el año 2001, del total de las modificaciones de la inscripción solicitadas de titularidad privada (3.674), un 55% (2.026) han modificado una parte importante de la inscripción (3 o más apartados). Los apartados que han sido modificados en un mayor número de casos, han sido el de responsable del fichero o tratamiento, el de encargado del tratamiento, las medidas de seguridad, nombre del fichero, sistemas de tratamiento y estructura de datos.

Del total de operaciones de supresión realizadas a solicitud de los responsables de ficheros de titularidad privada (2.903), el 69% han tenido como motivo de la supresión la modificación de los sistemas de información y el 16% causas relacionadas con el cese de la actividad del responsable, fusión o absorción de empresas. El resto de las supresiones han tenido como motivo declarado de las mismas la destrucción de los datos por no ser necesarios para la actividad para la que se crearon los ficheros, no contener datos de carácter personal, etc.

Al notificar los cambios producidos en la inscripción, algunos responsables han optado por realizar nuevas inscripciones y proceder, al mismo tiempo, a la supresión de los ficheros inscritos, mientras que en otros casos han optado por solicitar las modificaciones de las inscripciones realizadas en años anteriores.

En relación con estos cambios resulta pertinente señalar que no existe un desarrollo reglamentario que establezca el procedimiento a seguir en estos casos. De esta manera queda a criterio del responsable del fichero optar por solicitar una modificación, o bien, solicitar una nueva inscripción, junto con la supresión del fichero que constaba inscrito anteriormente.

En otros casos, las adaptaciones de los sistemas de información, han llevado a los responsables de los ficheros a solicitar nuevas inscripciones de ficheros con finalidades similares a la de tratamientos que ya constaban inscritos, debido

a que en ciertos casos, desconocían la existencia de inscripciones iniciales. Esta circunstancia ha implicado la necesidad de realizar controles, tanto con carácter previo a la inscripción, como a posteriori, con el fin de detectar la existencia de inscripciones duplicadas. Este hecho ha obligado a requerir al responsable del fichero con el fin de que se hicieran efectivas, a efectos registrales, las oportunas modificaciones para reflejar la situación real.

Además, se ha puesto especial atención en informar a los responsables de la necesidad de mantener actualizada y operativa la dirección dónde los afectados puedan ejercer los derechos de oposición, acceso, rectificación y cancelación previstos en la LOPD, toda vez que ésta es la finalidad fundamental del Registro.

Por otra parte, en algunos casos se ha puesto de manifiesto que se estaba solicitando la inscripción en el RGPD desde diversos departamentos de una misma entidad, existiendo la duda de si dichas solicitudes se estaban realizando por duplicado o de una forma coordinada. Esta situación se ha puesto de manifiesto en grandes entidades que tienen una organización territorial.

A este respecto, y con el fin de evitar esta situación, sería recomendable que las entidades establezcan una figura que pudiera coordinar la comunicación con el RGPD, a los efectos de mejorar y centralizar todas las previsiones formales que la ley exige.

En este sentido, la Directiva 95/46/CE recoge en su artículo 18, la figura del encargado de protección de datos personales, designado por el responsable del fichero, que tendría los cometidos de hacer aplicar en el ámbito interno de las organizaciones, las disposiciones nacionales de protección de datos, así como llevar un registro de los tratamientos efectuados por el responsable del tratamiento.

Otra circunstancia que se ha detectado, se refiere a los casos en los que se notifica un único fichero con finalidades que podrían resultar incompatibles entre sí, o que los datos y colectivos que se incluyen en los mismos no se rigen por las mismas previsiones legales, como por ejemplo el colectivo de empleados y el de clientes. En estos casos, los datos de estos colectivos no serían recabados para la misma finalidad.

Cuando los datos se recaben del colectivo de empleados, la finalidad legítima del tratamiento sería la relativa a la gestión de los recursos humanos, gestión de nóminas, etc. En el caso de la gestión de clientes, la finalidad legítima estaría relacionada con las necesarias para desarrollar la relación contractual.

Al declarar un único tratamiento, se está notificando que se recaban distintos tipos de datos, entre los que pueden estar incluidos datos especialmente protegidos de salud y afiliación sindical, que no son adecuados para las finalidades de gestión comercial, pero que sí resultan pertinentes y no excesivos para la finalidad de gestión de recursos humanos, además de ser necesario adoptar un nivel de medidas de seguridad distinto para cada tratamiento.

Es criterio del Registro, que en estos casos, en los que existan finalidades que podrían resultar incompatibles, colectivos, tipos de datos y medidas de seguridad diferentes, se deben declarar tratamientos diferentes.

Por otra parte, se producen confusiones debido a la dificultad de distinguir cuándo un responsable proporciona los datos de carácter personal a un encargado del tratamiento, según lo previsto en el artículo 12 de la LOPD, o cuándo los cede a un tercero según lo establecido en el artículo 11 de la citada ley.

La LOPD define en el artículo 3 g) como "*Encargado del tratamiento, la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero"* y en el artículo 12 que "*No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento* ".

Por su parte, el artículo 11.2 de la citada Ley, en su apartado c), establece como excepción al principio cardinal de la existencia del consentimiento del interesado para realizar la cesión de datos, "*cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique* ".

No obstante, es importante hacer notar la diferencia fundamental existente entre un caso y otro, y que viene establecida en los apartados 2, 3 y 4 del artículo 12 de la ley, que establecen que:

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal

objeto del tratamiento.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

A efectos de inscripción, únicamente se considerará encargado del tratamiento a la persona física o jurídica que trate datos por cuenta del responsable y, en estos casos, el encargado nunca deberá figurar en el RGPD, como entidad responsable de los ficheros o tratamientos. Si el responsable del fichero tuviera previsto realizar tratamientos por cuenta de terceros, y fueran entidades distintas las que prestaran estos servicios, en los términos a que se refiere el artículo 12 de la LOPD, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.

Otra situación que se está poniendo de manifiesto con frecuencia, es la presentación de notificaciones en las que se cumplimentan los apartados del modelo de declaración con llamadas a anexos que se acompañan a la solicitud de inscripción, en el que figuran varios encargados de tratamiento que no pueden incluirse en el modelo de notificación ya que en el mismo únicamente está previsto la declaración de un encargado.

En el caso de que existan varios encargados del tratamiento y se desee que esta información conste en el RGPD, se recomienda que se consignen en el apartado correspondiente los datos del encargado del tratamiento principal. El resto de los encargados del tratamiento, se podrán comunicar, mediante un escrito adjunto a la notificación para que el RGPD tome nota a los efectos informativos.

Esta situación también puede resolverse declarando tratamientos diferentes, en los que se hiciera constar cada uno de los encargados de tratamiento que el responsable quiere que consten inscritos.

Por último, en algunas notificaciones que utilizan el modelo en soporte papel, se declara la información relativa a algunos apartados en anexos, en lugar de utilizar el espacio destinado a tal fin en el modelo normalizado de notificación.

Es necesario tener en cuenta que el modelo normalizado de notificación ha de cumplimentarse conforme a las instrucciones que lo acompañan, no pudiendo hacer constar los datos que se solicitan en un lugar distinto del previsto a estos efectos en el modelo. No obstante, si el responsable desea hacer alguna aclaración adicional a la declaración, puede acompañar junto al modelo de notificación, correctamente cumplimentado, un escrito en el que se incluyan las aclaraciones que considere necesarias a su declaración.

El artículo 26.3 de la Ley Orgánica 15/1999 obliga a notificar cualquier modificación posterior que se hubiera producido en el contenido de los extremos a que se refiere el artículo 26 de la LOPD. El artículo 26.3 hace una referencia expresa a las variaciones que se hayan producido en la finalidad del fichero, en su responsable o en la dirección de la ubicación.

Como ocurre también en los ficheros de titularidad pública, la falta de notificación podría suponer una infracción conforme al artículo 44 de la LOPD, siendo de aplicación el régimen sancionador previsto en la misma. A este respecto, el artículo 44.2 establece, en su apartado c), que se considera infracción leve, no solicitar la inscripción del fichero de datos de carácter personal en el RGPD, cuando no sea constitutivo de infracción grave.

El artículo 6 del Real Decreto 1332/1994 establece que la persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos en modelo normalizado que al efecto elabore la Agencia, en el que se especificarán los siguientes extremos:

a) Nombre, denominación o razón social, documento nacional de identidad o código de identificación fiscal, dirección y actividad u objeto social del responsable del fichero.
b) Ubicación del fichero.
c) Identificación de los datos que se pretendan tratar, individualizando los supuestos de datos especialmente protegidos.
d) Dirección de la oficina o dependencia en la cual puedan ejercerse los derechos de acceso, rectificación y cancelación.
e) Origen o procedencia de los datos.
f) Finalidad del fichero.
g) Cesiones de datos previstas.
h) Transferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos.
i) Destinatarios o usuarios previstos para las cesiones o transferencias.
j) Sistemas de tratamiento automatizado que se vayan a utilizar.
k) Medidas de seguridad.

El artículo 8.2 del citado Reglamento obliga en el caso de ficheros de titularidad privada a que cualquier modificación posterior en el contenido de los extremos a que se refiere el artículo 6 citado anteriormente, se comunicará, a efectos de inscripción, en su caso, a la Agencia de Protección de Datos dentro del mes siguiente a la fecha en que aquélla se hubiera producido. En igual plazo se comunicará la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

La falta de este trámite podría ser considerada una infracción grave, conforme al artículo 44.3.i), que establece como tal, no remitir a la Agencia de Protección de Datos las notificaciones previstas en la Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquella a tales efectos.

A su vez, se considera infracción grave en previsión del artículo 44.3.k), no inscribir el fichero de datos de carácter personal en el RGPD, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

4.2. Inscripción de ficheros en el ámbito de Internet.

La actividad en el entorno de Internet ha continuado desarrollándose a lo largo del año 2001, lo que ha llevado aparejado un incremento en la declaración de tratamientos que recogen y tratan datos de carácter personal en la red. En la memoria de la Agencia del año 2000, se hacía referencia a diversos aspectos relacionados con el tratamiento de datos de carácter personal en Internet, tanto desde el punto de vista de la legislación aplicable, como de la problemática específica en relación con la inscripción de este tipo de tratamientos.

A partir de la publicación de las recomendaciones al sector del comercio electrónico, disponible en la página web de la Agencia, se ha informado a los responsables de los tratamientos relacionados con este sector de la existencia de estas recomendaciones, en relación con la justificación del consentimiento del afectado para la realización de transferencias internacionales.

Como parte de la información que se ha de facilitar al interesado, las citadas recomendaciones señalan que, además de la exigida por el citado artículo 5 de la LOPD, "*se especificará una referencia al código de inscripción asignado por el Registro General de Protección de Dato* s".

La inclusión de la referencia al código de inscripción, es de especial relevancia, de cara a facilitar, con eficacia, el ejercicio de los derechos previstos en la LOPD, de tal manera que se puedan identificar con claridad los datos registrales del fichero donde se han almacenado los datos de carácter personal del interesado. Además, esta referencia actúa como valor añadido, en el sentido de generar una mayor confianza en el usuario, al poder constatar que la entidad responsable del fichero, ha cumplido con las exigencias legales, en materia de inscripción al RGPD.

Durante 2001 se han inscrito 426 ficheros, cuyos responsables declaran que realizan tratamientos relacionados con el comercio electrónico. Estos tratamientos incluyen transacciones entre particulares y empresas, así como entre empresas, grandes superficies, subastas, portales corporativos de empresas que ofrecen algún servicio añadido, portales de contenidos diversos, concursos, recopilación de direcciones, prestadores de servicios de telecomunicación, entidades registradoras de dominios, entidades que gestionan los servicios de búsqueda, entidades de certificación de firma digital, gestión del curriculum vitae para buscar empleo en la red, etc.

Por la propia naturaleza de los tratamientos que utilizan Internet como medio, se pone de manifiesto que muchas de estas entidades realizan transferencias internacionales de datos de carácter personal, con el fin de prestar el servicio solicitado. Esta circunstancia se explica en el apartado de esta memoria que trata sobre transferencias internacionales.

4.3. Inscripción de ficheros de titularidad privada con datos especialmente protegidos de ideología, creencias, religión y afiliación sindical

El artículo 7.2 de la Ley, señala que los datos especialmente protegidos de ideología, creencias, religión y afiliación sindical son datos que únicamente pueden ser recabados con el consentimiento expreso y por escrito del afectado.

Durante el año 2001 se han inscrito un total de 730 ficheros con datos especialmente protegidos de ideología, creencias, religión y afiliación sindical. Se han inscrito 619 ficheros, cuyos responsables han declarado el tratamiento de datos relativos a la afiliación sindical, la mayor parte de ellos relacionados con lo previsto en la Ley Orgánica de Libertad Sindical, con la finalidad de hacer efectivo el pago de la cuota a la organización sindical correspondiente, a solicitud del afiliado.

En la LORTAD, no se citaba expresamente la afiliación sindical como un tipo de dato especialmente protegido, por lo que no se incluía en el modelo normalizado de notificación de ficheros. Al carecer el modelo de notificación de un apartado específico para declarar este tipo de datos, en algunas declaraciones se señalaba el tipo de dato de ideología. Este hecho explica que las cifras de este año, relativas a los datos de ideología, se hayan reducido notablemente, una vez que el nuevo modelo de notificación incluye un apartado específico para declarar los datos de afiliación sindical.

Durante el año 2001, se han inscrito 13 ficheros cuyos responsables han declarado que recaban datos especialmente protegidos de ideología. La mayor parte de ellos, se refieren a los tratamientos relacionados con la declaración de la renta y tratamientos realizados por organizaciones no gubernamentales (ONG) y partidos políticos. En todos estos casos, se ha declarado que este tipo de dato ha sido recabado con el consentimiento expreso y por escrito del afectado.

Por lo que se refiere a los datos especialmente protegidos de religión, durante el año 2001, se han inscrito 142 ficheros que incluyen este tipo de datos. El incremento con respecto al año anterior ha sido relevante, dado que en 2000 se inscribieron únicamente 31 ficheros con ese tipo de dato. La mayor parte de estos tratamientos se enmarcan en la

confección de autoliquidaciones del IRPF, Impuesto sobre el Patrimonio y las deducciones por inversiones y donativos. Por otra parte, en algunos casos, los titulares de estos ficheros son colegios que han declarado que recaban datos de religión, dentro del marco del currículum escolar.

El incremento de la inscripción de ficheros que incluyen en su declaración datos especialmente protegidos relativos a las creencias, se refiere a los tratamientos relativos a la tramitación de la declaración de la renta, anteriormente señalado, datos relativos a los voluntarios de algunos centros asistenciales pertenecientes a ordenes religiosas y expedientes de despachos de abogados que han justificado que este tipo de dato es necesario para la defensa de sus clientes.

En todas ellas, se ha procedido a requerir a los responsables de los ficheros cuando del contenido de su declaración se observaban dudas razonables, en relación con la pertinencia del tratamiento de este tipo de datos. En todos los casos requeridos, el responsable ha justificado la necesidad del tratamiento de esos datos, o ha subsanado, comunicando que se habían producido errores en su notificación inicial.

Únicamente dos de estos ficheros, uno de ellos relativo a los miembros de una orden religiosa, y el otro declarado por un partido político, se han amparado en la excepción prevista en el segundo inciso del artículo 7.2, que excepciona del consentimiento expreso y por escrito para tratar datos especialmente protegidos de ideología, afiliación sindical, religión y creencias a "*los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado* ".

Este supuesto no se contemplaba en el modelo anterior, ya que la LORTAD, excluía del ámbito de aplicación de la ley, en su artículo 2.e "*a los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieren a sus asociados o miembros y ex-miembros ...*". No obstante, es necesario recordar que los ficheros que anteriormente estaban exceptuados del ámbito de aplicación de la LORTAD y la Ley vigente los incluye en su ámbito, tienen un plazo transitorio hasta el 14 de enero de 2003 para declararlos.

4.4. Inscripción de ficheros de titularidad privada con datos especialmente protegidos de origen racial, salud y vida sexual

Por su parte, el artículo 7.3 de la LOPD establece que los datos relativos al origen racial, a la salud y a la vida sexual, *"sólo podrán ser recabados, tratados y cedidos, cuando por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".*

Durante el año 2001, se ha experimentado un extraordinario incremento de las inscripciones de ficheros cuyos responsables han declarado el tratamiento de datos especialmente protegidos de origen racial, salud y vida sexual de los afectados. Se han inscrito un total de 5.859 ficheros con este tipo de dato, frente a los 769 ficheros que se inscribieron con el mismo tipo de dato, durante el año anterior.

Fundamentalmente, dos han sido las causas de este incremento, la notificación de tratamientos relacionados con la gestión de nóminas, recursos humanos y fiscal, y la inscripción realizada a solicitud de los responsables de oficinas de farmacia, centros sanitarios y profesionales médicos.

La recogida y el tratamiento de los datos especialmente protegidos de salud en el entorno de gestión de nóminas está motivada por la declaración del dato del grado de minusvalía para el cálculo de las retenciones prevista en la legislación del IRPF. Cuando el fichero incluye las fechas de alta y baja de los trabajadores por razón de enfermedad, asociados a un código que identifique la causa de la baja como enfermedad profesional, accidente laboral o enfermedad común, se considera que incluyen y tratan datos de salud, por lo tanto, en ambos casos, se debe declarar el tipo de dato de salud en el apartado correspondiente de *Estructura básica y descripción de los tipos de datos / otros datos especialmente protegidos* .

La consideración de este tipo de información como un dato de salud, y la consiguiente obligatoriedad de implantar las medidas de nivel alto, hace que los sistemas informáticos que tratan este tipo de datos de carácter personal relativos a las cotizaciones a la seguridad social y a las retenciones del I.R.P.F. tengan que adoptar las medidas de nivel alto.

El artículo 23 del Reglamento de Medidas de Seguridad, establece que la distribución de soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Asimismo, el artículo 24 del Reglamento de Medidas de Seguridad, dispone para este tipo de datos la obligación de implantar un registro de accesos.

Es cada día más común que las normas legales citen circunstancias personales y familiares del perceptor que haya que tener en cuenta por el pagador para la aplicación de porcentaje de retención correspondiente.

En relación con los tratamientos cuya finalidad es la gestión de nóminas de la cual se obtienen las cotizaciones a la

Seguridad Social, es necesario tratar los datos de fechas de alta y baja de los trabajadores por razón de enfermedad, asociados a un código que identifique la causa de baja como enfermedad profesional, accidente laboral o enfermedad común, la consideración de este tipo como un dato de salud hace necesario aplicar las medidas de seguridad de nivel alto anteriormente expuesto.

Esta problemática, ha puesto de manifiesto la existencia de un colectivo de responsables, cuyos tratamientos se encuentran obligados a tener implantadas las medidas de seguridad calificadas de nivel alto, con la consiguiente dificultad y coste al acometer los requerimientos que el reglamento de medidas de seguridad exige para este nivel de seguridad.

Esto hace conveniente contemplar la necesidad de estudiar el establecimiento de determinadas excepciones a la obligación de adoptar las medidas de nivel alto, para determinados tratamientos de datos, con el fin de que no conlleve una dificultad y coste excesivo, teniendo en cuenta que estos responsables recaban este tipo de datos obligados por la legislación específica.

Todo ello limitado a los supuestos en que el tratamiento de estos datos venga exigido por disposiciones legales y se evite la realización de tratamientos con fines diferentes.

Por lo que respecta a los datos especialmente protegidos de origen racial, se han inscrito 50 ficheros de titularidad privada que incluyen este tipo de dato en su declaración. Las finalidades declaradas de estos ficheros están relacionadas con el mantenimiento del historial clínico, la orientación psicopedagógica, estudios epidemiológicos y de reacciones adversas a los medicamentos.

Por su parte, los 58 ficheros que se han inscrito durante el año 2001, cuyos responsables han declarado que se recababan datos especialmente protegidos de vida sexual, se refieren, en su mayoría, a los datos relativos a la salud incluidos en los tratamientos cuya finalidad es la de mantener el historial clínico del paciente. Hay que hacer la aclaración de que cuando este tipo de datos se refiere a determinadas enfermedades, como por ejemplo las de transmisión sexual, se debe consignar como un dato relativo a la salud del afectado y no como un dato referente a la vida sexual.

Además, se han declarado datos especialmente protegidos de vida sexual en tratamientos relacionados con contactos personales, defensa jurídica de los clientes de bufetes de abogados, participación en concursos de televisión que implican unas especiales condiciones de convivencia entre los participantes, etc.

De los 5.851 ficheros de titularidad privada inscritos con datos especialmente protegidos de salud, solamente el 11% (654 ficheros) han declarado que recaban, tratan y ceden los datos, únicamente amparados en la existencia de una ley que, por razones de interés general, así lo dispone.

Las leyes declaradas por los responsables de los ficheros para tratar este tipo de datos son, mayoritariamente, la Ley General de Sanidad, la Ley del Medicamento, la Ley de Prevención de Riesgos Laborales y la Ley del Impuesto sobre la Renta de las Personas Físicas.

4.5. Responsable de ficheros establecido fuera del territorio español

Durante el año 2001 se han inscrito en el RGPD un total de 12 ficheros, pertenecientes a 10 empresas cuyas sedes sociales se encuentran fuera del territorio español. La mayor parte de estos responsables se encuentran establecidos en países de la Unión Europea (8), mientras que únicamente 2 responsables han declarado que se encuentran establecidos en países que no pertenecen a la Unión Europea, como es el caso de Estados Unidos de América y Suiza.

En el caso de las entidades cuyas sedes no se encuentran establecidas en un país perteneciente a la Unión Europea, ha sido necesario requerir a los responsables de los ficheros, con el fin de determinar que los tratamientos que solicitan inscribir se encontraban dentro del ámbito de aplicación de la LOPD. Según lo dispuesto en el artículo 2 de la Ley Orgánica 15/1999, se regirá por la misma, todo tratamiento de datos de carácter personal:

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

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

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

Asimismo, el artículo 5 de la citada Ley, dispone que "*cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento* ".

El considerando 19 de la Directiva 95/46/CE señala "*el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho estableci-*

miento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades"

En los requerimientos para que se aportase la documentación necesaria para garantizar las previsiones de los artículos 2 y 5 de la LOPD, anteriormente citados, se hacía hincapié en la solicitud de información adicional con el fin de determinar que se estaban utilizando medios, situados en territorio español, que no fuesen los de mero tránsito.

En los dos casos en que los responsables de los ficheros estaban establecidos en países no pertenecientes a la Unión Europea, se ha requerido la documentación necesaria para acreditar la representación y poderes suficientes de los responsables para que la entidad representante en España actúe en su nombre, así como, que los afectados, cuyos datos personales han sido recabados, han sido informados de los extremos previstos en el artículo 5 de la LOPD, en especial dónde poder ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Para que los afectados puedan ejercer los derechos anteriormente citados, el responsable del fichero, ha de incluir, en la declaración, los datos del representante en España. Esta situación se deberá hacer constar en el apartado de Servicio o Unidad de Oposición, Acceso, Rectificación y Cancelación, de acuerdo a las instrucciones publicadas junto al modelo normalizado de notificación de ficheros.

4.6. Tratamientos no automatizados

Durante el año 2001 se han inscrito en el RGPD 326 ficheros manuales, según han declarado sus responsables, ya que realizaban tratamientos no automatizados sobre los datos de carácter personal.

En estas inscripciones, que han representado un incremento significativo respecto de las realizadas durante el año anterior (51), se incluyen las declaraciones realizadas por algunas oficinas de farmacia, con el fin de mantener el libro recetario oficial, consultas de médicos, con la finalidad de gestionar el historial clínico y despachos de abogados, para llevar el control de los expedientes relativos a la defensa de sus clientes.

Algunas de estas inscripciones de ficheros no automatizados, presentan una incidencia mayor en unas áreas geográficas que en otras, dado que han sido impulsadas por los correspondientes colegios oficiales.

Al tramitar algunos expedientes de inscripción, han surgido dudas acerca de sí un fichero manual se encontraba dentro del ámbito de aplicación de la Ley, ya que no estaba claro que los datos estuviesen contenidos en un archivo, conforme a criterios específicos relativos a las personas, tal como establece la Directiva 95/46/CE. Esta duda también se ha manifestado, en forma de consulta, por parte de los responsables.

El Considerando 27 de la citada Directiva señala *"que la protección de las personas 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 alusión; que, no obstante, por lo que respecta al tratamiento manual, la Directiva sólo abarca los ficheros, y no se aplica las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 22, 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 carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la Directiva".*

La Directiva permite a los estados que regulen los criterios que permitan determinar los elementos de un conjunto estructurado de datos y los distintos criterios que regulan el acceso a dicho conjunto de datos. No obstante, la Ley española no ha tenido en cuenta esta consideración y no hace ninguna referencia a los ficheros manuales, excepto en la Disposición Adicional Primera para establecer el límite del plazo para su notificación.

En este sentido, se ha informado a los responsables de que para que un fichero manual se encuentre incluido en el ámbito de aplicación de la Ley, los datos de carácter personal han de encontrarse contenidos en un archivo estructurado, según criterios específicos relativos a las personas, a fin de que se puedan acceder fácilmente a los datos de carácter personal que se tratan.

Asimismo, se ha informado de lo dispuesto en la Disposición Adicional Primera de la Ley Orgánica 15/1999, en el sentido de que la notificación de los ficheros manuales o no automatizados, no sería obligatoria hasta el 24 de octubre de 2007.

Teniendo en cuenta estas consideraciones, los ficheros manuales que se refieren a las historias clínicas, pueden ser el ejemplo más claro de tratamientos no automatizados incluidos dentro del ámbito de aplicación de la Ley.

Relacionado con este tipo de tratamientos, se debe mencionar que los ficheros manuales no se incluyen en el ámbito

de aplicación del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Por lo tanto, si el responsable desea que consten inscritos los ficheros manuales, se recomienda la utilización del modelo normalizado de notificación en soporte papel, dado que en el modelo de notificación realizado mediante el programa de ayuda, el apartado de medidas de seguridad es de cumplimentación obligatoria. No obstante, es previsión de este Registro poner a disposición de los responsables una nueva versión del citado programa que contemple la posibilidad de inscripción de ficheros manuales.

4.7. Oficinas de farmacia

En junio de 2001 finalizaba el plazo para la adopción de las medidas de seguridad de nivel alto, no obstante este plazo fue ampliado hasta el 26 de junio de 2002, mediante resolución del Ministerio de Justicia.

Este hecho motivó que las oficinas de farmacia de algunas comunidades autónomas adaptasen los sistemas informáticos a los requerimientos previstos en el reglamento de medidas de seguridad. Como continuación de dicha adaptación, e informadas por sus respectivos colegios profesionales, se ha producido un número muy importante de notificaciones de inscripción de los ficheros de las oficinas de farmacia.

En la mayoría de los ficheros declarados, se recaban los datos básicos de identificación del prescriptor, paciente y medicamentos incluidos en la receta. Además, para la dispensación de sustancias estupefacientes, se han de realizar las anotaciones previstas legalmente en los libros recetarios y de estupefacientes y psicotrópicos, según lo dispuesto en la Ley General de Sanidad, Ley del Medicamento, así como en las respectivas legislaciones establecidas por las Comunidades Autónomas.

Durante el año 2001 se han inscrito un total de 2.638 ficheros, pertenecientes a 1.684 oficinas de farmacia. La distribución por comunidades autónomas ha sido desigual, siendo las que más incidencia han tenido la Comunidad Autónoma de Cataluña, Comunidad Valenciana y la Comunidad Autónoma de Canarias.

4.8. Inscripción por Comunidades Autónomas y provincias

Del análisis de las cifras de ficheros inscritos en el RGPD por comunidades autónomas y provincias, que se incluyen en el apartado correspondiente del Registro en cifras, se pueden observar, grosso modo, algunas particularidades.

Al igual que en años anteriores, Barcelona y Madrid han sido las provincias que más ficheros han notificado durante el año 2001. Sin embargo, teniendo en cuenta los ficheros que constaban inscritos en cada provincia en años anteriores, porcentualmente, Santa Cruz de Tenerife (52%), Málaga (43%) y Las Palmas (31%) han sido las provincias dónde se ha experimentado un aumento más significativo, respecto de los ficheros que constaban inscritos en el RGPD, hasta el año 2000.

Este incremento de las provincias de Málaga y Santa Cruz de Tenerife se debe, en buena medida, a la actividad desarrollada por los Colegios Profesionales, promoviendo las inscripciones de las oficinas de farmacia y clínicas médicas. En el caso de Málaga, este incremento ha afectado, además, a otros sectores de actividad como la hostelería, inmobiliarias, etc.

5. TRANSFERENCIAS INTERNACIONALES DE DATOS

Durante el año 2001, se han tramitado e inscrito3 637 declaraciones de transferencias en los ficheros de titularidad privada y siete en los de titularidad pública, lo que ha producido un aumento considerable en la notificación de Transferencias Internacionales4, habiéndose producido un incremento del 137% con respecto al año anterior.

El total de ficheros que constan inscritos en el Registro General de Protección de Datos con transferencias internacionales a 31 de diciembre de 2001 es de 1.843 de titularidad privada y 61 de titularidad pública, lo que supone 1.904 ficheros inscritos con transferencias.

Estas declaraciones se han amparado en los distintos supuestos previstos en el artículo 34 de la Ley, que establece las excepciones a la norma general del movimiento internacional de datos previsto en el artículo 33.1 *"No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas."*

Durante este año también se han tramitado once expedientes de autorización de transferencia internacional en previsión del artículo 33 anteriormente citado, que por su importancia se describen con más detalle en el siguiente subapartado.

En todos los casos se ha solicitado al responsable que acreditase los supuestos en los que amparaba su solicitud siguiendo los criterios previstos en la Instrucción 1/2000, de 1 de diciembre de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos señalado en la Sección I, Norma Tercera. La notificación se efectuará en los términos que se contienen en el apartado 12 *Transferencias internacionales de datos,* del modelo normalizado, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la Ley. En estos casos deberá aportar la documentación que acredite el cumplimiento del supuesto invocado por el responsable.

A continuación se refleja el número de supuestos en los que se han fundamentado las transferencias. Las cifras reflejadas no corresponden al número de ficheros, toda vez, que una transferencia puede ampararse en más de un supuesto.

	TITULARIDAD PUBLICA	**TITULARIDAD PRIVADA**
	2001	**2001**
SE EFECTÚA CON DESTINO A PAÍSES QUE PROPORCIONAN UN NIVEL DE PROTECCIÓN EQUIPARABLE	3	546
RESULTA DE LA APLICACIÓN DE TRATADOS O CONVENIOS EN LOS QUE SEA PARTE ESPAÑA	6	139
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	2	2
ES NECESARIA PARA LA PREVENCIÓN O PARA EL DIAGNÓSTICO MÉDICOS, LA PRESTACIÓN DE ASISTENCIA SANITARIA O TRATAMIENTO MÉDICOS O LA GESTIÓN DE SERVICIOS SANITARIOS	1	21
SE REFIERE A TRANSFERENCIAS DINERARIAS, CONFORME A SU LEGISLACIÓN ESPECÍFICA	1	41
EL AFECTADO HA DADO SU CONSENTIMIENTO	5	445
ES NECESARIA PARA LA EJECUCIÓN DE UN CONTRATO ENTRE EL AFECTADO Y EL RESPONSABLE DEL FICHERO O PARA LA ADOPCIÓN DE MEDIDAS PRECONTRACTUALES ADOPTADAS A PETICIÓN DEL AFECTADO	2	164
ES NECESARIA PARA LA CELEBRACIÓN O EJECUCIÓN DE UN CONTRATO CELEBRADO O POR CELEBRAR, EN INTERÉS DEL AFECTADO, POR EL RESPONSABLE DEL FICHERO Y UN TERCERO	2	150
ES NECESARIA O LEGALMENTE EXIGIDA PARA LA SALVAGUARDA DE UN INTERÉS PÚBLICO	2	6
ES PRECISA PARA EL RECONOCIMIENTO, EJERCICIO O DEFENSA DE UN DERECHO EN UN PROCESO JUDICIAL	3	7
SE EFECTÚA, A PETICIÓN DE PERSONA CON INTERÉS LEGÍTIMO, DESDE UN REGISTRO PÚBLICO Y ES ACORDE CON LA FINALIDAD DEL MISMO	2	19

Como ya se anunciaba en la memoria anterior, la mayor parte de las transferencias se declaran sin solicitar autorización de la Agencia, ya que los responsables de ficheros se amparan en algunas de las excepciones que la Ley ha previsto en sustitución de la autorización prevista en el citado artículo 33.

La publicación de la Instrucción 1/2000 ha supuesto que los responsables de ficheros tuvieran unos criterios orientativos en relación con los tratamientos que suponen un movimiento internacional de datos.

Se han constatado las ventajas de la publicación de los procedimientos que deberían seguir los responsables para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos.

La declaración de una transferencia internacional implica, además del aspecto de fondo, el formal de cumplimentación del modelo de notificación, siendo necesario especificar tanto el país o países destinatarios como la denominación de la entidad o entidades destinatarias de las transferencias.

Se han inscrito 546 transferencias que tienen como destino países considerados de igual nivel de protección, que son los estados miembros de la Unión Europea, Espacio Económico Europeo5, más Suiza y Hungría y «el conferido por el principio de Puerto Seguro» a las empresas de los Estados Unidos adheridas «a los principios de Puerto Seguro».

Los países de la Unión Europea destinatarios de mayor número de transferencias han sido Alemania (136), Reino

Unido (99), Francia (82), Bélgica (31), Países Bajos (31) e Italia (20).

Los países considerados de igual protección por las Decisiones de la Comisión de las Comunidades Europeas, Hungría y Suiza han sido destinatarios de una y 18 transferencias respectivamente.

Por otra parte, se está tramitando una solicitud amparándose en la adecuación de protección conferida por los principios de Puerto Seguro. En estos casos, se deberá acreditar que la entidad destinataria en Estados Unidos se encuentra entre las entidades que se han adherido a los principios de Puerto Seguro, así como, que se encuentra sujeta a la jurisdicción de uno de los Organismos Públicos Estadounidenses que figuran en el Anexo VII de la Decisión 2000/520/CE publicada en los anexos de la memoria de la Agencia de Protección de Datos del año pasado.

El resto de transferencias se han declarado a países que no proporcionan un nivel de protección equiparable y, en el caso de Estados Unidos, a entidades que no están adheridas «a los principios de Puerto Seguro», siendo Estados Unidos el país destinatario de la mayor parte. Como se refleja en la tabla anterior el supuesto que más se ha invocado del artículo 34 es el establecido en su apartado e) "*Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista*", a continuación le siguen todos aquellos que han declarado y acreditado que la transferencia era necesaria para la ejecución de un contrato celebrado o por celebrar entre el afectado y el responsable o en interés del afectado, por el responsable del fichero y un tercero.

A continuación se detallan los colectivos y las finalidades de los ficheros en los que se han declarado transferencias internacionales, teniendo en cuenta el volumen de las notificaciones.

El mayor número de transferencias declaradas se refiere a colectivos de empleados. Las finalidades declaradas son las relacionadas con gestión de recursos humanos, formación de personal, selección de personal, promoción y gestión de empleo y prestaciones sociales.

Le siguen en número las relacionadas con la gestión contable y administrativa de las entidades. El colectivo de personas que suelen incluir este tipo de ficheros son clientes. En el caso de que los clientes sean personas jurídicas se incluyen como datos personales los datos identificativos de las personas físicas que mantienen la relación comercial.

A continuación se encuadran aquellos ficheros relacionados con finalidades de seguros de vida y salud. También en este mismo nivel podemos encuadrar los ficheros cuya finalidad está relacionada con servicios de telecomunicaciones entre los que se pueden destacar comercio electrónico, prestación de servicios de telecomunicaciones y prestación de servicios de certificación.

Por último, se pueden referenciar no por el número sino por su singularidad todas aquellas que suponen fines de investigación epidemiológica y actividades análogas en el sector de la sanidad.

A continuación por su especial interés, se exponen algunos de los supuestos en los que se producen transferencias internacionales.

5.1. Supuestos de especial interés

5.1.1. Registro de certificados de firma electrónica

El responsable del fichero es una sociedad española que se dedica a la prestación de servicios de certificación electrónica y seguridad en las comunicaciones electrónicas.

El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica establece la obligación para los prestadores de servicios de certificación de "*mantener un registro de certificados en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de sus efectos* ".

A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario [artículo 11e)]. En este mismo sentido, el artículo 12 c) establece que los prestadores de servicios de certificación que expidan certificados reconocidos deberán "*garantizar la rapidez y la seguridad en la prestación del servicio. En concreto, deberán permitir la utilización de un servicio rápido y seguro de consulta del Registro de certificados emitidos y habrán de asegurar la extinción o suspensión de la eficacia de éstos de forma segura e inmediata* ".

Por lo tanto, el Registro de Certificados deberá ser accesibe por medios telemáticos, pudiendo ser consultado por los usuarios del sistema, entendiendo por tales a las personas que voluntariamente confían y hacen uso de los certificados, previo consentimiento del signatario.

A este respecto, es necesario resaltar la posibilidad de que, por el propio funcionamiento del sistema de certificación electrónica, dicha consulta pueda ser solicitada desde cualquier país del mundo, por lo que nos encontraríamos ante un supuesto de transferencia internacional de datos personales.

El certificador podrá, o bien obtener un consentimiento inequívoco, artículo 34.e) de la Ley, o bien ampararse en el contrato que firme con el suscriptor en previsión del artículo 34.f) de la Ley.

En relación con la cumplimentación del impreso de notificación, la circunstancia de que la solicitud pueda ser realizada desde cualquier país del mundo y por diversas entidades o personas físicas, impide poder especificar los países y entidades destinatarias de los datos, ya que, en todo caso, dependerá de quienes sean o lleguen a ser usuarios del sistema.

En este caso, únicamente se cumplimentará el apartado denominado "destinatarios determinables o categorías de destinatarios" indicando las reglas que permitan identificar las categorías y, como país de destino se consignará "Internacional".

5.1.2. *Destinatarios de pedidos a través de Internet*

El responsable del fichero es un suministrador de productos a través de una web establecida en España. Se produce una transferencia, cuando la realización de la transacción requiere que los datos se transfieran a una entidad radicada en otro país, o cuando el comprador solicita que el producto se envíe a un tercero distinto de él (fundamentalmente como regalo) y este tercero reside en otro país.

Este tipo de tratamiento únicamente estará justificado con la finalidad de entregar el producto a la dirección postal indicada. Se trata por tanto de un fichero con datos que sólo son mantenidos hasta que el producto se recibe de conformidad y, que debe ser cancelado, o en su caso bloqueado, desde el momento que el producto es entregado.

También tiene lugar una transferencia internacional en el caso de que la mercancía tenga que ser transportada por un operador logístico ubicado en país distinto al del responsable. Se estaría produciendo una transferencia internacional en interés del afectado.

En estos casos, se han celebrado dos contratos. En uno de ellos, las partes son el comprador y la entidad vendedora. La transferencia es necesaria para la ejecución de un contrato entre el responsable y el afectado (comprador) amparado en el artículo 34.f) de la Ley.

Por otro lado, se celebra otro contrato (en interés del afectado) entre el responsable y el operador logístico (establecido fuera de España) o entre el responsable y el comprador en interés del tercero (destinatario establecido fuera de España). En ambos casos, la transferencia se ampararía en el supuesto previsto en el apartado g) del artículo 34 de la Ley.

5.1.3. *Solicitud de servicios de Registro de Dominios*

El cliente (afectado) solicita un Registro de un dominio, por medio de un formulario "on line" de una página web de un responsable establecido en España, que actúa como un agente del cliente ante una tercera entidad (establecida en EE. UU.) acreditada por la ICANN6 (The Internet Corporation for Assigned Names and Numbers) para el registro de dominios.

Los datos suministrados por el cliente pasarán a formar parte de un fichero del responsable y, además, se transmitirán a la entidad extranjera (destinataria de los datos) acreditada para registrar dominios.

A su vez, la entidad registradora está obligada a hacer públicos en la base de datos WHOIS cuyo titular es la ICANN los datos de los titulares del registro del dominio.

En la situación expuesta se producen una serie de cesiones y transferencias en cadena, todas ellas dependientes de la voluntad del cliente para obtener un registro de dominio.

Existen, en primer lugar, unas condiciones contractuales que regulan el servicio de Registro de Dominios entre el afectado y el responsable del fichero. En segundo lugar, un contrato entre la entidad registradora de dominios y el responsable (establecido en España). A su vez la entidad registradora está sometida a las normas del ICANN.

El cliente deberá estar informado de la obligación, de toda entidad de registro, de facilitar los datos del solicitante del dominio a la ICANN, quién es responsable de la base de datos pública "whois directory".

Particularmente, deberá informar de que el país donde está establecido el destinatario de los datos es un país que no garantiza un nivel de protección adecuada.

En este caso, las excepciones aplicables son las previstas en el apartado f) y g) del artículo 34 de medidas contractuales a petición del afectado, si bien en el presente supuesto se ha solicitado además el consentimiento.

5.1.4. *Contratos de Servicios de correo electrónico*

Los usuarios de un portal generalista en Internet, de una sociedad española, se pueden registrar electrónicamente para contratar un servicio de correo electrónico que ofrece una compañía establecida en un tercer país, cuyos servidores se encuentran ubicados en Estados Unidos de América.

Por una lado, para poder ser usuario del portal, con derecho de acceso a los productos y servicios que en el mismo se ofrecen, el afectado deberá cumplimentar todos los campos que aparecen en el formulario de registro.

La finalidad del tratamiento a que van a ser sometidos sus datos es mantener y cumplir la relación negocial que entable

con el portal mediante la contratación o uso de los productos y servicios que se ofrecen en el mismo.

Se solicita el consentimiento del afectado en cumplimiento de lo dispuesto en el artículo 34 e), para que sus datos puedan ser transferidos a cualquier país del mundo, incluso a aquellos que no ofrezcan un nivel de protección equiparable al de la LOPD, con la finalidad de que terceras empresas radicadas en dichos países puedan prestar determinados servicios de tratamiento de datos por cuenta del responsable (housing, hosting, servicio de correo electrónico, etc.)

Asimismo, y en el caso que contrate el servicio de correo electrónico (Webmail) que ofrece la entidad con razón social en un tercer país se solicita el consentimiento en los términos del artículo 34 e) para los fines de la prestación del servicio de correo electrónico.

5.1.5. *Prestación de servicios "hosting"*

Una entidad española tiene contratado el servicio de "hosting" (alquiler de ordenador y servicio de web) con una entidad norteamericana. Este servicio de "hosting" se ofrece en exclusiva a la actividad de la entidad española.

La entidad española tiene una política de privacidad en cada una de sus páginas web que deberá ser explícitamente aceptada mediante la activación de una casilla (checkbox), que se ejecuta previamente al registro de datos en los formularios en los que se pida más información de carácter personal que el alias y dirección de correo electrónico. En los casos de solicitud de consentimiento la activación es obligatoria y previa a la introducción de los datos personales.

Los servidores en los que se alojan los servicios web, correo electrónico y almacenamiento de datos, se encuentran ubicados en Estados Unidos de América.

Aunque los datos técnicamente se recopilan a través del servidor web alojado en Estados Unidos y, se almacenan en dicho país, esta situación no excluye que se produzca una transferencia internacional a terceros países, ya que el responsable del fichero es una entidad establecida en España.

Tampoco puede fundarse la inexistencia de transferencia internacional en el hecho de que la empresa que aloja los servidores, se dedica al alquiler de ordenadores y a la conexión de los mismos a Internet para la prestación del servicio de "hosting". En este supuesto existirá una transferencia internacional por ser responsable del tratamiento una entidad española, siendo una entidad norteamericana la que tendrá la condición de encargado del tratamiento (artículo 12 de la Ley).

Por lo tanto, si no se acredita el consentimiento inequívoco del afectado, se tendrá que solicitar la preceptiva autorización del Director de la Agencia presentando un contrato en los términos previstos en la Decisión de la Comisión de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados de tratamiento establecidos en terceros países (2002/16/CE). Los criterios orientativos seguidos por la Agencia en relación con estos tratamientos se establecen en la Norma Sexta de la Instrucción 1/2000.

5.1.6. *Subastas On-Line*

Una empresa perteneciente a un grupo multinacional dedicado a realizar subastas "on-line" notifica un fichero para la gestión de dicha actividad. Conforme a la información aportada, los tratamientos que se producen son los siguientes:

Los servidores web de esta sociedad que permiten el almacenamiento y tratamiento de los datos personales están ubicados en Estados Unidos (país de distinto nivel de protección ya que esta sociedad en particular no está adherida «a los principios de Puerto Seguro») y son de titularidad de una empresa norteamericana del mismo grupo.

La información que se recaba del afectado es la que se indica en cada uno de los formularios que cumplimenta para solicitar los servicios o funcionalidades de la página web de la que es responsable una entidad establecida en Suiza, país considerado por la Comisión de nivel de protección adecuado.

Esta entidad en determinadas circunstancias, solicita información financiera si el usuario se registra con la finalidad de vender en la red.

Si el usuario solicita una cuenta de crédito con el responsable del fichero, se recaban datos tales como dirección a efectos de facturación, nº de tarjeta de crédito, fecha de caducidad.

También se almacena automáticamente información sobre la actividad del usuario dentro de la página web, sobre la URL a la que accede, sobre el tipo de navegador, y sobre la dirección IP.

Se informa de que se utilizan "cookies", entre otras funcionalidades, para que el usuario no tenga que volver a introducir la contraseña durante una nueva sesión de navegación. Asimismo, se informa de que pueden existir "cookies" instaladas por terceros en páginas web creadas por otros usuarios, que posibilitan el tratamiento invisible de la información por parte de otros.

Si el usuario selecciona pujar, comprar o vender, se recoge información acerca de cómo hace sus pujas, compras y ventas, se recogen los comentarios que sobre el afectado hacen otros usuarios en las áreas de votaciones.

Si se envían mensajes en los Foros del responsable, también se recoge la información personal que facilite.

Este procedimiento de la recogida de datos pretende proporcionar una experiencia fácil, eficiente y personalizada en la página web. De esta manera es posible ofrecer servicios personalizados. Esta información es utilizada también, para resolver las cuestiones que se susciten respecto del cumplimiento de las condiciones de uso para la realización de transacciones a través de esta web.

En el caso de que el afectado tome parte en una transacción, se transfiere al resto de los usuarios la dirección de correo y datos de contacto del afectado.

El sistema descrito supone el acceso a la información personal por parte de diversos proveedores externos de servicios (página webs compartidas, servicios de búsqueda de artículos, servicio de depósito, autenticación, mediación).

Asimismo, implican múltiples transferencias internacionales de datos a países que pueden no ofrecer un nivel adecuado de protección por lo que, para ser lícitas, deberán basarse en lo que no se derive de la relación contractual, en la excepción prevista en el artículo 34e) y contar en consecuencia, con el consentimiento informado del afectado.

En todo caso, la prestación de servicio, por parte de la empresa ubicada en Estados Unidos, que ostenta la condición de encargado del tratamiento, exigirá el consentimiento informado del afectado o la celebración de un contrato cuyas cláusulas se adecúen a las exigencias de la Instrucción 1/2000 en su Norma Sexta.

5.1.7. *Proyectos internacionales convocados por instituciones públicas.*

El responsable del fichero es una firma consultora establecida en España que participa en proyectos internacionales de consultoría convocados por instituciones internacionales públicas (Banco Mundial, Órganos de la Unión Europea, Asociación Internacional del Fomento (AIF), etc.)

Estas organizaciones convocan licitaciones internacionales para el desarrollo de proyectos de servicios públicos.

En las ofertas para participación en el proceso de licitación, se suministra información sobre posibles consultores, personas físicas, que implican una transferencia internacional, cuyos datos constarán en el fichero objeto de la transferencia.

Si la institución o la Unión Europea le adjudica el contrato, se procede a formalizar el mismo con la entidad adjudicataria, que suscribe los contratos con los consultores.

Inicialmente, no es posible aportar los contratos porque aún no se han celebrado. Sin embargo, esta situación está prevista en la excepción de los apartados g) y f) del artículo 34, toda vez que las transferencias sean necesarias para la ejecución de un contrato celebrado o por celebrar, en interés del afectado o para la adopción de medidas precontractuales adoptadas a petición del afectado.

Además, el artículo 34 a) establece que la transferencia de datos a terceros países se pueda realizar "cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que España sea parte".

5.1.8. *Convenios de Universidad*

Una Universidad Pública prevé la realización de transferencias de datos a países de la Unión Europea, Sudamérica y Norteamérica, así como a aquellos países con los que la Universidad celebre convenios de colaboración.

Las finalidades de la transferencia son:

* Prácticas en entidades extranjeras. En estos casos se transfieren los datos de los alumnos a los cuales se les informa de las previsiones del artículo 5 y se les solicita expresamente el consentimiento para realizar la cesión de sus datos a las empresas o instituciones de destino con el fin de que se gestione la práctica.

Sin perjuicio de recabar el consentimiento, este supuesto de transferencia puede estar amparado en la excepción de los apartados f) y g) del artículo 34, "*necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado*" o bien "*necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero"*

* Movilidad del profesorado. En el caso del fichero de personal las transferencias se refieren fundamentalmente a la movilidad de los profesores.

En estos casos se firma un convenio con el personal docente en el que se les informa y consienten expresamente para la transmisión de datos a las instituciones de destino, así como, a la Agencia Nacional Erasmus y cualquier otro Organismo necesario para la gestión del programa, con la finalidad de gestionar su movilidad en los términos del contrato.

5.1.9. *Compañías y Organismos Oficiales relacionados con las emergencias aéreas*

El responsable del fichero es una compañía aérea, y tiene previsto la realización de la transferencia internacional de los datos de carácter personal de los pasajeros (afectados), que se encuentren implicados en una emergencia, en un vuelo de la compañía.

La transferencia internacional tiene como destino de los datos, tanto a entidades y organismos establecidos en países con nivel de protección equiparable, como a terceros países.

Por la naturaleza del tratamiento, declaran que se recaban datos relativos a la salud, amparados en lo establecido en el artículo 7.6 de la LOPD, ya que el tratamiento de dichos datos puede resultar necesario para la prestación de asistencia sanitaria o tratamientos médicos de los pasajeros afectados por la emergencia.

Para la realización de la transferencia a terceros países, el responsable del fichero declara que dicha transferencia se encuentra amparada en las excepciones previstas en el artículo 34, en su apartado c), que exime de la norma general, establecida en el artículo 33, cuando:

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

5.2. Expedientes de Autorización de Transferencias Internacionales

La petición de autorización de transferencias internacionales de datos efectuada al amparo del artículo 33 de la Ley exige una serie de garantías que deben ser prestadas por la entidad que realiza la transferencia, establecida legalmente en nuestro país. Dicha entidad, como responsable de los ficheros, deberá garantizar el cumplimiento de todas las obligaciones y derechos establecidos en la Ley nacional, así como que se continuará facilitando desde España el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de los datos almacenados en terceros países. El Director de la Agencia de conformidad con lo dispuesto en el artículo 33 viene exigiendo garantías que se traducen en cláusulas contractuales apropiadas.

La autorización será otorgada siempre y cuando se cumplan todas las previsiones de la Ley nacional y el responsable del fichero aporte un contrato entre el transmitente y el destinatario, en el que consten las necesarias garantías. El citado contrato deberá contener, al menos, las cláusulas contractuales tipo previstas en la Decisión de la Comisión de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países. (Norma Sexta Instrucción 1/2000)

Durante el año 2001 se han tramitado once expedientes de autorización de Transferencias Internacionales.

Como ya se citaba en la memoria anterior, la inclusión en la nueva Ley del consentimiento del afectado como excepción a la preceptiva autorización necesaria en la LORTAD, ha supuesto que se soliciten menos autorizaciones para realizar transferencias internacionales.

De las once solicitudes de autorización, al amparo del artículo 33 de la Ley, se ha procedido a autorizar nueve de ellas, una se ha resuelto declarando su archivo y otra ha sido denegada.

Ocho de las nueve autorizaciones resueltas favorablemente, han sido presentadas por entidades pertenecientes a un mismo grupo empresarial de ámbito mundial.

En todas las autorizaciones de transferencias resueltas, los destinatarios realizan una prestación de servicio al responsable del tratamiento. La realización del tratamiento por parte de estos encargados está regulada en los contratos aportados que vinculan al encargado con el responsable del tratamiento, en los términos a que se refiere el artículo 12 de la Ley. Las cláusulas exigidas se corresponden con las publicadas en la Instrucción 1/2000.

Los nueve expedientes de autorización tramitados y resueltos durante el año 2001 tenían en común el país de destino, Estados Unidos de América.

La finalidad de la primera transferencia autorizada es la prestación de servicios de procesamiento, tratamiento, mejora y optimización de la base de datos de clientes de titularidad de una empresa española, por parte de dos entidades que, aunque una ellas es de nacionalidad canadiense, están establecidas en Estados Unidos. En cumplimiento de lo establecido en la Norma Sexta apartado 2 de la Instrucción 1/2000, el contrato se ha celebrado entre el transmitente y cada una de las entidades que presta los servicios de tratamiento.

En las restantes transferencias autorizadas, solicitadas por las ocho entidades españolas pertenecientes a la misma organización, la finalidad es centralizar el tratamiento de los datos de personal a nivel mundial, poder optimizar y mejorar la operativa de la organización y la prestación de los servicios de gestión contable y administrativa, así como la obtención de estadísticas diversas, por parte de la compañía de nacionalidad estadounidense. Los datos objeto de la transferencia son de carácter identificativo, características personales, circunstancias sociales, datos académicos y profesionales, detalles de empleo y económico-financiero.

En el presente caso, no se realizaban cesiones de datos, únicamente la comunicación a la organización mundial se fundamenta en el acceso a los datos como encargado de tratamiento. Se advirtió expresamente a los responsables de los ficheros que el tratamiento de datos por parte de las filiales de la organización mundial, requería el consentimiento de los afectados en los términos previstos en el artículo 11 de la Ley Orgánica 15/1999. Cuando esas filiales estén

establecidas en terceros países, será necesario declarar la transferencia internacional de datos a los efectos de su inscripción en el Registro General de Protección de Datos en los términos previstos en la Norma Tercera de la Instrucción 1/2000.

Como antes quedó señalado, se archivó un expediente de solicitud de transferencia. En este caso, se requirió al responsable para que aportara un contrato con los extremos previstos en la Instrucción 1/2000. Una vez transcurridos los plazos concedidos, no se recibió notificación o aclaración alguna al respecto, produciéndose en consecuencia el archivo de la solicitud. En la resolución se les advirtió expresamente que en cumplimiento del artículo 33.1 de la LOPD *"No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas".* No obstante, se les informaba de que si subsanaban los extremos requeridos y aportaban garantías suficientes podrían volver a solicitar de nuevo la autorización.

Por último, se ha dictado otra resolución en la que se deniega la autorización de transferencia internacional.

Entre las alegaciones fundamentadas por el responsable se citaba textualmente que la finalidad de la transferencia internacional era "poder intercambiar entre las partes datos personales sobre la totalidad o parte de sus empleados con objeto de facilitar la coordinación del personal, tanto dentro de sus respectivos territorios como a nivel mundial. Este intercambio de datos pretende beneficiar a los empleados del grupo empresarial de todo el mundo, ya que permite un proceso de planificación más eficiente de las carreras profesionales de dichos empleados, facilitando los intercambios entre las sociedades del grupo".

Esta solicitud se ha denegado por dos motivos fundamentales:

En primer lugar, la exigencia de autorización del Director de la Agencia, establecido en el artículo 33 de la Ley 15/1999, no exime del cumplimiento previo de las disposiciones contenidas en la Ley nacional. En particular, en el expediente que nos ocupa, dado que existían cesiones o comunicaciones entre la empresa solicitante y las filiales de su grupo empresarial se debía cumplir, antes de la autorización de la transferencia, los requisitos establecidos en el artículo 11 de la Ley. A tal efecto, se requirió a la entidad solicitante para que acreditara el cumplimiento de lo dispuesto en este precepto, sin que se obtuviera una respuesta satisfactoria al respecto.

En segundo lugar, el contrato presentado por la entidad solicitante no identificaba ni los países ni las filiales destinatarias de los datos personales. Por ello se requirió a la entidad solicitante para que identificara en el contrato a cada una de las filiales destinatarias de la transferencia. La entidad responsable presentó escrito de alegaciones sin que aportara otro contrato que cumpliera las garantías adecuadas, por lo que se denegó la autorización solicitada. Finalmente, por todo lo expuesto, en la resolución se advirtió expresamente al responsable del fichero que el tratamiento de datos que implique cesiones de datos a terceros deberá realizarse cumpliendo en origen la Ley 15/1999, pudiendo en otro caso incurrir en las infracciones previstas en la misma.

Se ha dado traslado al Ministro de Justicia de las resoluciones de autorización de transferencia internacional, a fin de que se dé cumplimiento al artículo 26 de la Directiva 95/46/CE, en el que se dispone que los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2 de dicho artículo

(1) 2.*2.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 refieren a sus asociados o miembros y ex miembros, ..."
(2) Artículo 2c) de la Directiva 95/46/CE se entenderá por *"fichero de datos personales: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica"* .
(3) A 31 de diciembre de 2001, cinco de estos ficheros constaban suprimidos.
(4) Nótese que las cifras son relativas a notificación de transferencias, ya sean asociadas a una nueva inscripción o a modificaciones de inscripciones existentes.
(5) El Espacio Económico Europeo incluye a Islandia, Liechtenstein y Noruega además de los países de la Unión Europea.
(6) ICANN, órgano que coordina la gestión de Registros de nombre y dominios de la corporación de Internet para la Asignación de Nombres y Números.
GAC: Comité Asesor Gubernamental de ICANN, participa como miembro del mismo, el Ministerio de Ciencia y Tecnología.

6. EL REGISTRO EN CIFRAS

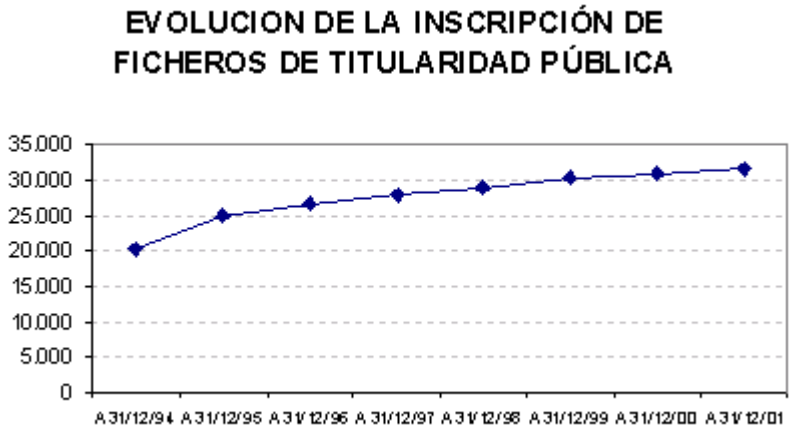
A continuación se detalla la situación y características principales de los ficheros inscritos en el Registro General de Protección de Datos. Como en años anteriores, se ha tratado de establecer la comparación entre los ficheros según la titularidad del responsable, público o privado, así como el estudio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

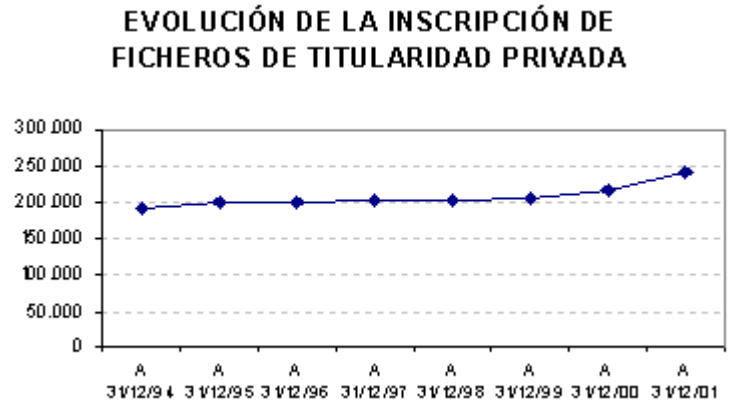
A fecha 31 de diciembre de 2001, el número de ficheros inscritos en el Registro General de Protección de Datos era de 271.875, de los cuales 31.805 correspondían a inscripciones de titularidad pública y 240.070 a inscripciones de titularidad privada.

RESUMEN DETALLADO DE LOS FICHEROS INSCRITOS EN EL RGPD, SEGÚN LA TITULARIDAD

Se recoge en esta tabla el número de ficheros inscritos en el Registro General de Protección de Datos a 31 de diciembre de cada año, de acuerdo con los datos que aparecen en las memorias anuales de la Agencia, según la titularidad de los mismos.

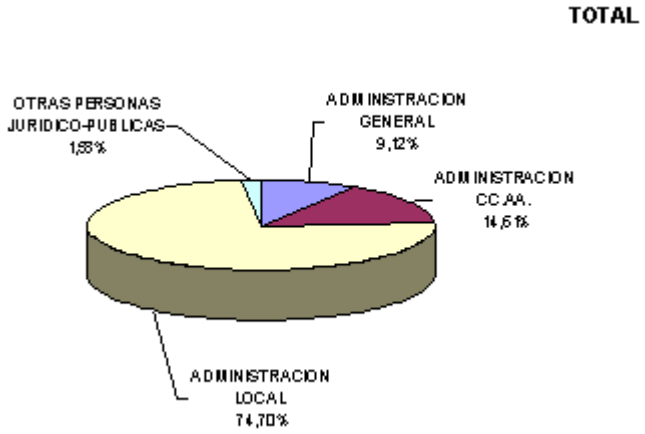
	A 31/12/94	A 31/12/95	A 31/12/96	A 31/12/97	A 31/12/98	A 31/12/99	A 31/12/00	A 31/12/01
TITULARIDAD PUBLICA	20.198	24.923	26.541	27.969	28.890	30.431	31.155	31.805
TITULARIDAD PRIVADA	192.097	199.933	201.054	201.835	203.138	204.737	218.054	240.070
T O T A L	212.295	224.856	227.595	229.804	232.028	235.168	249.209	271.875





DISTRIBUCION DE FICHEROS DE TITULARIDAD PÚBLICA INSCRITOS EN EL RGPD, SEGÚN EL TIPO DE ADMINISTRACIÓN AL QUE PERTENECEN

	2001	TOTAL
ADMINISTRACION CENTRAL	87	2.901
ADMINISTRACION CC.AA.	664	4.646
ADMINISTRACION LOCAL	407	23.757
OTRAS PERSONAS JURIDICO-PUBLICAS	28	501
TOTAL	1.186	31.805



DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACIÓN CENTRAL INSCRITOS EN EL RGPD

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

	2001	TOTAL
MINISTERIO DE ADMINISTRACIONES PUBLICAS	0	215
MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACIO	1	38
MINISTERIO DE ASUNTOS EXTERIORES	0	522
MINISTERIO DE CIENCIA Y TECNOLOGIA	0	44
MINISTERIO DE DEFENSA	4	39
MINISTERIO DE ECONOMIA	3	102
MINISTERIO DE EDUCACION, CULTURA Y DEPORTE	2	135
MINISTERIO DE FOMENTO	3	213
MINISTERIO DE HACIENDA	20	146
MINISTERIO DE JUSTICIA	0	22
MINISTERIO DE LA PRESIDENCIA	0	39
MINISTERIO DE MEDIO AMBIENTE	0	170
MINISTERIO DE SANIDAD Y CONSUMO	4	651
MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES	41	298
MINISTERIO DEL INTERIOR	9	260
MINISTERIO PORTAVOZ DEL GOBIERNO	0	3
PRESIDENCIA DEL GOBIERNO	0	4
TOTAL	87	2.901

DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACION DE LAS COMUNIDADES AUTONOMAS INSCRITOS EN EL RGPD

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

COMUNIDAD AUTONOMA	2001	TOTAL
ANDALUCIA	41	529
ARAGON	3	178
CANARIAS	2	254
CANTABRIA	5	26
CASTILLA - LA MANCHA	3	96
CASTILLA Y LEON	0	221
CATALUÑA	8	501
COMUNIDAD VALENCIANA	37	349
EXTREMADURA	1	64
GALICIA	420	539
ISLAS BALEARES	0	31
LA RIOJA	33	162
MADRID	100	908
NAVARRA	6	100
PAIS VASCO	0	306
PRINCIPADO DE ASTURIAS	0	143
REGION DE MURCIA	5	154
CEUTA	0	23
MELILLA	0	62
TOTAL	664	4.646

DISTRIBUCION DE FICHEROS DE TITULARIDAD PUBLICA DE LA ADMINISTRACION LOCAL INSCRITOS EN EL RGPD

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

	ENTIDADES LOCALES		FICHEROS	
	2001	TOTAL	2001	TOTAL
ANDALUCIA	**8**	**685**	**21**	**5.482**
ALMERIA	0	104	0	951
CADIZ	2	49	2	334
CORDOBA	1	61	2	260
GRANADA	0	168	0	1.183
HUELVA	0	85	0	1.150
JAEN	0	82	0	468
MALAGA	1	41	11	396
SEVILLA	4	95	6	740
ARAGON	**0**	**434**	**0**	**1.967**
HUESCA	0	156	0	536
TERUEL	0	45	0	152
ZARAGOZA	0	233	0	1.279
ASTURIAS	**3**	**49**	**17**	**294**
ILLES BALEARS	**0**	**67**	**0**	**650**
CANARIAS	**5**	**73**	**36**	**451**
LAS PALMAS	3	30	9	204
SANTA CRUZ DE TENERIFE	2	43	27	247
CANTABRIA	**0**	**43**	**0**	**192**
CASTILLA-LA MANCHA	**1**	**343**	**1**	**1.850**
ALBACETE	0	74	0	356
CIUDAD REAL	0	107	0	557
CUENCA	0	82	0	556
GUADALAJARA	0	11	0	58
TOLEDO	1	69	1	323
CASTILLA Y LEON	**3**	**501**	**9**	**2.209**
AVILA	1	7	1	21
BURGOS	1	92	4	322
LEON	1	164	4	805
PALENCIA	0	18	0	76
SALAMANCA	0	80	0	338
SEGOVIA	0	14	0	104
SORIA	0	9	0	31
VALLADOLID	0	82	0	355
ZAMORA	0	35	0	157
CATALUÑA	**20**	**566**	**180**	**2.661**
BARCELONA	15	316	139	1.452
GIRONA	4	59	35	382
LLEIDA	0	106	0	398
TARRAGONA	1	85	6	429

DISTRIBUCION DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD

En esta tabla aparecen, diferenciados por Comunidades Autónomas y Provincias, los ficheros inscritos por responsables de titularidad privada.

	RESPONSABLES		FICHEROS INSCRITOS	
	2.001	TOTAL	2.001	TOTAL
ANDALUCIA	**1.535**	**10.755**	**2.670**	**20.751**
ALMERIA	55	461	79	911
CADIZ	26	1.757	86	2.838
CORDOBA	68	1.180	222	2.694
GRANADA	87	836	206	1.698
HUELVA	21	651	49	1.079
JAEN	21	854	50	1.821
MALAGA	1.107	3.133	1.610	5.330
SEVILLA	154	1.899	368	4.380
ARAGON	**333**	**8.348**	**743**	**14.006**
HUESCA	85	1.870	153	2.669
TERUEL	13	596	70	1.002
ZARAGOZA	235	5.888	520	10.335
ASTURIAS	**167**	**2.118**	**514**	**4.209**
ILLES BALEARS	**158**	**1.411**	**531**	**3.645**
CANARIAS	**364**	**1.659**	**990**	**3.464**
LAS PALMAS	209	954	447	1.874
SANTA CRUZ DE TENERIFE	155	709	543	1.590
CANTABRIA	**60**	**631**	**146**	**1.417**
CASTILLA-LA MANCHA	**104**	**3.094**	**306**	**5.613**
ALBACETE	35	952	69	1.520
CIUDAD REAL	24	643	84	1.229
CUENCA	8	532	28	872
GUADALAJARA	13	231	29	562
TOLEDO	34	736	96	1.430
CASTILLA Y LEON	**263**	**4.839**	**684**	**9.112**
AVILA	3	206	5	393
BURGOS	33	1.300	80	2.125
LEON	51	707	144	1.392
PALENCIA	22	259	46	511
SALAMANCA	23	563	67	1.282
SEGOVIA	19	307	41	553
SORIA	6	248	15	402
VALLADOLID	90	998	242	1.853
ZAMORA	16	257	44	601
CATALUÑA	**3.466**	**35.499**	**7.392**	**68.495**
BARCELONA	2.453	26.701	5.514	52.671
GIRONA	243	3.228	481	5.841
LLEIDA	404	3.211	684	5.586
TARRAGONA	367	2.397	713	4.397

FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD POR RESPONSABLES CON SEDE EN EL EXTRANJERO

La Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en su artículo 2.1 fija su ámbito de aplicación a cualquier tratamiento de datos de carácter personal efectuado en el territorio español, se encuentre el establecimiento del responsable en España, en territorio de la Unión Europea o fuera de ésta.

	RESPONSABLES		FICHEROS	
	2.001	TOTAL	2.001	TOTAL
RESPONSABLES EN LA UNION EUROPEA	8	13	10	18
FRANCIA	2	5	4	10
ITALIA	0	1	0	1
REINO UNIDO	5	6	5	6
SUECIA	1	1	1	1
RESPONSABLES EN TERCEROS PAISES	2	2	2	2
ESTADOS UNIDOS	1	1	1	1
SUIZA	1	1	1	1

DISTRIBUCIÓN DE FICHEROS SEGÚN LA TIPOLOGÍA DE DATOS QUE CONTIENEN

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2001	TOTAL	2001	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS (Ideología, creencias, religión y afiliación sindical)	160	224	730	1.249
OTROS DATOS ESPECIALMENTE PROTEGIDOS (Origen racial, salud y vida sexual)	223	2.220	5.859	10.019
DATOS RELATIVOS A INFRACCIONES	61	1.302	---	---
DATOS DE CARÁCTER IDENTIFICATIVO	1.186	31.805	24.838	240.070
DATOS DE CARACTERISTICAS PERSONALES	587	16.368	11.350	99.450
DATOS DE CIRCUNSTANCIAS SOCIALES	273	8.270	4.228	26.914
DATOS ACADEMICOS Y PROFESIONALES	484	10.541	4.664	33.571
DETALLES DE EMPLEO Y CARRERA ADMINISTRATIVA	434	7.340	9.039	78.592
DATOS DE INFORMACION COMERCIAL	118	6.520	3.702	44.017
DATOS ECONOMICO-FINANCIEROS	407	14.123	11.599	122.408
DATOS DE TRANSACCIONES	102	5.834	5.903	60.534

--- No aplicable a esta titularidad

DISTRIBUCIÓN DE FICHEROS INSCRITOS CON DATOS SENSIBLES

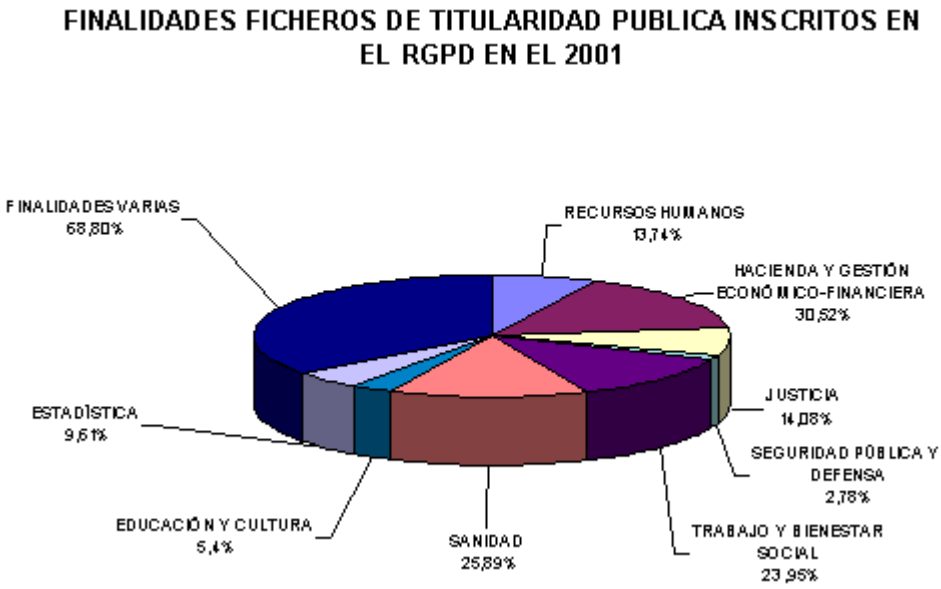
	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2001	TOTAL	2001	TOTAL
DATOS ESPECIALMENTE PROTEGIDOS	160	224	730	1249
Ideología	2	36	13	150
Creencias	1	21	27	68
Religión	119	134	142	344
Afiliación Sindical	40	48	619	785
OTROS DATOS ESPECIALMENTE PROTEGIDOS	223	2.220	5.859	10.019
Origen Racial	11	104	50	111
Salud	220	2.199	5.851	9.986
Vida Sexual	126	492	58	187
DATOS RELATIVOS A INFRACCIONES	61	1.302	---	---
Infracciones Penales	16	766	---	---
Infracciones Administrativas	59	968	---	---

--- No aplicable a esta titularidad

DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PÚBLICA INSCRITOS EN EL RGPD, SEGÚN SU FINALIDAD

	2001	TOTAL
RECURSOS HUMANOS		
GESTIÓN DE PERSONAL	121	4.538
GESTIÓN DE NÓMINA (*)	75	83
FORMACIÓN DE PERSONAL	31	1.451
ACCIÓN SOCIAL A FAVOR DEL PERSONAL DE LAS ADMONES. PÚBLICAS	40	842
PROMOCIÓN Y SELECCIÓN DE PERSONAL, OPOSICIONES Y CONCURSOS (*)	24	30
PREVENCIÓN DE RIESGOS LABORALES (*)	11	12
CONTROL HORARIO	21	26
CONTROL DE INCOMPATIBILIDADES	44	666
CONTROL DE PATRIMONIO DE ALTOS CARGOS PÚBLICOS	4	223
HACIENDA Y GESTIÓN ECONÓMICO-FINANCIERA		
GESTIÓN TRIBUTARIA Y DE RECAUDACIÓN	133	6.806
GESTIÓN ECONÓMICA Y CONTABLE	115	6.051
GESTIÓN DE FACTURACIÓN (*)	187	189
GESTIÓN FISCAL (*)	76	80
GESTIÓN DEUDA PÚBLICA Y TESORERÍA	41	2.499
GESTIÓN DE CATASTROS INMOBILIARIOS RÚSTICOS Y URBANOS	19	1.859
RELACIONES COMERCIALES CON EL EXTERIOR	11	433
REGULACIÓN DE MERCADOS FINANCIEROS	1	30
DEFENSA DE LA COMPETENCIA	2	27
JUSTICIA		
PROCEDIMIENTOS JUDICIALES	158	1.033
REGISTROS VINCULADOS CON LA FE PÚBLICA (*)	9	26
PRESTACIÓN SOCIAL SUSTITUTORIA	0	848
TRAMITACIÓN DE INDULTOS	1	263
SEGURIDAD PÚBLICA Y DEFENSA		
PROTECCIÓN CIVIL	14	1.667
SEGURIDAD VIAL	19	1341
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES POLICIALES	16	2.070
ACTUACIONES DE FUERZAS Y CUERPOS DE SEGURIDAD CON FINES ADMINISTRATIVO	15	1.829
GESTIÓN Y CONTROL DE CENTROS E INSTITUCIONES PENITENCIARIAS	0	325
TRAMITACION SERVICIO MILITAR	0	2131
SOLICITUDES DE VISADO/RESIDENCIA (*)	2	2
TRABAJO Y BIENESTAR SOCIAL		
PROMOCIÓN Y GESTIÓN DE EMPLEO	69	885
RELACIONES LABORALES Y CONDICIONES DE TRABAJO	41	1396
INSPECCIÓN Y CONTROL DE SEGURIDAD Y PROTECCIÓN SOCIAL	11	700
FORMACIÓN PROFESIONAL OCUPACIONAL	12	1.104
PRESTACIONES A DESEMPLEADOS	35	1.004
PRESTACIONES DE GARANTÍA SALARIAL	36	303
PRESTACIONES DE ASISTENCIA SOCIAL	143	1.729
PENSIONES, SUBSIDIOS Y OTRAS PRESTACIONES ECONÓMICAS	69	1.996
ACCIÓN A FAVOR DE INMIGRANTES	40	433
SERVICIOS SOCIALES A MINUSVÁLIDOS	27	818
SERVICIOS SOCIALES A LA TERCERA EDAD	32	1103
PROMOCIÓN SOCIAL A LA MUJER	29	656
PROMOCIÓN SOCIAL A LA JUVENTUD	24	700
PROTECCIÓN DEL MENOR	3	796
ACCIÓN A FAVOR DE TOXICÓMANOS (*)	17	18
AYUDAS ACCESO A VIVIENDA	22	1.073

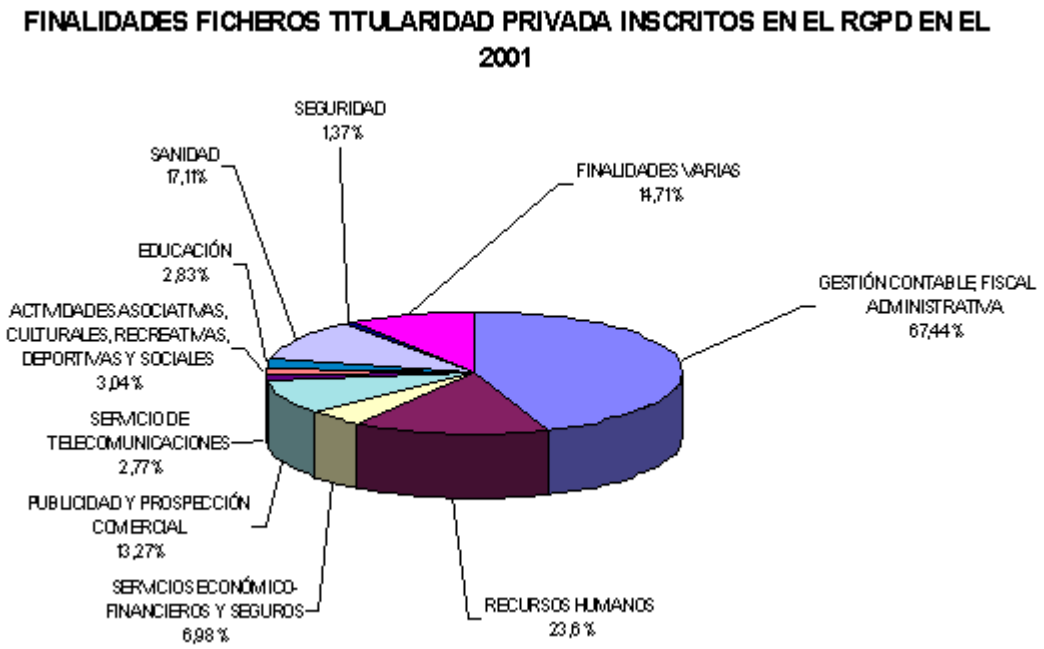
(*) Finalidades que se incluyeron en el nuevo modelo de formulario publicado tras la entrada en vigor de la Ley 15/1999.



DISTRIBUCIÓN DE FICHEROS DE TITULARIDAD PRIVADA INSCRITOS EN EL RGPD, SEGÚN SU FINALIDAD

	2001	TOTAL
GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA		
GESTIÓN ECONÓMICA Y CONTABLE	8.071	147.534
GESTIÓN FISCAL	5.481	144.289
GESTIÓN ADMINISTRATIVA	10.556	149.647
GESTIÓN DE FACTURACIÓN (*)	8.685	9.980
GESTIÓN DE CLIENTES	9.684	77.841
GESTIÓN DE PROVEEDORES (*)	5.442	6.392
GESTIÓN DE COBROS Y PAGOS	8.785	101.839
ADMINISTRACIÓN DE FINCAS (*)	274	296
CONSULTORÍAS, AUDITORÍAS, ASESORÍAS Y SERVICIOS RELACIONADOS	965	14.948
HISTÓRICOS DE RELACIONES COMERCIALES	3.033	37.111
RECURSOS HUMANOS		
GESTIÓN DE PERSONAL	3.876	60.558
GESTIÓN DE NÓMINAS	4.014	4.944
FORMACIÓN DE PERSONAL	1.381	3.385
PRESTACIONES SOCIALES	1446	15.530
SELECCIÓN DE PERSONAL	1184	5.786
GESTIÓN DE TRABAJO TEMPORAL (*)	439	499
PROMOCIÓN Y GESTIÓN DE EMPLEO (*)	635	775
PREVENCIÓN RIESGOS LABORALES (*)	1.098	1.255
CONTROL HORARIO (*)	1.009	1.195
SERVICIOS ECONÓMICO-FINANCIEROS Y SEGUROS		
CUENTA DE CRÉDITO	239	4.559
CUENTA DE DEPÓSITO	244	2.627
GESTIÓN DE PATRIMONIOS	196	2.383
GESTIÓN DE FONDOS DE PENSIONES Y SIMILARES	191	2.341
GESTIÓN DE TARJETAS DE CRÉDITO Y SIMILARES	146	1.706
REGISTRO DE ACCIONES Y OBLIGACIONES	156	2.320
OTROS SERVICIOS FINANCIEROS	323	4.260
CUMPLIMIENTO/INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS (*)	222	295
PRESTACIÓN DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CRÉDITO	63	3.421
SEGUROS DE VIDA Y SALUD	676	6.528
OTRO TIPO DE SEGUROS	631	6.363
PUBLICIDAD Y PROSPECCIÓN COMERCIAL		
PUBLICIDAD PROPIA	2574	23.687
VENTA A DISTANCIA (*)	451	3.391
ENCUESTAS DE OPINIÓN	1136	4.496
ANÁLISIS DE PERFILES (*)	707	828
PROSPECCIÓN COMERCIAL	1558	9.207
SEGMENTACIÓN DE MERCADOS (*)	742	898
SISTEMAS DE AYUDA A LA TOMA DE DECISIONES (*)	760	894
RECOPILACIÓN DE DIRECCIONES (*)	822	959
SERVICIO DE TELECOMUNICACIONES		
PRESTACIÓN DE SERVICIOS DE TELECOMUNICACIONES	312	1.681
GUÍAS/REPERTORIOS DE SERVICIOS DE TELECOMUNICACIONES (*)	94	115
COMERCIO ELECTRÓNICO (*)	426	529
PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN (*)	31	36
ACTIVIDADES ASOCIATIVAS, CULTURALES, RECREATIVAS, DEPORTIVAS Y SOCIALES		
GESTIÓN DE ACTIVIDADES CULTURALES (*)	186	228
GESTIÓN DE CLUBES O ASOCIACIONES DEPORTIVAS, CULTURALES, PROFESIONALES Y		

(*) Finalidades que se incluyeron en el nuevo modelo de formulario publicado tras la entrada en vigor de la Ley 15/1999.



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

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
PROCEDENCIA DE LOS DATOS	**2.001**	**TOTAL**	**2.001**	**TOTAL**
EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL	1.117	29.823	24.081	218.604
OTRAS PERSONAS DISTINTAS AL AFECTADO O SU REPRESENTANTE	183	4.196	725	5.093
FUENTES ACCESIBLES AL PUBLICO (*)	33	2.866	923	10.358
Censo Promocional	0	0	0	0
Guías y Servicios de Telecomunicaciones	16	18	453	550
Listas de personas pertenecientes a grupos profesionales	19	25	548	650
Diarios y Boletines Oficiales	22	24	209	243
Medios de Comunicación	13	14	463	545
REGISTROS PÚBLICOS	79	6.859	682	4.765
ENTIDAD PRIVADA	47	3.264	919	27.830
ADMINISTRACIONES PUBLICAS	237	11.438	835	4.659
PROCEDIMIENTO DE RECOGIDA	**2.001**	**TOTAL**	**2.001**	**TOTAL**
ENCUESTAS O ENTREVISTAS	325	4.663	11.716	59.771
FORMULARIOS O CUPONES	973	27.138	10.149	102.732
TRANSMISION ELECTRONICA DE DATOS	488	5.279	3.199	8.772
OTROS PROCEDIMIENTOS DE RECOGIDA	185	4.887	9.088	90.107
SOPORTE	**2.001**	**TOTAL**	**2.001**	**TOTAL**
SOPORTE PAPEL	1.107	20.124	20.414	194.766
SOPORTE INFORMATICO/MAGNETICO	645	12.582	8.088	40.039
VIA TELEMATICA	472	3.836	3.145	10.869
OTROS SOPORTES	21	3.182	2.626	38.232

(*) Para aquellos ficheros que hubieran declarado con anterioridad a la entrada en vigor de la Ley 15/1999 la procedencia de los datos de fuentes accesibles al público no constan diferenciados los tipos indicados en la citada Ley, apareciendo estos tipos diferenciados en la tabla únicamente para los ficheros inscritos con posterioridad a Julio de 2000, o aquellos anteriores que han sufrido modificaciones después de esta fecha.

DISTRIBUCIÓN DE FICHEROS INSCRITOS EN EL RGPD QUE DECLARAN LA REALIZACIÓN DE CESIONES DE DATOS

	FICHEROS INSCRITOS AÑO 200			TOTAL FICHEROS		
	CON CESIONES	**TOTAL**	**%**	**CON CESIONES**	**TOTAL**	**%**
TITULARIDAD PÚBLICA	705	1.186	59,44	18.520	31.805	58,23
TITULARIDAD PRIVADA	7.135	24.838	28,73	44.526	240.070	18,55
TOTAL	7.840	26.024	30,13	63.046	271.875	23,19

NOTA.- El número total de ficheros activos inscritos en el año 2001 es de 26.024, correspondiente a las altas de ficheros realizadas en el año 2001 (26.113) menos los ficheros de este año suprimidos en el mismo año de su inscripción (89).

SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LAS CESIONES DE DATOS INSCRITAS EN EL RGPD

	TITULARIDAD PUBLICA		TITULARIDAD PRIVADA	
	2001	TOTAL	2001	TOTAL
EXISTE CONSENTIMIENTO DE LOS AFECTADOS	258	7.203	4.808	24.586
EXISTE UNA RELACION JURIDICA CUYO DESARROLLO, CONTROL Y CUMPLIMIENTO IMPLICA NECESARIAMENTE LA CONEXION DEL FICHERO CON FICHEROS DE TERCEROS	335	4.322	5.292	19.208
EXISTE UNA NORMA REGULADORA QUE LAS AUTORIZA	189	11.041	3.464	24.129
SE TRATA DE DATOS RECOGIDOS DE FUENTES ACCESIBLES AL PUBLICO	34	4.811	311	2.829
CORRESPONDEN A COMPETENCIAS IDENTICAS O QUE VERSAN SOBRE LAS MISMAS MATERIAS, EJERCIDAS POR OTRAS ADMINISTRACIONES PUBLICAS	278	10.821	---	---
SON DATOS OBTENIDOS O ELABORADOS CON DESTINO A OTRA ADMINISTRACION PUBLICA	276	9.590	---	---
LA COMUNICACIÓN TIENE POR OBJETO EL TRATAMIENTO POSTERIOR DE LOS DATOS CON FINES HISTORICOS, ESTADISTICOS O CIENTIFICOS	473	525	---	---
TOTAL FICHEROS INSCRITOS CON CESIONES	**705**	**18.520**	**7.135**	**44.526**

--- No aplicable a esta titularidad

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

TRANSFERENCIAS INTERNACIONALES DE DATOS INSCRITAS EN EL AÑO 2001

	TRANSFERENCIAS 2001	TOTAL FICHEROS INSCRITOS 2001	TOTAL FICHEROS CON TRANSFERENCIA A 31/12/2001	TOTAL FICHEROS INSCRITOS
TITULARIDAD PÚBLICA	7	1.186	61	31.805
TITULARIDAD PRIVADA	637	24.838	1.843	240.070
TOTAL	644	26.024	1.904	271.875

NOTA.- El número total de ficheros activos inscritos en el año 2001 es de 26.024, correspondiente a las altas de ficheros realizadas en el año 2001 (26.113) menos los ficheros de este año suprimidos en el mismo año de su inscripción (89).

SUPUESTOS LEGALES EN LOS QUE SE AMPARAN LAS TRANSFERENCIAS INTERNACIONALES DE DATOS INSCRITAS EN EL RGPD EN EL AÑO 2001

	TITULARIDAD PUBLICA	TITULARIDAD PRIVADA
	2001	2001
SE EFECTÚA CON DESTINO A PAÍSES QUE PROPORCIONAN UN NIVEL DE PROTECCIÓN EQUIPARABLE	3	546
RESULTA DE LA APLICACIÓN DE TRATADOS O CONVENIOS EN LOS QUE SEA PARTE ESPAÑA	6	139
SE REALIZA A EFECTOS DE PRESTAR AUXILIO JUDICIAL INTERNACIONAL	2	2
ES NECESARIA PARA LA PREVENCIÓN O PARA EL DIAGNÓSTICO MÉDICOS, LA PRESTACIÓN DE ASISTENCIA SANITARIA O TRATAMIENTO MÉDICOS O LA GESTIÓN DE SERVICIOS SANITARIOS	1	21
SE REFIERE A TRANSFERENCIAS DINERARIAS, CONFORME A SU LEGISLACIÓN ESPECÍFICA	1	41
EL AFECTADO HA DADO SU CONSENTIMIENTO	5	445
ES NECESARIA PARA LA EJECUCIÓN DE UN CONTRATO ENTRE EL AFECTADO Y EL RESPONSABLE DEL FICHERO O PARA LA ADOPCIÓN DE MEDIDAS PRECONTRACTUALES ADOPTADAS A PETICIÓN DEL AFECTADO	2	164
ES NECESARIA PARA LA CELEBRACIÓN O EJECUCIÓN DE UN CONTRATO CELEBRADO O POR CELEBRAR, EN INTERÉS DEL AFECTADO, POR EL RESPONSABLE DEL FICHERO Y UN TERCERO	2	150
ES NECESARIA O LEGALMENTE EXIGIDA PARA LA SALVAGUARDA DE UN INTERÉS PÚBLICO	2	6
ES PRECISA PARA EL RECONOCIMIENTO, EJERCICIO O DEFENSA DE UN DERECHO EN UN PROCESO JUDICIAL	3	7
SE EFECTÚA , A PETICIÓN DE PERSONA CON INTERÉS LEGÍTIMO, DESDE UN REGISTRO PÚBLICO Y ES ACORDE CON LA FINALIDAD DEL MISMO	2	19

DISTRIBUCIÓN DE DOCUMENTOS DE ENTRADA/SALIDA RELACIONADOS CON EL RGPD DURANTE EL AÑO 2001

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
DOCUMENTOS DE ENTRADA													
NOTIFICACIONES INSCRIPCION	1.110	1.135	922	824	997	1.945	2.083	894	1.176	1.812	1.333	847	15.078
SOPORTE PAPEL	416	317	317	285	299	842	935	306	299	536	328	146	5.026
SOPORTE MAGNÉTICO	146	131	128	99	111	243	181	106	115	112	159	88	1.619
SOPORTE INTERNET	548	687	477	440	587	860	967	482	762	1.164	846	613	8.433
OTRAS SOLICITUDES	148	124	159	127	162	199	188	106	144	219	174	46	1.796
T O T A L E S	1.258	1.259	1.081	951	1.159	2.144	2.271	1.000	1.320	2.031	1.507	893	16.874
	ENE	**FEB**	**MAR**	**ABR**	**MAY**	**JUN**	**JUL**	**AGO**	**SEP**	**OCT**	**NOV**	**DIC**	**TOTAL**
REGISTROS DE SALIDA													
SALIDAS VARIAS	28	52	75	52	74	55	96	29	71	104	67	105	808
RESOLUCIONES DE INSCRIPCIÓN	2.643	2.940	2.236	1.748	2.059	2.232	4.361	3.396	2.574	3.346	2.498	3.278	33.311
RESOLUCIONES NEGATIVAS	166	90	70	73	64	97	228	94	68	59	71	46	1.126
REQUERIMIENTOS DEL RGPD	89	77	108	94	48	123	223	60	75	110	67	178	1.252
T O T A L E S	2.926	3.159	2.489	1.967	2.245	2.507	4.908	3.579	2.788	3.619	2.703	3.607	36.497

RESUMEN DE OPERACIONES DE INSCRIPCIÓN REALIZADAS EN EL RGPD DURANTE EL AÑO 2001

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
OPERACIONES A INSTANCIA DEL INTERESADO													
Altas	2.029	2.122	1.395	1.448	1.713	1.753	3.755	2.838	2.211	2.276	1.662	2.911	26.113 (1)
Modificaciones	355	615	1.187	187	252	312	409	202	271	612	546	213	5.161
Supresiones	284	248	382	323	120	166	274	356	116	538	455	177	3.439
T O T A L	2.668	2.985	2.964	1.958	2.085	2.231	4.438	3.396	2.598	3.426	2.663	3.301	34.713
OPERACIONES DE SUBSANACION DE OFICIO													
Modificaciones	60	544	140	141	231	117	106	202	107	260	286	47	2.241 (2)
Supresiones	0	3	0	8	0	1	0	2	0	0	0	0	14
T O T A L	60	547	140	149	231	118	106	204	107	260	286	47	2.255
T O T A L E S	**2.728**	**3.532**	**3.104**	**2.107**	**2.316**	**2.349**	**4.544**	**3.600**	**2.705**	**3.686**	**2.949**	**3.348**	**36.968**

(1) A 31 de diciembre de 2001, 89 de estas operaciones de alta constaban suprimidas
(2) En estas modificaciones de oficio se contabilizan 6 operaciones que han supuesto la inscripción de 6 ficheros no contabilizados en las operaciones de alta

III. SUBDIRECCIÓN GENERAL DE INSPECCIÓN DE DATOS

1. INTRODUCCIÓN: ACTIVIDAD DE LA INSPECCIÓN DE DATOS.

La Subdirección General de Inspección de Datos es el órgano de la Agencia de Protección de Datos (APD) que tiene encomendada las funciones básicas para velar por el cumplimiento efectivo de la normativa de protección de datos como son la inspectora y la instructora de expedientes.

En la Memoria correspondiente al ejercicio anterior se recogen exhaustivamente las normas reguladoras de ambas funciones, así como sus características. A ella debe remitirse al lector interesado.

Basta aquí con señalar que la función inspectora o de investigación tiene como finalidad la averiguación de los hechos que hayan concurrido en el tratamiento de datos personales y que la función instructora despliega sus efectos en una doble orden de procedimientos: los expedientes sancionadores por infracción de la LOPD, tanto respecto de los responsables de ficheros de titularidad pública como de titularidad privada o de encargados del tratamiento, en su caso; y los expedientes de tutela de derechos dirigidos a garantizar el ejercicio de los que la norma citada atribuye a los ciudadanos.

1.1. Expedientes relacionados con la función inspectora

En el ejercicio de la función inspectora realizada por la APD durante el año 2001 se iniciaron **405** actuaciones de investigación o inspección, en su mayor parte promovidas por denuncias presentadas por los ciudadanos ante la APD, con el objeto de comprobar posibles vulneraciones de los principios de la LOPD.

De estas **405** actuaciones de inspección iniciadas durante 2001, **286** han finalizado en dicho ejercicio, estando el resto: **119**, pendientes de concluir. A las **286** actuaciones de inspección iniciadas y finalizadas en 2001 hay que añadir aquellas otras, en concreto **132**, que iniciadas el año anterior finalizaron en el presente año, lo que hace un total de **418** actuaciones de inspección terminadas en 2001.

Así mismo, y al margen de lo anterior, se han realizado durante el mismo año **171** actuaciones de información previa con el fin de determinar con carácter preliminar si concurrían circunstancias que justificaran la iniciación de una actuación de inspección y, en su caso, posterior incoación del correspondiente procedimiento.

El fundamento de este tipo de actuaciones se encuentra en el art. 69.2 de la Ley 30/1992, de 26 de noviembre, desarrollado por el art. 12 del Real Decreto 1298/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora, que permiten realizar actuaciones previas con anterioridad a la iniciación de un concreto procedimiento. Añade el citado precepto reglamentario que las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia; en nuestro caso, los Inspectores de Datos conforme a lo previsto en el art 40.2 LOPD.

1.2. Expedientes relacionados con la función instructora

De las tres clases de procedimientos incoados en 2001 por lo órganos instructores de la Inspección de Datos, **138** corresponden a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad privada; **80** a procedimientos sancionadores iniciados frente a responsables de ficheros de titularidad pública (procedimientos por infracciones de las Administraciones Públicas); y **363** se corresponden a los iniciados por procedimientos de tutela de derechos.

De los **138** procedimientos sancionadores iniciados durante el año 2001, han finalizado en dicho ejercicio **65**, estando el resto: **73** pendientes de concluir. A los **65** procedimientos sancionadores iniciados y finalizados en el 2001 hay que añadir aquellos otros, en concreto **60**, que iniciados el año anterior finalizaron en el presente, lo que suma un total de **125** procedimientos sancionadores terminados en 2001.

De los **80** procedimientos por infracciones de las Administraciones Públicas iniciados en el 2001, **5** han finalizado en dicho año, estando los **75** restantes pendientes de conclusión. Así mismo, se han concluido durante el presente ejercicio **9** procedimientos de esta clase provenientes del año anterior, lo que supone la conclusión de **14** procedimientos por infracciones de las Administraciones Públicas en 2001.

A los anteriores procedimientos deben añadirse 210 Resoluciones de Archivo, que debidamente motivadas se dictan tras la correspondiente investigación previa de los hechos denunciados, después de comprobar que no constituyen infracción de la legislación en materia de protección de datos o bien que no entran en el ámbito de aplicación de la misma.

Así mismo, se han dictado 5 Resoluciones a raíz de diversas peticiones de colaboración realizadas por el Presidente de la Comisión Nationale de L'Informatique et des Libertes (CNIL), autoridad competente en materia de protección de datos en Francia, al amparo del art. 114.2 del Convenio Schengen, en relación con peticiones de acceso y cancelación de los ficheros del Sistema de Información Schengen.

Finalmente, de los **363** procedimientos de tutela de derechos iniciados en 2001, **264** han finalizado en el mismo ejercicio, quedando tan sólo **99** pendientes de concluir. A los **264** antes citados hay que añadir los procedimientos de esta clase iniciados el año anterior, en concreto **56**, y terminados en el presente, lo que hace un total de **320** procedimientos de tutela de derechos concluidos en el 2001.

A todos los procedimientos anteriores deben añadirse la resolución de **95** recursos de reposición resueltos durante el mismo año 2001. La Ley 4/1999, de 13 de enero, de Modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ha restablecido el recurso de reposición contra los actos que ponen fin a la vía administrativa, con carácter potestativo (art. 116 Ley 30/1992), lo que ha supuesto aumentar notablemente la carga de trabajo, no sólo de la actividad de instrucción sino también de la Secretaría General de la Agencia en cuanto que es este órgano el que califica la pertinencia de las garantías presentadas por el recurrente con objeto de obtener la suspensión de la ejecución del acto impugnado.

De los **95** recursos de esta clase presentados, **1** ha sido estimado, **1** estimado parcialmente, **20** inadmitidos por extemporáneos o falta de legitimación y **73** desestimados por falta de fundamento de las pretensiones formuladas. No obstante, aun en estos últimos, su formulación ha facilitado la petición de suspensión de la ejecución de la Resolución sancionadora, lo que ha sido concedido por la Agencia en todos los casos en que se han considerado cumplidos los requisitos exigidos por la Ley 30/1992, de 26 de noviembre.

Como conclusión ha de señalarse que durante el ejercicio 2001 se han emitido un total de 769 Resoluciones, que comprende la suma de los procedimientos sancionadores, resoluciones de archivo, actuaciones de colaboración con la CNIL, procedimientos de tutela de derechos y recursos de reposición.

1.3. Estadísticas mediante gráficos de los expedientes referidos.

1.3.1. Gráficos correspondientes a la función inspectora.

A continuación, se puede observar en los gráficos I, II, y III la distribución geográfica de las actuaciones de investigación o inspección correspondientes al año 2001, referida anteriormente en el apartado 1.1, y separadas por provincia del denunciante, provincia del denunciado y sectores de actividad inspeccionados.

GRÁFICO I
ACTUACIONES DE INSPECCIÓN INICIADAS POR PROVINCIA DEL DENUNCIANTE

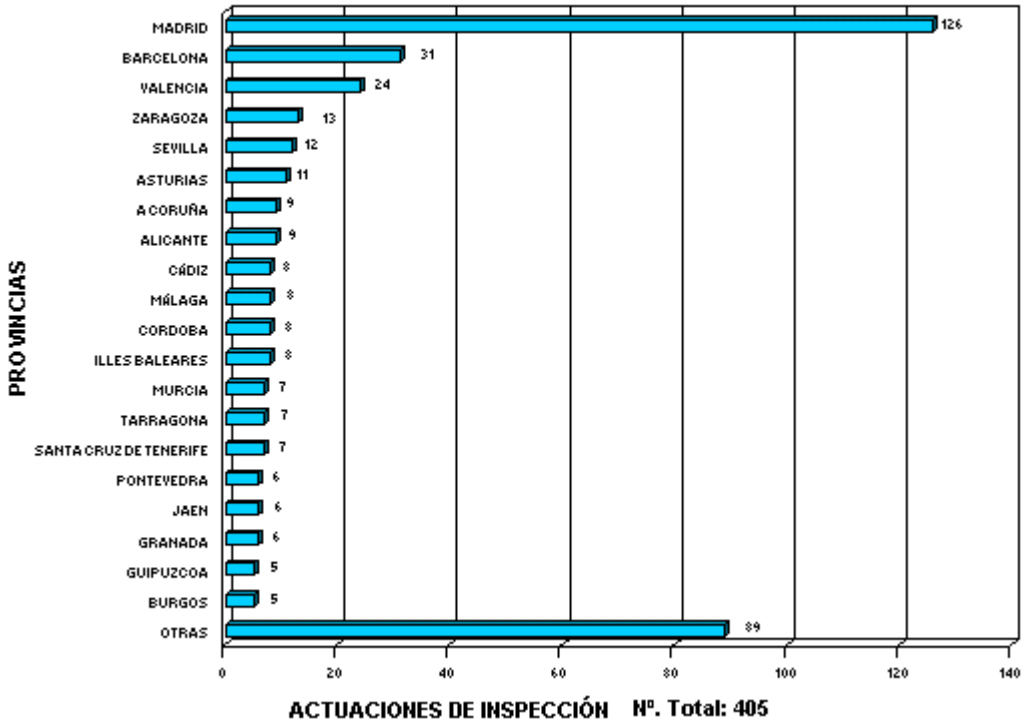


GRÁFICO II
ACTUACIONES DE INSPECCIÓN INICIADAS POR PROVINCIA DEL DENUNCIADO

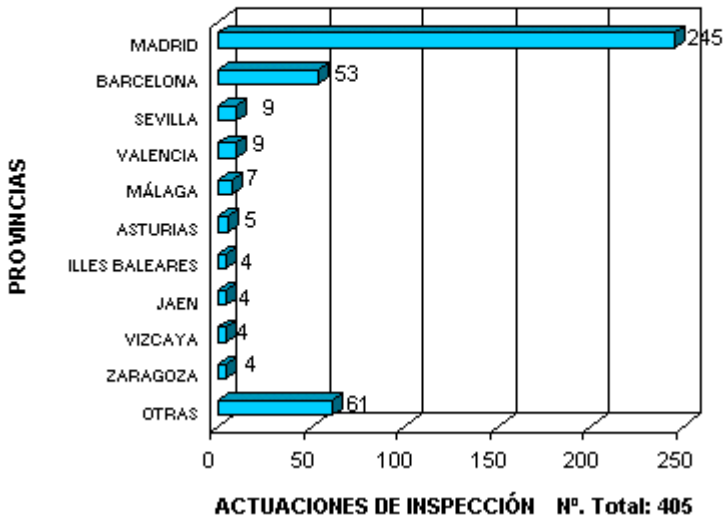
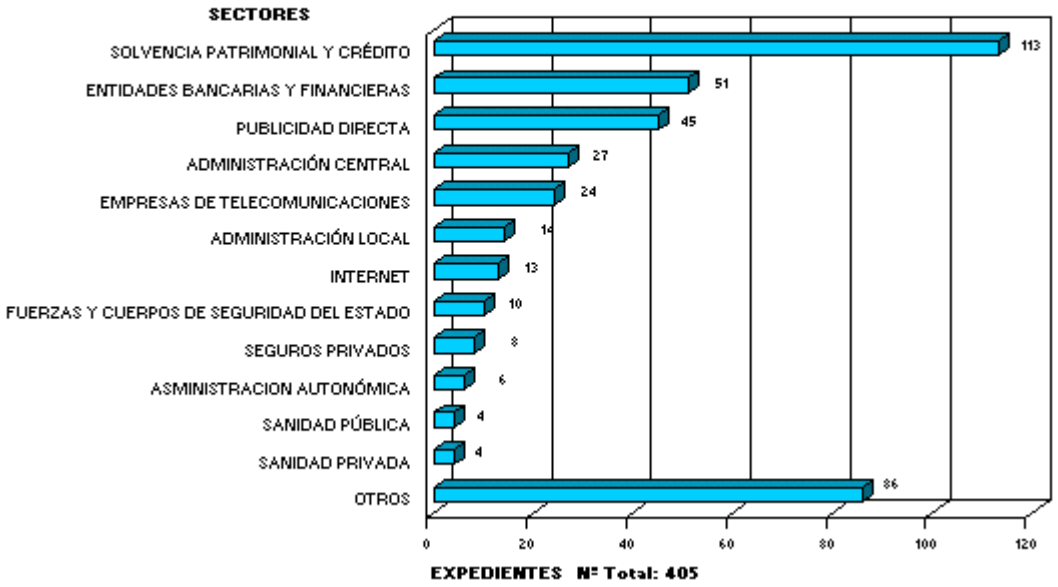
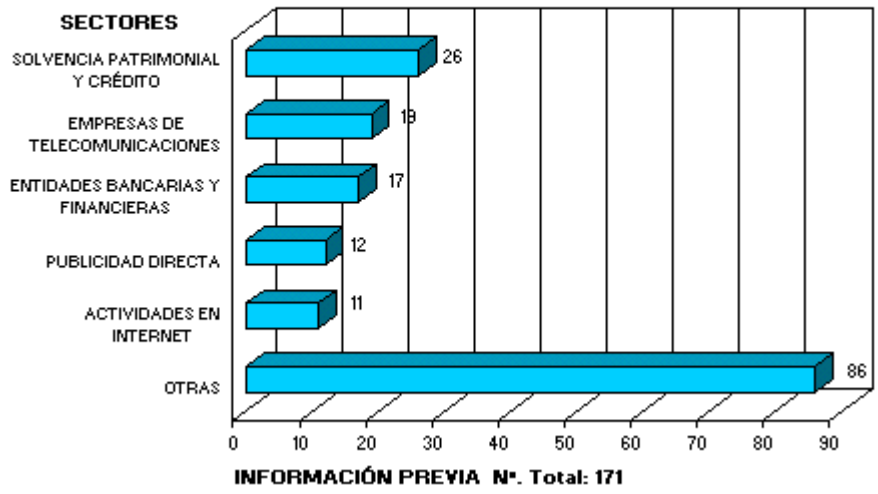


GRÁFICO III
ACTUACIONES DE INSPECCIÓN INICIADAS POR SECTORES DE ACTIVIDAD



A continuación, en el gráfico IV, se puede apreciar detalladamente la distribución por sectores de actividad de las actuaciones de información previa realizadas en 2001 a las que alude el anterior apartado 1.1.

GRÁFICO IV
ACTUACIONES DE INFORMACIÓN PREVIA POR SECTORES



1.3.2. Gráficos correspondientes a la función instructora

Seguidamente, en los gráficos V y V bis, VI y VI bis y VII, se puede apreciar de forma detallada la evolución del número de expedientes tramitados durante 2001 y que afectan a la función instructora a la que alude el anterior apartado 1.2., esto es, procedimientos sancionadores incoados frente a responsables de ficheros de titularidad privada, procedimientos sancionadores por infracciones de las Administraciones Públicas y procedimientos de tutela de derechos.

Así mismo, y dentro de la función instructora destaca el gráfico VIII que presenta la situación de los recursos de reposición.

GRÁFICO V
PROCEDIMIENTOS SANCIONADORES INICIADOS POR SECTORES

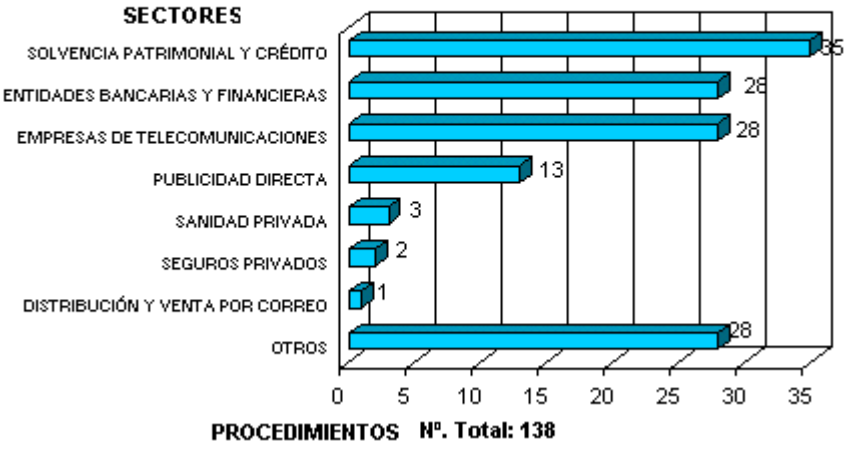


GRÁFICO V-bis
PROCEDIMIENTOS SANCIONADORES INICIADOS POR PROVINCIAS

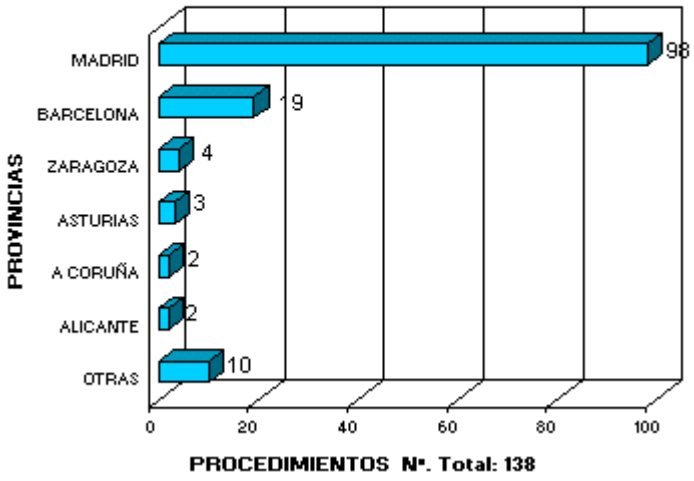


GRÁFICO VI
PROCEDIMIENTOS DE LAS AAPP INICIADOS POR SECTORES

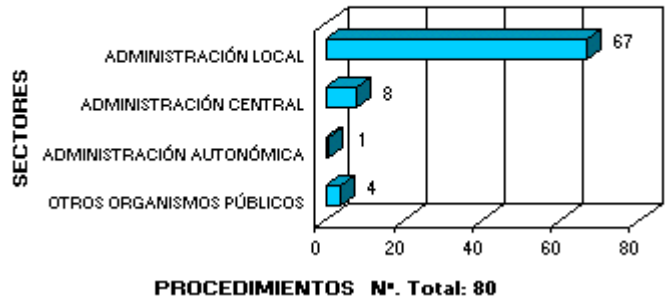


GRÁFICO VI- bis
PROCEDIMIENTOS DE LAS AAPP INICIADOS POR PROVINCIAS

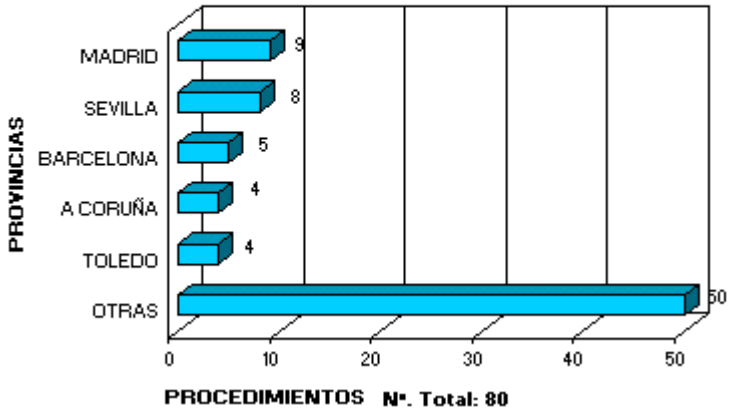


GRÁFICO VII
PROCEDIMIENTOS DE TUTELA DE DERECHOS INICIADOS POR SECTORES

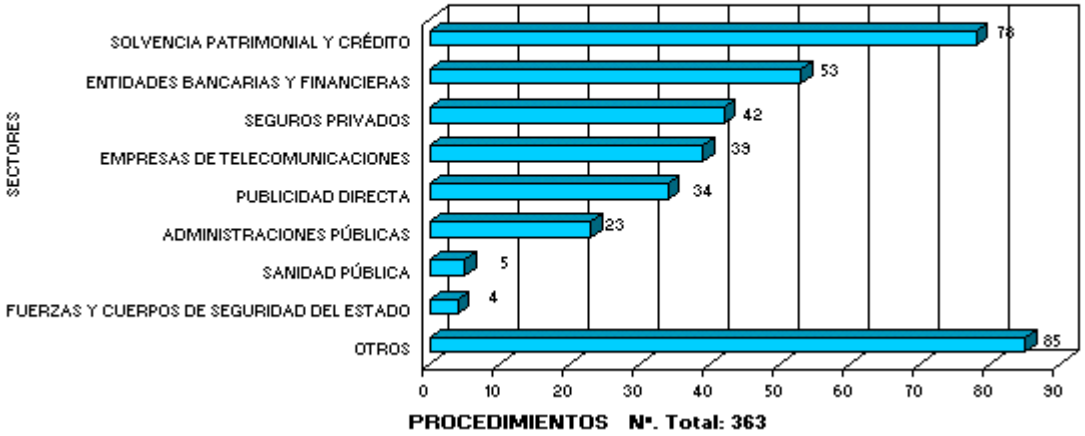
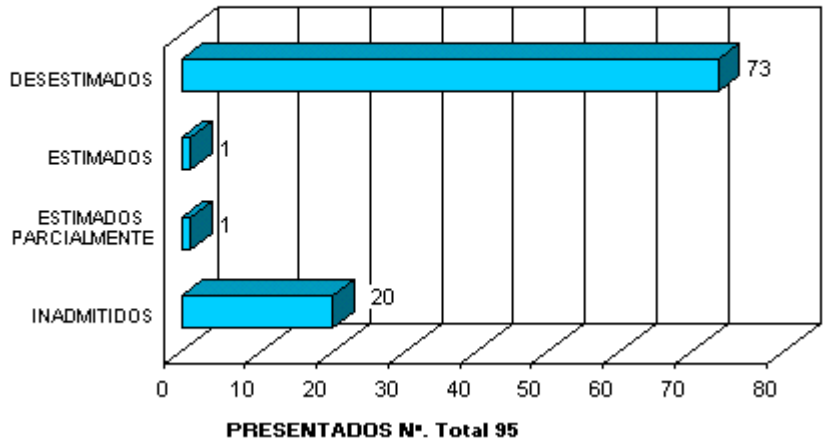
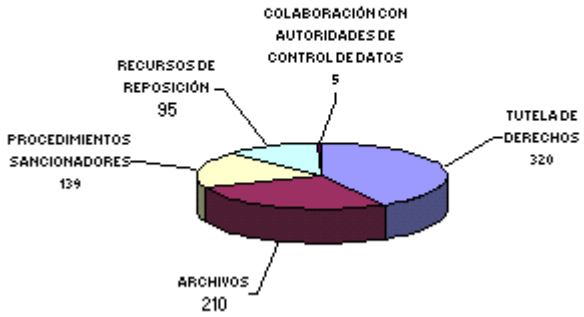


GRÁFICO VIII
RECURSO DE REPOSICIÓN



Por último, en el gráfico IX se presentan el total de resoluciones correspondientes a los procedimientos terminados durante el año 2001.

GRÁFICO IX
PROCEDIMIENTOS TERMINADOS
TOTAL RESOLUCIONES AÑO 2001: 769



2. PLANES SECTORIALES DE OFICIO

Una de las modalidades a través de la cual actúa la Inspección de Datos es la realización de Planes Sectoriales de Oficio. Con ellos se pretende evaluar el grado de cumplimiento de la normativa de protección de datos en el conjunto de un sector de actividad previamente definido. Estas inspecciones concluyen habitualmente con la formulación por el Director de la Agencia de RECOMENDACIONES, dictadas al amparo y en virtud de las potestades que le otorga el artículo 5 c) del Real Decreto 426/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, con el fin de que sean conocidas y cumplidas no solo por las entidades inspeccionadas, sino por el conjunto de responsables de ficheros que operan en el sector.

Las inspecciones sectoriales abarcan, cada año, a sectores de actividad de naturaleza pública y privada.

Durante el año 2001 finalizaron las Inspecciones Sectoriales realizadas al Consorcio de Compensación de Seguros, Sector de Grandes Superficies Comerciales y Comercio Electrónico, dictándose las correspondientes RECOMENDACIONES de las que se informa a continuación. Respecto del sector de Telefonía Móvil se detallan básicamente, las conclusiones de la Inspección, sobre las que deberán posteriormente dictarse Recomendaciones.

2.1. Actuaciones derivadas de los Planes de Oficio 2000

2.1.1. Recomendaciones al Consorcio de Compensación de Seguros.

Como ya se indica en la Memoria anterior, en el transcurso del año 2001 se han dictado las pertinentes Recomendaciones del Plan de Inspección de Oficio realizado al Consorcio de Compensación de Seguros, que deberán ser observadas por la entidad inspeccionada al objeto de adecuar plenamente los tratamientos automatizados a los principios de protección de datos y que se transcriben a continuación:

Recomendación Primera: Cancelación de Datos.

El Consorcio mantiene datos personales en los Sistemas de Información *Expedientes de Siniestros*, *Seguros Directos* y *Fichero Informativo de Vehículos Asegurados* desde la creación de los mismos en el año 1968, 1975 y 1996, respectivamente.

La Ley Orgánica 15/1999, en el artículo 4.5 bajo el epígrafe "calidad de datos", consagra el principio de conservación limitada de los datos al disponer: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados*" .

Por otra parte, los apartados 3 y 5 del artículo 16 de la citada Ley especifican: "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".

Por ello, en virtud de las prescripciones legales transcritas, el Consorcio deberá proceder al bloqueo de todos aquellos datos de carácter personal incluidos en sus Sistemas de Información que hayan dejado de ser necesarios al fin para el que fueron recabados o registrados y proceder a su cancelación definitiva una vez cumplidos los plazos de prescripción derivados de las obligaciones o responsabilidades nacidas del tratamiento. Por excepción, se podrán mantener determinados datos por interés histórico, estadístico o científico, de acuerdo con su legislación específica.

Recomendación Segunda: Derecho de Información en la recogida de Datos.

El Consorcio, con objeto de cumplir las funciones que legalmente tiene atribuidas, recaba información de los propios afectados por medio de los pertinentes modelos o impresos, así como de entidades públicas o privadas en los términos establecidos en las normas por las que se rige. Sin embargo, se han observado ciertas deficiencias respecto del deber de información que establece la legislación sobre protección de datos.

Según prevé el apartado 1 del artículo 5 de la LOPD "Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma legible, las advertencias a que se refiere el apartado anterior".

En este sentido, el Consorcio de Compensación de Seguros deberá tener en cuenta que cuando proceda a la recogida de datos personales a través de impresos o cuestionarios – y se den las circunstancias previstas en el artículo 5.3 de la LOPD – , el responsable de la recogida deberá informar en todo caso al menos de los aspectos que referencian los apartados a) y e) anteriores, a cuyo efecto los modelos de impresos o cuestionarios que se establezcan por el Consorcio deberán incluir las correspondientes cláusulas informativas.

Entiende esta Agencia de Protección de Datos que el contenido de los mencionados apartados a) y e) del art. 5.1 de la LOPD constituyen elementos básicos para ejercer los derechos de acceso, rectificación, cancelación y oposición, por lo que son de obligada comunicación por el responsable del fichero, toda vez que el desconocimiento de estos aspectos esenciales supone una clara indefensión para el ciudadano que le imposibilita el ejercicio de tales derechos.

Recomendación Tercera: Consentimiento del afectado en el tratamiento de sus datos personales.

El Consorcio de Compensación de Seguros procede a recabar y tratar datos personales sin el consentimiento de los afectados en el ámbito del ejercicio de las funciones que tiene encomendadas por la Ley. La información es facilitada en los impresos establecidos al efecto por el Organismo requiriéndose en los mismos la firma del solicitante o afectado.

Por aplicación del artículo 6.1 de la Ley Orgánica 15/1999, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. Sin embargo, el artículo 6.2 de la citada norma establece que no será preciso el consentimiento del afectado cuando sus datos personales se recojan para el

ejercicio de las funciones propias del Consorcio en el ámbito de sus competencias, esto es, tratándose del *Fichero Informativo de Vehículos Asegurados* de titularidad pública; así como tampoco será preciso dicho consentimiento cuando los datos recogidos afecten a las partes de un contrato y sean necesarios para su mantenimiento o cumplimiento, tal como sucede para los ficheros *Seguros Directos* y *Expedientes de Siniestros* de titularidad privada.

No obstante, el Consorcio trata datos especialmente protegidos de los regulados en el artículo 7 de la citada Ley, que se refieren a la salud de las personas implicadas en un siniestro y que son facilitados por los propios afectados o por terceros. En estos casos, y salvo excepción legal, se requiere que el consentimiento del afectado para el tratamiento de sus datos de salud sea dado con las garantías y formalidades prescritas en el artículo 7.3 de la LOPD, esto es, de forma expresa.

En consecuencia, siempre que resulte necesario para la tramitación de un siniestro derivado del Seguro de Responsabilidad Civil de Automóviles de suscripción obligatoria en los que el Consorcio tenga la condición de asegurador o reasegurador, podrá tratar datos de salud sin consentimiento expreso de los interesados en la medida en que dicho tratamiento resulte necesario para la finalidad que la norma habilita. En aquellos otros casos en los que el Consorcio no cuente con cobertura legal suficiente para tratar datos especialmente protegidos en los términos expuestos en el anterior apartado 1.6, se deberá establecer por el mismo un procedimiento que permita prestar el consentimiento expreso de los afectados para el tratamiento de sus datos de salud, a excepción del supuesto en que el afectado esté física o jurídicamente incapacitado para ello.

Recomendación Cuarta: Comunicación de datos.

De acuerdo a lo establecido en el artículo 11 de la LOPD, "los datos de carácter personal objeto de tratamiento sólo podrán se comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". El consentimiento no será preciso, entre otros, cuando la cesión está autorizada en una Ley o si la comunicación se efectúa previo procedimiento de disociación.

De la normativa aplicable se desprende que el Consorcio sólo podrá facilitar datos personales incluidos en sus ficheros automatizados a personas físicas y entidades públicas y privadas, a los efectos del cumplimiento de la normativa sobre Tributos y Seguros, así como para facilitar el control de la obligación de asegurarse.

Recomendación Quinta: Acceso a los datos por cuenta de terceros.

El Consorcio de Compensación de Seguros tiene contratado con terceros la prestación de servicios informáticos del *Fichero Informativo de Vehículos Asegurados* y el Servicio de Atención Telefónica de información sobre *Expedientes de Siniestros*.

De conformidad con lo dispuesto en el artículo 12.2 de la LOPD, "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará ni siquiera para su conservación, a otras personas. En el contrato se estipularán, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar". De otro lado, el Real Decreto 994/1999, establece las medidas de seguridad que deberán de cumplir los ficheros automatizados que contengan datos de carácter personal, tanto por el responsable del fichero como por el encargado del tratamiento.

Por todo ello, con objeto de conseguir una mejor adecuación de los tratamientos automatizados a los principios de la normativa de protección de datos, el Consorcio deberá establecer las medidas de seguridad que el "encargado" del tratamiento está obligado a implementar, así como efectuar los controles necesarios con objeto de verificar de forma periódica el cumplimiento de las mismas.

Por otro lado, deberá tenerse en cuenta que el acceso a los datos personales por cuenta de terceros para la prestación de servicios deberá ser adecuado, pertinente y no excesivo en relación con el cumplimento de las finalidades establecidas en el contrato. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Consorcio como responsable del fichero.

Recomendación Sexta: Derechos de acceso, rectificación, cancelación y oposición.

De conformidad con lo dispuesto en los artículos 15 y siguientes de la Ley Orgánica 15/1999, los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados, se configuran como uno de los ejes fundamentales sobre los que se articula la protección de los datos de ciudadanos, y aparecen regulados, además, en el Real Decreto 1332/1999 y en la Instrucción 1/1998 de la Agencia de Protección de Datos. Los derechos de acceso, así como los de rectificación y cancelación de datos son derechos personalísimos y el Consorcio de Compensación de Seguros, como responsable del fichero, resolverá sobre la solicitud en los plazos establecidos por la ley. En el supuesto de que el Organismo considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente en el plazo legalmente establecido. Si no fuere debidamente atendido, el afectado podrá reclamar ante la Agencia de Protección de Datos.

La norma Primera de la Instrucción 1/1998, establece los requisitos generales a cumplir tanto por el ciudadano en la solicitud del ejercicio de los derechos como por parte del responsable del fichero con objeto de resolver sobre la solicitud. A tal efecto, el apartado 5 de la citada norma dispone "*El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos".*

En este sentido, esta Agencia entiende que a fin de dar una mejor respuesta a los ciudadanos en el ejercicio de sus derechos, sería conveniente que el Consorcio de Compensación de Seguros estableciera un procedimiento documentado con objeto de su conocimiento y cumplimiento por parte de todas las personas que integran la Organización.

De otro lado, el artículo 6.4 de la LOPD establece que, "En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación persona". En tal supuesto, el Consorcio como responsable del fichero excluirá del tratamiento los datos relativos al afectado cuando se den todas las circunstancias previstas en la norma transcrita.

Recomendación Séptima: Reglamento de medidas de seguridad.

La Ley Orgánica 15/1999, en su artículo 9 dispone que "el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria".

El Real Decreto 994/1999, aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que se clasifican en tres niveles atendiendo a la naturaleza de la información tratada y la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

De acuerdo a lo establecido en el citado Reglamento, el Consorcio deberá cumplir con carácter general las medidas de seguridad de nivel medio establecidas en los artículos 15 y siguientes.

En particular, el *Fichero Informativo de Vehículos Asegurados* deberá cumplir con las medidas de nivel básico previstas en los artículos 8 y siguientes, y el Sistema de Información *Expedientes de Siniestros*, que incluye datos referentes a la salud de las personas que han sufrido daños personales, deberá adaptarse a las medidas de seguridad calificadas como de nivel alto y que se detallan en los artículos 23, 24, 25 y 26 del Real Decreto 994/1999, que serán exigibles a partir del 26 de junio de 2002, de conformidad con lo previsto en la Resolución del Ministerio de Justicia de 22 de junio de 2001 (B.O.E. 25 de junio de 2001).

De acuerdo con todo ello, el Consorcio deberá elaborar e implementar el Documento de Seguridad en los términos establecidos en el artículo 8 del Reglamento, "El documento deberá contener, como mínimo, los siguientes aspectos: a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos. b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento. c) Funciones y obligaciones del personal. d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan. e) Procedimiento de notificación, gestión y respuesta ante las incidencias. f) Los procedimientos de realización de copias de respaldo y de recuperación. El documento deberá mantenerse en todo momento actualizado (..)".

Por otra parte, el Consorcio adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento, informando de la obligación de guardar secreto de los datos personales a los que tengan acceso en el desempeño de sus funciones, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del fichero.

Sobre dichas Recomendaciones, el Consorcio de Compensación de Seguros ha informado a esta Agencia de las actuaciones llevadas a cabo durante los últimos meses con objeto de subsanar las deficiencias detectadas y, así, salvaguardar mejor los derechos de los ciudadanos. En este sentido, se ha procedido por parte del citado Organismo a la modificación del contenido de la inscripción en el Registro General de Protección de Datos de los ficheros automatizados cuya titularidad ostenta en los términos especificados en las conclusiones del Plan de Inspección.

2.1.2. Recomendaciones al sector del Comercio Electrónico

Teniendo como referencia el resultado de las actuaciones de Inspección llevadas a cabo en el pasado año 2000, y dándose la circunstancia de que en el momento de dictar las presentes Recomendaciones se había producido una coincidencia temporal con el análisis que el Grupo de Trabajo sobre la protección de datos personales integrado por las autoridades competentes de los Estados Miembros de la Unión Europea competente –Grupo del art. 29 de la Directiva 45/96/CE- ha realizado respecto de los "*requisitos mínimos para la recogida en línea de datos personales*", estos últimos se han tenido en cuenta en la medida en que los hechos constatados en la inspección permiten aplicar los requisitos del documento citado. De este modo, la Agencia Española de Protección de Datos trata de contribuir a la

aplicación eficaz y homogénea de las disposiciones nacionales adoptadas en la transposición de las Directivas comunitarias y, aportando el valor añadido de aquel documento, tratar de detallar, a escala europea, un conjunto mínimo de obligaciones que puedan seguir fácilmente los responsables del tratamiento.

Recomendación Primera: Información en la recogida de datos

De conformidad con lo establecido por el artículo 5 de la LOPD, los interesados a los que se soliciten datos personales a través de Internet deberán ser previamente informados de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En todas y cada una de las páginas web desde las que se recaben datos de carácter personal se incluirá claramente visible la información a la que hace referencia el artículo 5 de la LOPD, que el usuario deberá poder obtener con facilidad y de forma directa y permanente.

Podrá optarse por incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un "*click*", permita obtener la citada información. No obstante, se considera más adecuada una opción según la cual la lectura de dicha información se presente como ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.

En particular, se especificará claramente el nombre o denominación social y el domicilio del responsable del fichero al que se incorporarán los datos personales solicitados, así como una referencia al código de inscripción asignado por el Registro General de Protección de Datos. Deberá indicarse también la dirección ante la cual pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición, en el caso de que sea distinta del domicilio especificado, así como el procedimiento que deberán seguir los usuarios, ya sea electrónico, postal, telefónico o cualquier otro que se considere válido.

En el caso de que los datos personales vayan a ser inicialmente incorporados a los ficheros de distintos responsables, se referirá toda la información anterior a cada uno de ellos.

Cuando el responsable no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España.

En todo caso, la información deberá proporcionarse en el mismo idioma en que se recaban los datos personales.

Cuando para realizar una transacción comercial a través de Internet se estén utilizando los servicios de "*pasarela de pago*" prestados por determinadas entidades financieras no se almacenarán datos que puedan relacionar la identificación del medio de pago con la identidad de su titular, salvo que sea preciso para los fines legítimos que se persigan.

El usuario deberá estar convenientemente informado en todo caso del momento en que desde una web se transfiere el control a otra web, de tal forma que no pueda albergar dudas al respecto. En este sentido, se considera una buena práctica que el responsable de la web se cerciore de que las webs a las que se transfiere el control cumplen también los términos expresados en la presente Recomendación.

Recomendación Segunda: Consentimiento del afectado

De acuerdo con lo que dispone el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa o sean de aplicación las excepciones previstas en el apartado 2 del mismo artículo.

Cuando un usuario facilita voluntariamente sus datos de carácter personal a través de Internet para una finalidad distinta de la mera ejecución de la transacción comercial, se entenderá que consiente en el tratamiento de los mismos en los términos de los que ha sido convenientemente informado en el momento de la recogida.

Siempre que la Ley no lo impida y el afectado haya revocado su consentimiento para el tratamiento de sus datos de carácter personal, el responsable del fichero habilitará los medios oportunos para excluir del tratamiento dichos datos.

Recomendación Tercera: Usos y finalidades

Tal y como dispone el apartado 1 del artículo 4 de la LOPD, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

No se recabarán a través de Internet datos personales cuyo conocimiento por parte del responsable no esté justificado por la finalidad para la que se recaban y de la cual el usuario no haya sido previamente informado. A este respecto, se

considera una buena práctica que se facilite y permita la consulta anónima de sitios comerciales sin solicitar a los usuarios que se identifiquen mediante su nombre, apellidos, dirección electrónica u otros datos.

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquella que ha justificado su recogida. En este sentido, para que tales datos puedan ser usados con una finalidad no compatible con ésta, es imprescindible obtener previamente el consentimiento inequívoco del afectado. Para recabar este consentimiento en Internet, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar su voluntad en uno u otro sentido.

Para que la ausencia de manifestación de la voluntad del usuario pueda producir alguna consecuencia respecto del tratamiento de sus datos, deberá habérsele advertido expresamente de esta circunstancia, así como de los efectos de la misma.

Cuando se haya previsto que los datos sean utilizados de forma tal que los usuarios de una web puedan ser segmentados o categorizados con fines comerciales, a partir de la información personal y comercial que consta en los ficheros, se informará claramente de esta circunstancia al usuario en el momento de recabar sus datos. Así mismo, se le concederá la facultad de oponerse a esta modalidad de tratamiento, indicándole el procedimiento que deberá seguir en el caso de que decida hacer uso de ella.

Si, aparte de los datos personales que facilita voluntariamente el interesado a través de Internet, se utilizan procedimientos automáticos invisibles de recogida de datos relativos a una persona identificada o identificable (*cookies*, datos de navegación, información proporcionada por los navegadores, contenidos activos,...) se informará claramente de esta circunstancia al usuario, *antes* de comenzar la recogida de datos a través de ellos o de desencadenar la conexión del ordenador del usuario con otro sitio web.

Así mismo, se deberá informar al afectado del nombre de dominio del servidor que transmite o activa los procedimientos automáticos de recogida, de la finalidad de los mismos, de su plazo de validez, de si es necesaria o no la aceptación de dichos procedimientos para visitar el sito web y de la opción de que dispone todo usuario de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de dichos procedimientos, cuando dicha opción esté disponible para el usuario.

Cuando los datos recabados a través de Internet vayan a ser utilizados para el envío (postal o electrónico) de información comercial, se informará también de esta circunstancia al usuario en el momento de recabar sus datos. Así mismo, se le concederá la facultad de oponerse a esta modalidad de tratamiento, indicándole el procedimiento que deberá seguir en el caso de que decida hacer uso de ella.

Recomendación Cuarta: Cancelación de datos

Según prevé el apartado 5 del artículo 4 de la LOPD, los datos de carácter personal serán cancelados a propia iniciativa del responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. Igualmente serán cancelados cuando así lo solicite el interesado.

No obstante, la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Recomendación Quinta: Datos de salud y de vida sexual

De conformidad con lo establecido en el apartado 3 del artículo 7 de la LOPD, los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

Los ficheros con datos acerca de transacciones de adquisición de determinados productos o servicios (por ejemplo, productos eróticos u ortopédicos) podrían contener en ocasiones un conjunto de datos de carácter personal suficientes que permitan ser tratados para obtener una evaluación de la personalidad del individuo, relativa a su salud o a su vida sexual. En tales casos este tratamiento sólo podrá realizarse cuando el afectado haya consentido expresamente.

A estos efectos, se considerará válido un procedimiento en el que el usuario tenga una participación activa, de tal forma que, a través de la web, pueda manifestar expresamente su voluntad de que tales datos sean recabados y tratados.

Recomendación Sexta: Acceso a los datos por cuenta de terceros

De conformidad con lo dispuesto en el apartado 1 del artículo 12 de la LOPD, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el citado contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En particular, estas obligaciones se extenderán a todas aquellas entidades que, como encargados del tratamiento, intervengan en el desarrollo de la relación establecida con los usuarios de la web. A este respecto, el prestador del servicio no podrá utilizar los datos para fin distinto del que conste en el contrato, ni subcontratar la gestión del servicio con terceros, salvo que lo haga en nombre y por cuenta del responsable.

Recomendación Séptima: Comunicación de datos

Según dispone el apartado 1 del artículo 11 de la LOPD, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

A este respecto se tendrán en cuenta, sin embargo, las excepciones previstas en el apartado 2 del citado artículo, y en particular, la referida a la situación en la que el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este último caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

De acuerdo a lo que establece el apartado 3 del mismo artículo y en consonancia con lo expresado por el apartado 2 de la Recomendación Primera, será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

En este sentido, cuando los datos personales recabados a través de Internet vayan a ser comunicados a otras compañías (incluso cuando éstas pertenezcan al mismo grupo empresarial) deberá informarse al usuario, de tal forma que éste pueda conocer explícitamente las finalidades determinadas a las que se destinarán los datos. La información podrá referirse genéricamente a un sector de actividad económica (por ejemplo, servicios financieros,...), sin que puedan admitirse finalidades indeterminadas o no comprensibles para el usuario (por ejemplo, actividad comercial, actividad publicitaria, empresas del grupo,...).

Cuando una compañía transfiere a otra la titularidad de un servicio prestado a través de Internet y esta acción lleva asociado un cambio respecto del responsable del fichero que contiene los datos personales de los usuarios de ese servicio, tal acción puede comportar una cesión de datos. En este caso deberán observarse las previsiones legales y, en especial, la previa obtención del consentimiento de los usuarios, salvo que sea aplicable una excepción al mismo.

En el caso de que tal acción no comporte una cesión de datos, el nuevo responsable deberá informar convenientemente a los usuarios de modo expreso, preciso e inequívoco de su propia identidad y dirección, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. En este caso, tales datos sólo podrán ser utilizados por el nuevo responsable con las finalidades determinadas, explícitas y legítimas para las que hubieran sido obtenidos por el anterior responsable.

Los usuarios serán convenientemente informados en los casos en los que sus datos vayan a ser comunicados a los responsables de otras webs que pudieran estar vinculadas (por ejemplo, mediante un hiperenlace) con la web a través de la cual son recogidos, siempre y cuando la comunicación se realice en los términos expresados por el apartado 1 de la presente Recomendación. En tales casos, se especificará claramente qué datos serán comunicados, así como la identidad y dirección de los cesionarios.

Recomendación Octava: Movimiento internacional de datos

De conformidad con lo establecido por el artículo 33 de la LOPD, no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la Ley Orgánica, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos.

A este respecto, se tendrán en cuenta las excepciones previstas en el artículo 34 de la LOPD:

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

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

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

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

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

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

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

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

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

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

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.1

En particular, cuando sea de aplicación la legislación española sobre protección de datos, conforme al artículo 2.1 de la LOPD, y además el fichero que contiene los datos personales recabados a través de Internet se halle ubicado en el territorio de un Estado no miembro de la Unión Europea o respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, será precisa la autorización previa del Director de la Agencia de Protección de Datos, a menos que la transferencia internacional se fundamente en alguno de las excepciones comprendidas en los apartados a) a j) del artículo 34 de la LOPD antes citados. En todo caso, la transferencia internacional se deberá notificar a la Agencia de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

De acuerdo con lo que establece el artículo 5 de la LOPD y se recoge en la Norma Segunda de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.

El deber de información a que se refiere el apartado anterior no será de aplicación cuando la transferencia internacional tenga por objeto la prestación de un servicio al responsable del fichero, por parte de un tercero al que se le haya encargado el mismo en los términos establecidos por el artículo 12 de la LOPD.

Con independencia de lo anterior, en el caso de que la transferencia se legitime mediante la obtención del consentimiento inequívoco del afectado, el responsable del fichero se asegurará de que éste ha sido previamente informado de los extremos citados en el apartado 2.

Recomendación Novena: Seguridad de los datos

De acuerdo con lo establecido por el artículo 9 de la LOPD, el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas en el Reglamento de Medidas de Seguridad, aprobado mediante el Real Decreto 994/1999, de 11 de junio, las cuales se clasifican de acuerdo a los niveles de seguridad establecidos en su artículo 4.

Cuando los usuarios registrados en una web tengan acceso on-line a los datos de que dispone el responsable del fichero respecto a su persona, deberán establecerse procedimientos de identificación, autenticación y control de accesos, de acuerdo con lo establecido en el citado Reglamento.

A los ficheros con datos acerca de transacciones de compra de productos o servicios que, mediante un tratamiento de segmentación o categorización, permitan obtener una evaluación de la personalidad del individuo, les será de aplicación, al menos, lo establecido en el apartado 4 del artículo 4 del citado Reglamento, es decir, en tal caso deberán de garantizarse las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20 del mismo.

Se considera una buena práctica la adopción de medidas que eviten que la información circule por la red de forma inteligible y, por tanto, susceptible de ser conocida o manipulada por terceros. Del mismo modo, se considera buen práctica proporcionar al usuario información acerca del nivel de protección que proporciona la tecnología utilizada.

2.1.3. Recomendaciones para la Gestión de Tarjetas en Grandes Superficies Comerciales.

En el año 2000 se llevó a cabo una inspección de oficio al sector de la Gestión de Tarjetas en Grandes Superficies Comerciales. En la Memoria correspondiente a dicho año ya se citaban las conclusiones más relevantes de dicha inspección. Como consecuencia de las conclusiones alcanzadas, en el año 2001 el Director de la Agencia de Protección de Datos dictó unas Recomendaciones a dicho sector que se transcriben a continuación

Recomendación Primera: Derecho de información en la recogida de datos

Con carácter general se ha detectado que las entidades inspeccionadas cumplen las prescripciones previstas en el art. 5 L.O.P.D., en tanto en cuanto se informa de la existencia del fichero y finalidad de la recogida, obligatoriedad de facilitar los datos, posibilidad de ejercicio de los derechos que al afectado reconoce la ley y comunicación de datos a efectuar.

Sin embargo, se ha observado que en algunas ocasiones el personal del centro comercial recaba los datos directamente del solicitante de la tarjeta cumplimentando un formulario de uso interno que no facilita al interesado. En estos casos, cuando los formularios para la recogida de los datos no sean cumplimentados directamente por el interesado, deberán adoptarse las medidas pertinentes para asegurar que el personal del centro que proceda a la recepción de los datos facilite la información a la que se refiere el citado art. 5.1 de la L.O.P.D. por ser de obligada comunicación por el responsable del fichero, toda vez que el desconocimiento de esos datos básicos supone una clara indefensión para el cliente que le imposibilita el ejercicio de los derechos de acceso, rectificación, cancelación y oposición reconocidos por la Ley.

Recomendación Segunda: Consentimiento del afectado en el tratamiento de sus datos personales

De acuerdo con lo dispuesto en el apartado 1 del artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

Ciertamente, la Ley permite que en la mayoría de los casos el consentimiento se preste de forma "tácita". Sin embargo, en los supuestos aquí analizados, dada la trascendencia de las relaciones negociales o contractuales que se van a derivar, se considera una buena práctica que el afectado suscriba con su firma los formularios y solicitudes de contratos de tarjetas, como muestra de que consiente el tratamiento de sus datos personales en los mismos términos en los que se le informa en dichos formularios o contratos.

En particular, vistos los tratamientos que realizan los establecimientos financieros de crédito sobre los datos de los solicitantes de tarjetas y clientes, deberá prestarse especial atención en recabar el consentimiento para la valoración del riesgo crediticio de los datos personales aportados por los afectados en su solicitud de obtención de tarjeta, informando, en su caso, de que dicha valoración estará apoyada por la utilización de un sistema automático. En ningún caso podrá realizarse tal valoración si no se cuenta para ello con el consentimiento informado del interesado.

Además, y puesto que en algunos casos no se informa al interesado de que su solicitud de tarjeta le ha sido denegada, deberá tenerse en cuenta que de conformidad con el art. 13.2 L.O.P.D., el afectado podrá impugnar decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. Por ello, en el caso de que un establecimiento financiero de crédito deniegue una solicitud de las tarjetas que emita y, con el fin de permitir al interesado el recurso de dicha decisión, debería informarle de dicha denegación y de las razones que la hayan motivado

En relación a los clubes de fidelización promovidos por los centros comerciales y teniendo en cuenta los tratamientos que realizan sobre los datos de sus socios, deberá recabarse su consentimiento autorizando que se puedan realizar con sus datos estudios de mercado o elaboración de perfiles, a utilizar por el centro para campañas de promoción y lanzamiento de productos, salvo que tales estudios se realicen disociando los datos de los afectado.

Recomendación Tercera: Calidad de datos

El art. 4.2 L.O.P.D. dispone que *"los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos....."*

El envío de publicidad que realizan tanto los centros comerciales como los establecimientos financieros emisores de tarjetas, es, en principio, ajeno a la relación negocial o contractual existente entre las citadas entidades y los clientes. Por tanto, y a fin de evitar posibles infracciones del principio de calidad de datos consagrado en el artículo transcrito, desviando la finalidad para la que los datos fueron recabados, deberá obtenerse el consentimiento de los clientes para enviar publicidad personalizada de productos de terceras entidades.

Recomendación Cuarta: Cancelación de datos

Se ha comprobado que, en general, las entidades cancelan periódicamente de sus ficheros los datos personales de las solicitudes de tarjetas que fueron denegadas, aunque en un caso se comprobó que la entidad aún mantenía en sus ficheros gran número de solicitudes denegadas varios años atrás.

En este sentido, la Ley Orgánica 15/1999, en el artículo 4.5 bajo el epígrafe "calidad de datos", consagra el principio de conservación limitada de los datos al disponer: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados*" .

Por otra parte, los apartados 3 y 5 del artículo 16 de la citada Ley especifican: "*La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".*

Por ello, en virtud de las prescripciones legales transcritas, todas las entidades afectadas deberán proceder al bloqueo de todos aquellos datos de carácter personal incluidos en sus sistemas de información que hayan dejado de ser necesarios al fin para el que fueron recabados o registrados y proceder a su cancelación definitiva una vez cumplidos los plazos de prescripción derivados de las obligaciones o responsabilidades nacidas del tratamiento. El bloqueo sólo permitirá el tratamiento de tales datos para la finalidad que lo justifique. Por excepción, se podrán mantener determinados datos por interés histórico, estadístico o científico, de acuerdo con su legislación específica.

Recomendación Quinta: Comunicación de datos

De acuerdo a lo establecido en el artículo 11.1 de la L.O.P.D., *"los datos de carácter personal objeto de tratamiento sólo podrán se comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"*. El consentimiento no será preciso, entre otros, cuando la cesión está autorizada en una Ley o si la comunicación se efectúa previo procedimiento de disociación.

En consecuencia, cuando las entidades a las que afecta esta recomendación comuniquen o cedan los datos personales recabados de sus clientes a otras empresas del Grupo de sociedades al que pertenezca el establecimiento financiero o centro comercial, deberán cumplir acumulativamente las dos condiciones impuestas por el transcrito art. 11.1. Además, la finalidad de la cesión ha de ser cognoscible para el interesado en el momento de prestar el consentimiento, no siendo lícito el mero consentimiento genérico para ceder sus datos conforme a expresiones tales como "ceder sus datos a otras empresas del grupo", "realizar publicidad", "remitirle ofertas comerciales".....

En definitiva, el consentimiento ha de otorgarse para supuestos y finalidades concretas y determinadas, siendo nulo de pleno derecho, de conformidad con lo dispuesto en el art. 11.3 de la misma Ley, el consentimiento para la cesión absoluta o indeterminada.

Recomendación Sexta: Derechos de acceso, rectificación, cancelación y oposición.

De conformidad con lo dispuesto en los artículos 15 y concordantes de la Ley Orgánica 15/1999, los derechos de acceso, rectificación, cancelación y oposición de los datos de carácter personal contenidos en ficheros automatizados, se configuran como uno de los ejes fundamentales sobre los que se articula la protección de los datos de ciudadanos, y aparecen regulados, además, en el Real Decreto 1332/1999 y en la Instrucción 1/1998 de la Agencia de Protección de Datos. Los derechos de acceso, así como los de rectificación, cancelación y oposición de datos son derechos personalísimos y los responsables de los ficheros, resolverán sobre la solicitud en los plazos establecidos por la ley. En el supuesto de que el responsable considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente en el plazo legalmente establecido. Si no fuere debidamente atendido, el afectado podrá reclamar ante la Agencia de Protección de Datos.

La norma Primera de la Instrucción 1/1998, establece los requisitos generales a cumplir tanto por el ciudadano en la solicitud del ejercicio de los derechos como por parte del responsable del fichero con objeto de resolver sobre la solicitud. A tal efecto, el apartado 5 de la citada norma dispone "*El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos".*

Se ha detectado en la inspección practicada a los centros comerciales que es muy frecuente que el cliente se limite a solicitar la rectificación de sus datos personales (v. gr.: cambio de domicilio) personándose en el centro o incluso por teléfono (a lo que accede el personal del centro), pero sin que tal rectificación pueda considerarse "formalmente" como el derecho reconocido como tal en la L.O.P.D. Obviamente, no es competencia ni voluntad de esta Agencia regular el ejercicio de prácticas comerciales o relaciones negociales entre proveedor y cliente, pero sí entiende que a fin de dar una mejor respuesta a los ciudadanos en el ejercicio de sus derechos, sería conveniente que los responsables de los ficheros establecieran un procedimiento documentado con objeto de su conocimiento y cumplimiento por parte de todas las personas que integran la organización.

De otro lado, el artículo 6.4 de la L.O.P.D. establece que, "*En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste*

podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal". En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado cuando se den todas las circunstancias previstas en la norma transcrita.

Recomendación Séptima: Acceso a los datos por cuenta de terceros.

Todos los centros comerciales y entidades financieras tienen contratado con terceros la prestación de determinados servicios , lo que supone la entrega de soportes informáticos conteniendo datos personales.

De conformidad con lo dispuesto en el artículo 12.2 de la L.O.P.D., "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará ni siquiera para su conservación, a otras personas. En el contrato se estipularán, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".* De otro lado, la L.O.P.D., establece las medidas de seguridad que deberán de cumplir los ficheros automatizados que contengan datos de carácter personal, tanto por el responsable del fichero como por el encargado del tratamiento.

Por todo ello, con objeto de conseguir una mejor adecuación de los tratamientos automatizados a los principios de la normativa de protección de datos, los responsables de los ficheros deberán estipular las medidas de seguridad que el "encargado" del tratamiento está obligado a implementar, así como efectuar los controles necesarios con objeto de verificar de forma periódica el cumplimiento de las mismas.

Con base en estas consideraciones legales, que en cualquier caso siempre deberán ser tenidas en cuenta por los responsables de los ficheros, en la inspección practicada se han observado tres particularidades que deberán ser corregidas:

En un caso, el contrato de prestación de servicios ha sido firmado o celebrado por la matriz del Grupo al que pertenece el establecimiento financiero de referencia y el encargado del tratamiento. Pues bien, en todo caso el contrato de prestación de servicios deberá concluirse entre el responsable del fichero y el encargado del tratamiento, sin que pueda ser suscrito por otras empresas del Grupo de sociedades al que pertenezca dicho responsable.

El supuesto de subcontratación de prestación de servicios detectado en una de las entidades inspeccionadas no podrá llevarse a cabo a tenor de lo dispuesto en el art. 12.2 *in fine* L.O.P.D., que prohibe al "encargado" del tratamiento (prestador del servicio) ceder los datos obtenidos del "responsable" del fichero, cuando dice *"ni los comunicará ni siquiera para su conservación, a otras persona"*. La Ley impone, pues, una limitación a la subcontratación que impide la celebración del contrato aquí referido. No obstante, el encargado del tratamiento podrá celebrar estos contratos siempre y cuando actúe en nombre y por cuenta del responsable del fichero.

Finalmente, en el caso de acceso a los datos del cliente de los establecimientos financieros, realizado por el personal de los centros comerciales que presta servicios de atención al cliente, dicho acceso no podrá realizarse salvo que exista previa solicitud del interesado y esté amparado en el mantenimiento o cumplimiento de una relación contractual o esté regulada en un contrato de prestación de servicios.

Recomendación Octava: Notificación e inscripción registral.

La creación de ficheros de datos de carácter personal deberá ser notificada previamente a la Agencia de Protección de Datos, cumplimentando el formulario establecido al efecto en la Resolución del Director la Agencia, de 30 de mayo de 2000 (BOE nº 153, de 27 de junio de 2000), por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático, a través de los que deberán efectuarse las correspondientes solicitudes de inscripción en el Registro General de Protección de Datos, los cuales también pueden obtenerse a través de Internet en la página: www.agenciaprotecciondatos.org.

Los ficheros que recogen los datos de las operaciones efectuadas por los clientes en los centros comerciales utilizando tarjetas de pago, cuyos responsables son los propios centros, y que contengan cualquier información concerniente a personas físicas identificadas o identificables, como es el número de la tarjeta con la que se ha realizado la operación, son considerados ficheros con datos de carácter personal en los términos establecidos en la LOPD, siéndoles de aplicación todo lo dispuesto en la misma; por ello, la creación de estos ficheros deberá ser notificada a la Agencia.

Recomendación Novena: Seguridad de los datos.

La Ley Orgánica 15/1999, en su artículo 9 dispone que "*el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria".*

El Real Decreto 994/1999, aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que se clasifican en tres niveles atendiendo a la naturaleza de la información tratada y la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

En particular, los establecimientos financieros de crédito, al contener en sus ficheros datos de servicios financieros, deberán cumplir al menos las medidas de nivel básico y medio que en el citado Reglamento se establecen, de conformidad con lo previsto en su art. 4.2. Las mismas medidas deberán cumplir los ficheros de los que son responsables los centros comerciales cuando prestan servicios financieros.

En el supuesto en que, siendo de aplicación lo previsto en el art. 18.1 del Reglamento, se hayan creado usuarios genéricos que permitan el acceso a la información el responsable del fichero deberá establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. De esta forma, los establecimientos financieros de crédito deberán adoptar las medidas oportunas, para garantizar que se otorga un código de usuario único a cada una de las personas que accedan a sus ficheros, aun en el caso de que las mismas presten sus servicios en los centros comerciales, no siendo en ningún caso válidas las asignaciones genéricas de usuarios.

2.1.4. Recomendaciones a Operadores de telefonía móvil

* Introducción

Por acuerdo del Director de la Agencia de Protección de Datos (APD), se procedió durante el año 2000 a realizar un Plan de Inspección de oficio al sector de los Operadores de Telefonía Móvil con objeto de comprobar el grado de adecuación de los ficheros automatizados de las entidades del sector a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal, Ley 15/1999, de 13 de diciembre (LOPD) y normativa que la desarrolla, así como su adecuación a lo dispuesto en el Titulo V del Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento que desarrolla el Título III de la Ley General de Telecomunicaciones en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de Telecomunicaciones y por el que también se transponen las previsiones de la Directiva 97/66/CE, de 15 de diciembre, relativa a la protección de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

En la memoria del ejercicio de 2000 ya se informó acerca del objetivo y alcance de dicho plan y se describieron, de forma general, los principales tratamientos de datos personales de clientes realizados por los tres operadores que proporcionan servicio en la actualidad: TELEFÓNICA MÓVILES ESPAÑA, S.A., (bajo las denominaciones MOVISTAR y MOVILINE), AIRTEL MÓVIL, S.A. (bajo la anterior denominación AIRTEL, actualmente VODAFONE) y RETEVISÓN MÓVIL, S.A. (bajo la denominación AMENA).

Corresponde en la presente memoria exponer las conclusiones generales obtenidas de dichas inspecciones, así como el resultado derivado de las mismas y que ha llevado a formular recomendaciones a uno de los operadores y a realizar nuevas actuaciones respecto de los otros dos. Como consecuencia de estas últimas actuaciones se han iniciado dos procedimientos sancionadores, circunstancia que ha retrasado la elaboración de las correspondientes recomendaciones.

Finalmente, quiere puntualizarse que tanto en las conclusiones como en las recomendaciones que figuran a continuación no se expone un alto nivel de detalle, toda vez que, en otro caso, quedarían al descubierto datos relativos al modo de operar de las compañías, así como otros aspectos, que pudieran comprometer materias protegidas por el secreto comercial o industrial, por lo que, en aplicación de lo dispuesto en el artículo 37.5 d) de la Ley 30/1992, no ha parecido conveniente hacer público ningún dato que pudiera perjudicar a las compañías inspeccionadas en beneficio de las competidoras o de terceros.

* Conclusiones respecto de la Ley Orgánica 15/1999.

Las conclusiones relativas a los ficheros de clientes son las siguientes:

Origen de la información.

La datos personales de clientes tratados por los operadores de telefonía móvil en sus sistemas de información proceden de diversas fuentes:

* Información facilitada por el propio cliente. Mediante formularios y contratos establecidos al efecto se recaban datos básicos del cliente entre los que se encuentran sus datos identificativos, datos de domicilio y datos bancarios para el pago de los servicios.

* Información generada por la red de telefonía móvil. En este caso, los datos obtenidos se corresponden con la información sobre tráfico y facturación de las llamadas en las que interviene el cliente.

* Información que sobre el cliente se obtiene de ficheros comunes externos de incumplimiento de obligaciones dinerarias.

* Información relativa al comportamiento de pago de las facturas generadas al cliente.

* Información recabada mediante formularios-encuestas que voluntariamente remiten los clientes a los operadores.

* Otras informaciones procedentes de terceros.

Calidad de datos (artículo 4).

Respecto de la finalidad de los tratamientos:

De la información recabada de los ficheros de gestión de clientes se desprende que los datos personales tratados en cada uno de ellos son, en general, adecuados, pertinentes y no excesivos con las correspondientes finalidades.

Especial atención merece los ficheros de *DataWarehouse* que poseen las tres entidades dada la amplia estructura de datos que contiene y la diversidad de finalidades que en ellos concurren. Estos ficheros se constituyen como un almacén de datos corporativo en el que se recogen datos de los clientes (datos identificativos, datos de tráfico y de facturación, etc.) procedentes de otros ficheros con finalidades específicas (facturación, gestión de red, etc.), así como otras informaciones. Sobre estos ficheros se realizan, en general, tratamientos de diversa índole, entre los que se incluyen los realizados con fines de promoción comercial de los productos de los propios operadores.

Las finalidades de estos ficheros son diversas e incluyen:

* Soporte para la definición de estrategias y toma de decisiones, que se realiza mediante el análisis de información agregada.

* Actividades operativas de marketing para acciones publicitarias propias

* Gestión del negocio:

- Análisis sobre la evolución del negocio.

- Análisis de tarifas.

- Diseños de productos y servicios.

- Planificación de la red de telecomunicaciones.

- Análisis de previsión de demanda.

- Informes de gestión.

- Estudios de rentabilidad.

- Cumplimiento de obligaciones legales, donde se incluyen los requerimientos efectuados por autoridades públicas.

Respecto de la exactitud de los datos:

En la mayoría de los casos, los datos de los clientes son exactos y se encuentran actualizados.

No obstante, y como se detalla más adelante, en las actuaciones practicadas en dos de los operadores se han apreciado indicios de infracción que han dado lugar a la apertura de los correspondientes procedimientos sancionadores.

Respecto de la cancelaciones de datos:

En general, no existen procedimientos formalmente establecidos para la realización de las bajas en sus ficheros.

Derecho de información en la recogida de datos (artículo 5).

Los tres operadores incluyen cláusulas informativas en los contratos de prestación de servicios cuyo contenido recoge la existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de dicho tratamiento, la identidad y dirección del responsable y la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

No obstante, como se detalla más adelante, de las actuaciones practicadas en relación con la información facilitada por un operador a sus clientes se ha derivado la apertura de un procedimiento sancionador a uno de los operadores.

Consentimiento del afectado para el tratamiento (artículo 6).

Los tratamientos detectados cuentan, en términos generales, con el consentimiento de los afectados recabado mediante las correspondientes cláusulas informativas incorporadas en el contrato de adhesión al servicio.

No obstante, también en este ámbito se han apreciado indicios de infracción que han dado lugar a la apertura de un procedimiento sancionador por dos infracciones diferentes a un mismo operador.

Datos especialmente protegidos (artículos 7 y 8).

No se ha detectado datos especialmente protegidos en los ficheros de clientes.

Seguridad de los datos (artículo 9 y RD 994/1999)

Los tres operadores cuentan con diversa documentación relativa a la seguridad en sus ficheros, entre la que se encuentran los documentos de seguridad exigidos de forma explícita en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

En relación a los documentos de seguridad se han formulado una serie de recomendaciones a uno de los operadores, ya que se habían detectado algunos aspectos de carácter formal en los mismos que deberían ser mejorados y que no afectaban a la seguridad de los sistemas.

Deber de secreto (artículo 10).

Los tres operadores cuentan con contratos laborales que recogen cláusulas que obligan a sus empleados a guardar el deber de secreto respecto de los datos personales a los que tengan acceso como consecuencia de su labor.

De forma adicional, en los contratos de prestación de servicios en los que los operadores comunican a terceros datos de carácter personal de sus clientes se recogen cláusulas que obligan a las empresas prestatarias a mantener la confidencialidad sobre los datos personales que le son comunicados en virtud de la prestación.

Cesiones de datos (artículo 11).

Generalmente, los operadores informan a sus clientes de la posibilidad de ceder datos a empresas del grupo al que pertenecen o a aquellas con las que tengan una vinculación accionarial o de participación. En este sentido, en el caso de uno de los operadores se ha formulado una recomendación al considerar que la cláusula utilizada no es conforme a la LOPD. Sin embargo, como no se han llegado a efectuar tales cesiones no se ha iniciado procedimiento sancionador.

Acceso a los datos por cuenta de terceros (artículo 12).

Los tres operadores tienen contratadas con terceras empresas prestaciones de servicios que implican el acceso por parte de éstas a datos personales de sus clientes.

Habitualmente, todas estas prestaciones de servicios se encuentran plasmadas en contratos por escrito que recogen la finalidad de la prestación, así como cláusulas de confidencialidad respecto de los datos personales a los que se tiene acceso y el deber de mantener las medidas de seguridad legalmente exigidas. También se recoge en estos contratos la obligación de devolver o destruir la información una vez que la prestación haya finalizado.

En este sentido, se han formulado recomendaciones a uno de los operadores por apreciarse algunas deficiencias formales en los contratos de prestaciones de servicios elaborados al efecto.

Impugnación de valoraciones (artículo 13).

No se ha detectado en ninguno de los operadores que se tomen decisiones con efectos jurídicos que afecten a personas físicas y que tengan como fundamento únicamente un tratamiento de datos destinado a evaluar determinados aspectos de la personalidad del individuo.

Derecho de las personas: acceso, rectificación, cancelación y oposición. (artículos 15 y 16).

Los tres operadores cuentan con procedimientos para atender las solicitudes de ejercicio de los derechos reconocidos por la normativa de protección de datos sin que se hayan detectado deficiencias en los mismos.

Las entidades inspeccionadas informan a los usuarios de la posibilidad de ejercer estos derechos al tiempo que cuentan con procedimientos definidos para su ejercicio, siendo habitual que dichos procedimientos recojan lo dispuesto en la Instrucción 1/1998 de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Creación, notificación e inscripción en el Registro de la APD (artículos 25 y 26).

Las entidades analizadas han procedido a la inscripción en el Registro General Protección de Datos de la APD de sus ficheros de clientes y potenciales clientes.

Datos incluidos en fuentes accesibles al público (artículo 28).

Ninguno de los operadores publica ningún repertorio de clientes susceptible de considerarse fuente accesible al público. Tampoco utiliza ningún fichero con datos personales que procedan de fuentes accesibles al público.

Prestación de servicios de información sobre solvencia patrimonial y crédito (artículo 29).

Para la gestión de sus clientes, los tres operadores realizan tratamientos de datos relativos a incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. Dichos tratamientos son realizados tanto en la modalidad de consulta (acceso a posibles deudas del cliente con terceros) como de actualización (comunicación a terceros de las deudas del cliente con el operador).

El tratamiento realizado en modo consulta es utilizado por los tres operadores durante la tramitación del alta como cliente y en ocasiones, cuando se produce la contratación por parte de un cliente de determinados productos o servicios adicionales. Este tratamiento se encuadra dentro de un procedimiento de valoración o *scoring* cuya finalidad es la de comprobar la solvencia económica del cliente y evaluar el nivel de riesgo de impago. En este sentido, la normativa general de telecomunicaciones permite a los operadores condicionar la prestación de determinados servicios al depósito de una fianza, por lo que se utiliza a tal efecto el resultado del *scoring.*

En relación con lo anterior, se han detectado posibles infracciones en dos operadores, lo que ha dado lugar a la apertura de procedimientos sancionadores.

Tratamientos con fines de publicidad y de prospección comercial (artículo 30).

Los tres operadores realizan únicamente tratamientos de datos personales con fines de publicidad y prospección comercial sobre clientes. No se ha detectado la realización de campañas publicitarias personalizadas para captar nuevos clientes, utilizándose para ello campañas comerciales convencionales a través de medios de comunicación.

No se han detectado tratamientos con fines comerciales sobre clientes que se hayan opuesto a dicho tratamiento.

Movimiento internacional de datos: Norma general y Excepciones (artículos 33 y 34).

Los tres operadores realizan movimientos internacionales de determinados datos de sus abonados en dos situaciones distintas:

1. En las llamadas que los abonados realizan fuera de España, ya que puede comunicarse el número llamante al operador de la interconexión.

2. En la compensación entre operadores que se realiza con el fin de facturar las llamadas internacionales en los servicios de itinerancia o *roaming*. En este caso, la transferencia internacional es necesaria para la facturación de la llamada y por lo tanto para la ejecución del contrato entre el abonado y el operador.

* Conclusiones respecto del Título V del Real Decreto 1736/1998.

Respecto de los tratamientos de datos personales sobre tráfico y facturación (Artículo 65).

De las actuaciones practicadas se deriva, en principio, que los tres operadores realizan tratamientos de los datos de tráfico y facturación con fines comerciales propios. No obstante, únicamente dos de ellos informan a sus clientes acerca de la realización de dichos tratamientos.

En este sentido, se ha formulado una recomendación a uno de los operadores informantes para que incorpore un procedimiento que permita expresar al cliente la oposición a dicho tratamiento, como por ejemplo la inclusión de una casilla al efecto.

Respecto del operador que no informa acerca de dicho tratamiento se ha procedido a la apertura de un procedimiento sancionador, que se detalla más adelante, por posible infracción del artículo 6 de la LOPD, en relación con el artículo 65.3 del Real Decreto 1736/1998.

Respecto de la Protección de los datos personales en la facturación detallada (artículo 66).

No consta que el órgano competente de la Administración haya publicado aún la Resolución que determine las diferentes modalidades de facturación detallada que los abonados puedan solicitar a los operadores.

Respecto de las Guías de servicios de telecomunicaciones disponibles al público (Artículo 67).

No consta que el órgano competente de la Administración haya publicado ninguna Orden en la que se determinen las condiciones para hacer constar los datos personales en las guías de abonados.

Respecto de las llamadas no solicitadas con fines de venta directa (artículo 68).

Los tres operadores afirman no realizar campañas de venta directa mediante sistemas de llamada automática sin

intervención humana, ni faxes, ni para ofrecer productos propios ni de terceros.

No obstante, uno de los operadores sí reconoce realizar promociones de servicios de valor añadido sobre el servicio de mensajes cortos o SMS (estado de carreteras, información meteorológica, servicio multiasistencia, etc.). Dichas promociones se realizan enviando mensajes cortos en los que se informa a los clientes de la posibilidad de utilizar dichos servicios de forma gratuita durante un tiempo o un número de veces. Estos mensajes son remitidos mediante un procedimiento automático sin intervención humana. En este sentido se ha formulado una recomendación al citado operador.

Respecto de los servicios de identificación y restricción de la línea llamante y conectada (artículos 69, 70, 71, 73, 74, 75, 76, 77 y 79).

No consta que el órgano competente de la Administración haya establecido el calendario para el cumplimiento de la obligación recogida en el artículo 74 respecto al filtrado en destino de llamadas sin identificación.

No consta que el órgano competente de la Administración haya publicado una resolución por la que se apruebe la aplicación del mecanismo de eliminación de marcas de supresión en origen de la identificación de la línea llamante en relación con los servicios de urgencia (artículo 75).

No consta que el órgano competente de la Administración haya establecido los destinos que no dispongan de la facilidad de identificación de la línea llamante (artículo 76).

No consta que el órgano competente de la Administración haya publicado relación alguna de países a los que puede ser enviada la información sobre identidad de la línea llamante o conectada (artículo 79).

* Recomendaciones efectuadas.

De las conclusiones obtenidas en el análisis de los tratamientos realizados por uno de los operadores no se han encontrado aspectos que supongan infracciones a la normativa de protección de datos. No obstante, al objeto de adecuar plenamente los tratamientos automatizados que realiza el operador a los principios de la normativa vigente en materia de protección de datos de carácter personal y en virtud de las potestades otorgadas por el artículo 5 c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, se han formulado una serie de recomendaciones de las que se ha dado traslado al operador afectado. A continuación se recoge un resumen de las mismas:

* En relación a los artículos 6 de la LOPD y 65 del Real Decreto 1736/1998.

Dado que se ha detectado la posibilidad en el sistema *DataWarehouse* del operador de realizar tratamientos de datos de tráfico sobre un conjunto de datos más amplio que el contemplado en el artículo 65 del Real Decreto 1736/1998, se ha recomendado que se realice una adecuada delimitación de las funciones del personal con acceso al sistema y la correspondiente segregación de tipologías de datos, estableciendo los controles pertinentes de forma que los accesos que se realicen resulten adecuados a las funciones encomendadas. Así mismo, se ha recomendado disociar los datos en todos los tratamientos en los que no sea necesario identificar al cliente.

Por otra parte, se ha recomendado también la inclusión en el propio contrato de un procedimiento que permita expresar la oposición, en el momento de la contratación, al tratamiento de los datos de tráfico y facturación con fines de promoción comercial.

* En relación con la Seguridad de los Datos Personales. (artículo 9 de la LOPD y RD 994/1999)

La Ley Orgánica 15/1999, en su artículo 9 dispone que "El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."

El Real Decreto 994/1999, de 11 de junio de 1999, aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, que se clasifican en tres niveles atendiendo a la naturaleza de la información tratada.

En este sentido, el operador dispone de documentos de seguridad correspondientes a cada tipo de fichero. No obstante, se han detectado en algunos de los documentos de seguridad una serie de deficiencias formales relacionadas con los procedimientos de recuperación de datos, la definición de registros de incidencias, los procedimientos asociados a la gestión de soportes así como de otros aspectos. Dado que ninguna de las deficiencias encontradas compromete la seguridad de los sistemas, se han elaborado una serie de recomendaciones para su subsanación.

* En relación con la cesiones de datos (artículo 11 de la LOPD).

La Ley Orgánica 15/1999, en su artículo 11.1 establece que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legí-

timas del cedente y del cesionario con el previo consentimiento del interesado".

Respecto del consentimiento, el artículo 11.3 de la misma Ley puntualiza que "Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar".

Con el fin de poder realizar cesiones, el operador informa a través de una cláusula recogida en los contratos de adhesión al servicio de posibles cesiones de datos personales de clientes a empresas del grupo al que pertenece el operador, para la posterior remisión de ofertas de los servicios que puedan ser de interés del cliente.

En relación con dicha cláusula la Agencia ha considerado que su redacción actual resultaría insuficiente ya que no permite conocer la finalidad a que se destinarán los datos cedidos o el tipo de actividad de aquel a quien se pretenden comunicar, por lo que dicho consentimiento sería nulo a tenor de lo recogido en el artículo 11.3 de la LOPD.

Dado que no se han detectado cesiones de datos de clientes a empresas del grupo se ha recomendado que, en caso de que se prevea su realización, se recabe con carácter previo a la cesión el correspondiente consentimiento en los términos establecidos en la Ley.

* En relación con el acceso a los datos por cuenta de terceros (artículo 12 de la LOPD).

El operador tiene contratado con terceros la prestación de servicios informáticos que conlleva el acceso a determinados ficheros por parte de terceras empresas.

En este sentido, el artículo 12 de la LOPD, en sus apartados segundo y tercero, establece que: *"2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento."*

En general, las prestaciones de servicios analizadas se encuentran plasmadas en contratos por escrito que recogen la finalidad de la prestación, así como cláusulas de confidencialidad respecto de los datos personales a los que se tiene acceso y el deber de mantener las medidas de seguridad legalmente exigidas. También se recoge en estos contratos la obligación de devolver o destruir la información una vez que la prestación haya finalizado.

No obstante, se han detectado ciertas deficiencias formales en algunos de los contratos analizados que tienen que ver con la ausencia, en algunos de ellos, de cláusulas relativas a determinados aspectos del artículo 12.

En relación a lo anterior, se ha recomendado que en las prestaciones de servicios que tengan por objeto la realización de un tratamiento de datos por parte de un tercero el operador tenga en cuenta, como responsable del fichero, los siguientes aspectos con objeto de adecuar los contratos de prestación de servicios establecido con terceros a lo previsto en el artículo 12 de la LOPD:

* La prestación habrá de plasmarse en un contrato, que deberá constar por escrito, y que establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normativa española de protección de datos.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento

* La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.

* En relación al artículo 68 del Real Decreto 1736/1998.

Si bien el operador afirma no realizar campañas de venta directa mediante sistemas de llamada automática sin intervención humana, ni faxes, ni para ofrecer productos propios ni de terceros, lo cierto es que sí ha reconocido realizar promociones de servicios de valor añadido sobre el servicio de mensajes cortos o SMS (estado de carreteras, información meteorológica, servicio multiasistencia, etc.). Dichas promociones se realizan enviando mensajes cortos, mediante un procedimiento automático sin intervención humana, en los que se informa a los clientes de la posibilidad de utilizar

dichos servicios de forma gratuita durante un tiempo o un determinado número de veces.

En base a lo anterior se ha recomendado al operador que informe al menos a sus clientes a la hora de remitirles los citados mensajes SMS de la posibilidad de oponerse a la recepción de dichos mensajes.

Procedimientos sancionadores derivados de las actuaciones de oficio.

Como ya se ha mencionado, las actuaciones practicadas a los tres operadores han derivado en las recomendaciones ya descritas a uno de ellos, al entender que, no existiendo infracciones a la normativa de protección de datos, resultaba conveniente adecuar determinados aspectos puntuales a la citada normativa.

Por el contrario, respecto de los otros dos operadores y una vez fue analizada en el presente ejercicio toda la documentación recabada en las actuaciones realizadas durante el ejercicio de 2000, se apreciaron indicios de tratamientos que pudieran ser contrarios a la normativa de protección de datos. Esta circunstancia llevó a que se iniciaran nuevas actuaciones, con el fin de recabar información acerca del detalle de los tratamientos en cuestión.

De la nuevas actuaciones practicadas frente a los dos operadores se han apreciado, en ambos casos, que algunos de los tratamientos podrían vulnerar la normativa de protección de datos por lo que se ha procedido a la apertura de dos procedimientos sancionadores, uno a cada operador.

A continuación se recogen los aspectos básicos que han dado lugar a la apertura de los citados procedimientos sancionadores. De su conclusión se informará en la próxima memoria.

* En las actuaciones practicadas en dos de los operadores se constató que en la tramitación del alta como cliente se realiza un procedimiento de valoración o *scoring* con el fin de comprobar su solvencia económica y evaluar el nivel de riesgo de impago de dicho cliente. Dentro de este proceso de evaluación se realiza un acceso *on line* a la aplicación de consultas de un fichero común externo sobre incumplimiento de obligaciones dinerarias, registrando y manteniendo en sus propios ficheros los datos obtenidos del citado fichero externo en un momento dado. Este mantenimiento en el tiempo sin que exista un proceso de actualización puede llevar a que no se tenga en cuenta el principio de calidad de datos contemplado en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, por lo que dicha actuación pudiera derivar en una infracción que está tipificada como grave en el artículo 44.3f).

Además del hecho anterior, a uno de los dos operadores se le han imputado otras tres posibles infracciones:

* La primera tiene que ver con el hecho de que el operador comunica periódicamente a empresas de informes comerciales con las que tiene suscritos contratos de prestación de servicios, los datos bancarios de los nuevos clientes que figuran en el contrato, a fin de que confirmen con el banco del cliente si los datos facilitados por éste son correctos. Realizada dicha gestión, ambas empresas remiten al operador un fichero informático que contiene información adicional recabada por la propia empresa prestadora del servicio y para la cual no existe, en principio, consentimiento para su tratamiento. Esta información adicional es incorporada por el operador a su propio sistema informático y puede accederse a ella desde la base de datos que gestiona los datos personales de los clientes.

Este hecho podría suponer una infracción del artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, por el tratamiento de datos de sus clientes sin el consentimiento de estos, tipificada como grave en el artículo 44.3d) de la citada Ley.

* La segunda tiene que ver con la realización de presuntos tratamientos de datos de tráfico y facturación con fines comerciales sin contar para ello con el consentimiento del afectado ya que el operador no informa de la realización de dichos tratamientos.

Este hecho podría suponer una infracción del artículo 6 de la Ley Orgánica 15/1999, por tratamiento automatizado de datos de carácter personal sin consentimiento de los afectados, en relación con el artículo 65.3 del Real Decreto 1736/1998, de 31 de julio, tipificada como grave en el artículo 44.3d) de la Ley Orgánica 15/1999.

* Finalmente, y como tercer hecho, se da la circunstancia de que como resultado de unas actuaciones de inspección de esta Agencia ante dicho operador, se dictó resolución, en la que se recogía que no quedaba claro el carácter obligatorio o facultativo de aportar determinados datos en el contrato de servicio, ya que una cláusula de las condiciones generales de uso del servicio establecía, con carácter facultativo, la recogida de determinados datos personales de un subapartado concreto del contrato, cuando en el formulario de contrato no existía tal subapartado. Esto hecho dio lugar a confusión por recogerse una serie de datos personales que, en principio, pudieran parecer excesivos para la prestación del servicio.

Por otro lado, en las instrucciones dirigidas al distribuidor y facilitadas junto al contrato se indicaba que debían cumplimentarse todos los datos del mismo no figurando ninguna instrucción para que se informara sobre dicho carácter opcional.

Como consecuencia de lo anterior, el Director de la Agencia de Protección de Datos requirió al operador para que subsanara la deficiencias encontradas, dando cuenta a esta Agencia de las acciones emprendidas al efecto.

Durante el transcurso de las presentes actuaciones de oficio se ha constado que las deficiencias referidas anteriormente siguen existiendo, por lo que se ha procedido a la apertura de un procedimiento sancionador ya que pudiera

existir una infracción del artículo 5.1 de la Ley Orgánica 15/1999, tipificada como leve en el artículo 44.2d) de dicha norma.

2.2. Planes sectoriales de Oficio 2001

Se describen, a continuación las actuaciones inspectoras de carácter sectorial realizadas durante el año 2001.

2.2.1. Censos de Población y Viviendas 2001 del Instituto Nacional de Estadística. Recomendaciones.

Entre las actividades desarrolladas por la Agencia de Protección de Datos se encuentra la realización de un Plan de Inspección de Oficio al Proyecto *Censos de Población y Viviendas 2001*, cuya formación corresponde al Instituto Nacional de Estadística según establece el Real Decreto 1336/1999.

El Instituto Nacional de Estadística con la colaboración que pueda requerir de los Ayuntamientos y otros organismos o entidades públicas o privadas realizará los Censos de Población, en los que se incluirán exclusivamente el colectivo de personas que tengan fijada su residencia habitual en España. Este tipo de operaciones censales se deben efectuar cada diez años.

Con respecto a censos anteriores, es necesario subrayar la importante novedad que supone el nuevo sistema de gestión padronal impuesto por la Ley Reguladora de Bases del Régimen Local que otorga al citado Instituto la función de coordinación y depuración de los ficheros padronales y de comunicar a los Ayuntamientos las operaciones necesarias para la exactitud de los mismos.

Por otro lado, el Reglamento de Población y Demarcación Territorial de las Entidades Locales establece un nuevo marco de relación entre Censo de Población y Padrón Municipal de Habitantes, que preserva la tradicional relación de mutuo beneficio entre ambos. Así, el censo se apoyará en los datos padronales, utilizando éstos para mejorar la recogida de la información censal y los padrones también se beneficiarán de la operación censal, al utilizarse su estructura para realizar un contraste de los datos existentes en ellos.

Para dar cumplimiento a lo establecido en el citado Reglamento, en cada vivienda se entregarán, junto con los cuestionarios censales, unas hojas que contendrán preimpresos los datos padronales de las personas residentes en la misma, según la información que contienen los ficheros automatizados de que dispone el Instituto Nacional de Estadística, que son copia literal de los correspondientes ficheros padronales de los Ayuntamientos. Con esta notificación de los datos padronales vigentes, se considera cumplida la obligación establecida en el artículo 69.3 del Reglamento de Población, en virtud del cual todos los vecinos deben tener la oportunidad de conocer la información padronal que les concierne al menos una vez cada cinco años.

En todo caso, la recogida por parte del Instituto Nacional de Estadística de datos padronales, junto a la encuesta del censo, será en nombre y por cuenta de las Corporaciones Locales, dado que sin perjuicio de las funciones de control atribuidas al Instituto, la formación, mantenimiento, revisión y custodia del Padrón Municipal corresponderá a los propios Ayuntamientos, de conformidad con lo establecido en de la Ley de Bases de Régimen Local.

* Legislación aplicable.

Con carácter previo, los preceptos jurídicos aplicables en el ámbito del proyecto *Censos de Población y Viviendas 2001* pueden dividirse en dos grupos dependiendo de las características de la información objeto de tratamiento:

* La información padronal de carácter nominal y con efectos esencialmente administrativos que se encuentra contemplada en la Ley Reguladora de las Bases de Régimen Local que especifica que, *"Los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992"*, en la actualidad Ley Orgánica 15/1999 y, por consiguiente, en la normativa que la desarrolla como el Real Decreto 994/1999, por el que se aprueba el *Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal* .

* La información censal de carácter estadístico que se encuentra regulada por la Ley de la Función Estadística Pública, que establece que la recogida de datos con fines estadísticos se ajustará a los principios de secreto, transparencia, especialidad y proporcionalidad.

Otro aspecto a considerar con respecto a los ficheros estadísticos es que la Agencia de Protección de Datos según establece su Estatuto ejercerá el control de la observancia de lo dispuesto en la Ley de la Función Estadística Pública, y en especial:

* Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censales y otros documentos de recogida de datos con fines estadísticos.

* Dictaminará sobre los procesos de recogida y tratamiento automatizado de los datos personales a efectos estadísticos.

* Informará sobre los proyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley de la Función Estadística Pública.

* Dictaminará sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

* Objetivos.

Con base en las prescripciones legales aplicables a los *Censos de Población y Viviendas 2001*, por parte de la Agencia de Protección de Datos se establecieron en el presente plan de oficio los siguientes objetivos:

* Conocer los Sistemas de Información y los Procedimientos utilizados en el Proyecto.

* Identificar las entidades públicas y privadas participantes en el Proyecto, así como los datos personales de los ciudadanos tratados automatizadamente por cada una de ellas.

* Determinar el grado de cumplimiento y de adecuación del Proyecto a las disposiciones de la Ley Orgánica de Protección de Datos de Carácter Personal y de la normativa que la desarrolla, en lo que respecta a los datos padronales.

* Determinar el grado de cumplimiento y de adecuación del Proyecto a lo establecido en la Ley de la Función Estadística Pública, en lo que respecta a los datos censales.

* Alcance del Plan de Inspección.

Debido a la complejidad y magnitud del Proyecto *Censos de Población y Viviendas 2001*, se ha efectuado una selección inicial de las actividades que, en principio, se consideran de mayor interés por parte de la Agencia de Protección de Datos, en especial las que conllevan un tratamiento automatizado de datos de carácter personal.

Por ello, se ha desarrollado el plan en dos fases que coinciden con las actividades relativas al proyecto de los años 2001 y 2002. Las actuaciones desarrolladas en la primera fase se han circunscrito a los siguientes ámbitos:

* Servicios Centrales del Instituto Nacional de Estadística con objeto de determinar los aspectos generales del Proyecto en relación a los Procedimientos utilizados, Sistemas de Información y Entidades participantes que tratan los datos personales de los ciudadanos. En este ámbito la Inspección de Datos ha realizado actuaciones en las Subdirecciones Generales de Censos y Padrón, Difusión Estadística, Informática Estadística y Recogida de Datos.

* Empresas adjudicatarias de los concursos públicos convocados por el Instituto Nacional de Estadística con objeto de la personalización de la documentación: Cuestionarios Censales, Hoja Padronal y Cuadernos de Recorrido. Éstas prestaciones de servicios junto con la cumplimentación del censo por internet han sido consideradas por parte de la Agencia como las más interesantes del Proyecto desde el punto de vista de protección de datos, ya que, diversas empresas privadas, entre ellas algunas pertenecientes al sector del marketing, han tratado datos personales de millones de ciudadanos.

* Unión Temporal de Empresas adjudicataria de las actividades relativas a la cumplimentación del censo por internet y del Centro de Atención al Usuario, operativos hasta primeros de febrero de 2002.

* Empresa adjudicataria de las tareas relacionadas con el almacenamiento y transporte del material necesario para el desarrollo del Proyecto.

Como resumen de las actuaciones efectuadas durante el presente año podemos destacar, entre otras, que se han realizado investigaciones en trece empresas privadas y en los Servicios Centrales del Instituto Nacional de Estadística, habiéndose levantado un total de quince Actas de Inspección. A lo largo del año 2002 se continuará desarrollando la segunda fase del presente plan.

Del resultado de las actuaciones practicadas hasta la fecha por parte de la Inspección de Datos se observó un adecuado cumplimiento de las prescripciones de la Ley Orgánica 15/1999, si bien, se encontraron algunas deficiencias en relación con las contrataciones efectuadas por el Instituto Nacional de Estadística. Por ello, se procedió por parte del Director de la Agencia de Protección de Datos a dictar las Recomendaciones, que se recogen a continuación.

Recomendaciones de la Agencia de Protección de Datos al Instituto Nacional de Estadística para la adecuación de su funcionamiento a la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

* Introducción.

En virtud de las funciones que la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, otorga a la Agencia de Protección de Datos en el artículo 37 m): *"Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos...",* por acuerdo de su Director se procedió durante el año 2001 a realizar un Plan de Inspección de Oficio a los Sistemas de Información del Instituto Nacional de Estadística (INE) para comprobar su grado de funcionamiento y adecuación a las prescripciones de la citada Ley Orgánica y normativa que la desarrolla, concretándose las labores de inspección en la primera fase del Proyecto *Censos de Población y Viviendas 2001,* cuya formación constituye una competencia exclusiva del Instituto Nacional de Estadística.

Con carácter previo, y a tenor de la potestad que le confiere el Estatuto de la Agencia de Protección de Datos, el Director de la misma procedió a informar con carácter preceptivo el contenido y formato de los cuestionarios censales y de la hoja padronal utilizados como instrumentos para la recogida de datos del Proyecto *Censos de Población y Viviendas 2001*, así como el pliego de prescripciones técnicas del concurso para la prestación de servicios de un sistema telemático que permite la cumplimentación vía internet de los citados cuestionarios. Sobre esta segunda cuestión, el informe del Director dictaminó que "*será necesario que en el contrato que se celebre se incluya, en caso de que la entidad adjudicataria, como parece desprenderse del pliego facilitado, colabore efectivamente en el tratamiento de datos, una cláusula indicativa de los extremos del artículo 12 de la Ley Orgánica 15/1999, dado que así se garantizará la debida confidencialidad exigida por el secreto estadístico* ".

En el Censo de Población se incluyen todas las personas, ya sean españolas o extranjeras, que tienen fijada su residencia habitual en el territorio nacional, lo que supone un tratamiento de datos personales de millones de ciudadanos en el ámbito del mencionado Proyecto. Como consecuencia de la magnitud y complejidad del mismo y al no disponer el Instituto Nacional de Estadística de los recursos humanos y materiales precisos para la ejecución de las diversas actividades que supone la elaboración del citado Censo, ha sido necesaria la colaboración de otras Administraciones Públicas, así como la contratación de prestaciones de servicios con diversas empresas privadas, lo que ha supuesto el tratamiento masivo y obligado de datos de carácter personal por parte de entidades externas al INE.

* Conclusiones de la Inspección.

De las actuaciones realizadas por la Inspección de Datos en la primera fase del Plan de Inspección sobre el Instituto Nacional de Estadística y varias de las empresas que han colaborado con dicho Organismo en diversas labores preliminares de la operación censal, así como en la cumplimentación de los cuestionarios a través de internet, se desprenden las siguientes conclusiones que afectan, esencialmente, a los concursos públicos sobre prestaciones de servicios adjudicadas por el INE relativos a:

"Tirada y manipulado de cuestionarios personalizados de los Censos de Población y Viviendas 2001".

Las actividades realizadas por empresas externas en virtud de esta contratación consisten en la personalización de los cuestionarios censales y de la hoja padronal, antes de ser entregados en los domicilios de los ciudadanos para su cumplimentación. Tal prestación de servicios ha sido realizada por:

* PDM, Marketing Publicidad Directa, S.A.

* Unión Temporal de Empresas constituida por Comercial Importadora de Papel, S.A. y por Formularios Químicos, S.A.

* Venturini España, S.A.

* Mailgrafica Direct, S.A.

Las citadas empresas han tratado datos personales relativos a: "*dirección, nombre, apellidos, lugar de nacimiento, sexo, fecha de nacimiento, DNI o similar y nivel de estudios"* de unos trece millones de ciudadanos, a excepción de Mailgrafica Direct, S.A. que exclusivamente ha manejado información de un millón de ciudadanos.

"Edición de los cuadernos de recorrido de los Censos de Población y Viviendas 2001".

Las labores a realizar en virtud de esta contratación se corresponden con la personalización de los Cuadernos de Recorrido, instrumento de trabajo del agente censal, y han sido efectuadas por las compañías:

* Meydis Servicios, S.A., que, a su vez, ha subcontratado parte de la prestación del servicio con las empresas Cencla, S. A., Xerox España The Document Company, S.A.

* Venturini España, S.A., que, a su vez, ha subcontratado con las empresas Equipo Postal, S.A., Xerox España The Document Company, S.A.

Dichas sociedades han tratado datos personales de unos siete millones de ciudadanos relativos a: "*dirección y nombre y apellidos"* , así como información catastral asociada a edificios, viviendas y locales.

"Servicios de carácter informático para la implementación de un Sistema Telemático que permita la cumplimentación vía Internet de los Censos de Población y Viviendas 2001 y de un Centro de Atención al Usuario".

Este concurso público ha sido adjudicado a la Unión Temporal de Empresas formada por TS Telefónica Sistemas, S.A. y por Indra Sistemas, S.A. Así mismo han participado como subcontratistas las empresas Telefónica Data España, S.A., Atento Telecomunicaciones España, S.A. y Atlante, S.A.

Para la realización de las citadas tareas las empresas prestadoras del servicio y subcontratistas intervinientes han tratado datos personales de más de cuarenta millones de ciudadanos relativos a: "*dirección, nombre, apellidos, lugar de nacimiento, fecha de nacimiento, DNI o similar, nombre del padre y de la madre, nivel de estudios".*

Del análisis de la documentación contractual suscrita al amparo de los citados concursos y circunscrita al ámbito de las mencionadas prestaciones de servicios es destacable lo siguiente:

En los Pliegos de cláusulas administrativas figuran como obligaciones del adjudicatario que *"no podrá utilizar para sí ni proporcionar a terceros dato alguno de los trabajos contratados ni publicar, total o parcialmente, el contenido de los mismos sin autorización escrita del órgano de contratación. Adquiere igualmente el contratista el compromiso de la custodia fiel y cuidadosa de la documentación que se entregue para la realización del trabajo y, con ello, la obligación de que ni la documentación ni la información que ella contiene o a la que acceda como consecuencia del trabajo llegue en ningún caso a poder de terceras personas. El adjudicatario y todo el personal que intervenga en la prestación contractual quedan obligados por el deber de secreto estadístico establecido en el artículo 17 de la Ley de la Función Estadística Pública".*

Igualmente, en los Pliegos de cláusulas administrativas de los dos primeros concursos citados figuran como obligaciones del adjudicatario que: "*Una vez finalizada la edición, deberán devolverse los soportes magnéticos, ópticos o de cualquier otro tipo facilitados a la empresa adjudicataria para la realización del trabajo y un certificado en el que conste que no disponen de listados, ficheros, cintas o cualquier otro soporte con esta información o, en su caso, han sido destruidos los necesarios para la realización del trabajo".*

Así mismo, en el Anexo 3 del Pliego de prescripciones técnicas que rige el tercer concurso se incluye un apartado sobre la "*Confidencialidad de la información*", que ha de regir la actividad de formación de los Censos de Población. Por ello, la oferta deberá "*incluir un documento de seguridad de la instalación en la que se prestará el servicio"* para dar cumplimiento a las exigencias de las normativas legales siguientes:

La información de carácter padronal, regulada por la Ley Orgánica 15/1999 y normativa de desarrollo, en especial el Real Decreto 994/1999.

La información de carácter estadístico, regulada por la Ley 12/1989, de la Función Estadística Pública.

De otro lado, las sociedades intervinientes en la prestación de los servicios del apartado segundo y tercero han suscrito un contrato con el Instituto Nacional de Estadística por el que el citado Organismo autoriza a subcontratar y, en cumplimiento del artículo 12 de la Ley Orgánica 15/1999 y del Real Decreto 994/1999, acuerdan, entre otros puntos, que "*los encargados del tratamiento se comprometen únicamente a tratar los datos conforme a las instrucciones del Responsable del tratamiento (INE) ,y que no los utilizaran para otro fin distinto....".*

Finalmente, otro aspecto a considerar es que el INE ha establecido unos documentos que deben ser preceptivamente suscritos por las empresas que colaboran en los Censos de Población y por las personas que participan en los mismos, en el que declaran "*Haber leído y comprendido*" el contenido de su reverso en el que figuran aspectos sobre "*El secreto estadístico*", "*Las obligaciones que impone* " y "*Consecuencias de su vulneración* ".

* Recomendaciones al Instituto Nacional de Estadística.

A tenor de lo expuesto y en atención al resultado de las actuaciones practicadas por la Inspección de Datos, se han observado ciertas deficiencias en las contrataciones efectuadas por el Instituto Nacional de Estadística, que implican un acceso por cuenta de terceros a los Sistemas de Información cuya titularidad corresponde al citado Organismo y cuya subsanación supondría una sustancial mejora en el acatamiento de la Ley Orgánica 15/1999, de 13 de diciembre, y normativa que la desarrolla.

A tal efecto, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga el artículo 37 m) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el artículo 5 c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, dicta las siguientes recomendaciones que deberán ser observadas por el Instituto Nacional de Estadística, al objeto de adecuar plenamente los tratamientos automatizados que realiza a los principios de la citada Ley,

Recomendación Primera.

El Instituto Nacional de Estadística ha contratado con terceros la prestación de diversos servicios que implican el tratamiento automatizado de datos de carácter personal de millones de ciudadanos, que se encuentran incluidos en los Sistemas de Información cuya titularidad corresponde al citado Instituto. Dichos contratos se han realizado de conformidad con lo dispuesto en la Ley de Contratos de las Administraciones Públicas, Texto Refundido aprobado por Real Decreto Legislativo 2/2000, de 16 de junio, y normativa de desarrollo, que expresamente prevén la posibilidad de la subcontratación con ciertas limitaciones y modalidades.

Sin embargo, a tenor de lo dispuesto en el artículo 12.2 de la LOPD, *"la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin*

distinto al que figure en dicho contrato, ni los comunicará ni siquiera para su conservación, a otras personas. En el contrato se estipularán, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar". Por su parte, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad, establece las medidas de seguridad que deberán de cumplir los ficheros automatizados que contengan datos de carácter personal, tanto por el responsable del fichero como por el encargado del tratamiento.

Como consecuencia de ello, y a fin de cumplir plenamente con las prescripciones legales en materia de protección de datos, el INE, antes de la prestación del servicio, deberá suscribir con la empresa adjudicataria un contrato en el que consten y se cumplan los requisitos exigidos por el transcrito art. 12 de la LOPD, no siendo posible que el adjudicatario del concurso subcontrate los servicios con otra entidad a menos que actúe en nombre y por cuenta del Instituto Nacional de Estadística. En otro caso, el propio Instituto deberá contratar los servicios directamente con cada una de las entidades prestatarias del servicio.

Pero, además, el INE como responsable del fichero deberá establecer las medidas de índole técnica y organizativas que deben adoptar los encargados del tratamiento para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado. Así mismo, dependiendo de las características de la información tratada por el encargado del tratamiento en atención a su naturaleza y volumen, y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma, el INE realizará controles durante el periodo de vigencia del contrato para verificar el cumplimiento de las medidas de seguridad establecidas y adoptar las medidas correctoras oportunas.

Por otro lado, deberá tenerse en cuenta que el acceso a los datos personales por cuenta de terceros para la prestación de servicios deberá ser adecuado, pertinente y no excesivo en relación con el cumplimento de las finalidades establecidas en el contrato, y en el mismo deberá constar de conformidad con lo dispuesto en el art. 12.3 de la LOPD, que *"una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento al igual que cualquier soporte o documento en el que conste algún dato de carácter personal objeto del tratamiento".*

Con base en lo anterior, esta Agencia entiende que el Instituto Nacional de Estadística deberá establecer un modelo único de contrato en el que figuren cláusulas en los términos descritos en los párrafos anteriores.

Al margen de lo anterior, se considera una buena práctica que en los Pliegos de cláusulas administrativas particulares y Pliegos de prescripciones técnicas se incluyan unos apartados o cláusulas en las cuales se reflejen las anteriores prescripciones legales, de manera que tales Pliegos se ajusten no sólo a lo dispuesto en la Ley de Contratos de las Administraciones Públicas y normas complementarias, sino también a lo establecido en la LOPD y normativa de desarrollo.

En particular, de preverse o producirse una subcontratación que implique tratamiento de datos personales, deberán reflejarse en los citados Pliegos los requisitos exigidos por la LOPD, haciendo constar expresamente que, o bien el contratista adjudicatario del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento (INE) o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

Que los servicios a subcontratar se hayan previsto expresamente en el contrato originario celebrado entre el INE y el adjudicatario del servicio.

Que el contenido preciso del servicio subcontratado conste en el contrato originario.

Que el responsable del tratamiento establezca las instrucciones mediante las cuales el subcontratista tratará los datos, sin perjuicio de las instrucciones adicionales que pudieran establecerse por el adjudicatario del servicio.

Que en el contrato originario se establezcan las medidas de seguridad a adoptar por el subcontratista, sin perjuicio de las medidas adicionales que pudieran establecerse por el adjudicatario del servicio.

Recomendación Segunda.

La insuficiencia de medios personales y materiales para llevar a cabo un Proyecto de la magnitud y complejidad del ahora inspeccionado, ha obligado a contratar la prestación de servicios con empresas externas al INE. Igualmente, la premura de tiempo en que había de realizarse tal Proyecto, ha hecho necesario realizar subcontrataciones con otras empresas a fin de cumplir con los plazos legales establecidos al efecto. La consecuencia de todo ello ha sido, según se ha comprobado en la inspección practicada, que son numerosas las empresas contratistas y subcontratistas que han tratado millones de datos personales y han poseído copias con los datos registrados en los ficheros del INE.

Por ello, sin prejuzgarse por parte de esta Agencia situaciones pasadas o hipótesis de futuro, hay que convenir en lo delicado de una situación como la descrita, en la que numerosas empresas (alguna de las cuales incluso ha sido sancionada por infringir la propia LOPD) han venido a estar en posesión de la totalidad o gran parte de los ficheros del INE, que contienen millones de datos de españoles y residentes en España. Tal situación no sólo aconseja, sino que hace imprescindible prevenir sobre posibles utilizaciones ilícitas de tales datos personales.

En consecuencia, se considera una buena práctica que el INE establezca un procedimiento *ad hoc* que permita detec-

tar la utilización por los contratistas encargados del tratamiento y subcontratistas, de datos personales facilitados por el responsable del fichero, para finalidades distintas de las especificadas en el contrato de prestación de servicios.

A tal fin, se deberá incluir en las copias de los ficheros entregados a las empresas prestadoras de servicios un sistema de control (por ejemplo, incluyendo marcas diferenciadas en cada una de las copias) que permita identificar el origen exacto de la copia que se esté utilizando de manera ilegítima incumpliendo las estipulaciones del contrato.

Ello permitirá adoptar las medidas correctoras pertinentes y considerar a los encargados del tratamiento y subcontratistas como responsables del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente, de conformidad con lo prevenido en el art. 12.4 de la LOPD.

Recomendación Tercera.

El art. 20 del Texto Refundido de la Ley de Contratos de las Administraciones Públicas establece una serie de prohibiciones para contratar con la Administración por parte de aquellas personas en quienes concurran alguna de las circunstancias que señala. Entre tales circunstancias no se halla, sin embargo, la de haber sido sancionada por infracción de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Por lo tanto, mientras no se modifique la legislación vigente en el sentido aludido, no podrá prohibirse la contratación con empresas prestadoras de servicios que hayan sido sancionadas por la Agencia de Protección de Datos por infracción de la citada Ley Orgánica.

No obstante, no ve inconveniente esta Agencia y se considera una buena práctica, que en los pliegos de cláusulas administrativas se establezca alguna en la que a modo o especie de bonificación se favorezca la contratación con aquellas empresas que acrediten no haber sido sancionadas durante los dos últimos años previos al contrato por infracción grave o muy grave de las previstas en la Ley Orgánica 15/1999, de 13 de diciembre.

2.2.2. Fichero Histórico de Seguros del Automóvil. Recomendaciones

La Disposición Adicional Sexta de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, modifica el artículo 24.3, párrafo 2, de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción: "*Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley. También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación. En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado* ".

Con fecha de 30 de julio de 1998 se había inscrito en el Registro General de Protección de Datos el que actualmente se denomina "*FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL"* (código 1982110017), antes llamado "*FICHERO HISTÓRICO SINIESTRALIDAD CONDUCTORES*". En la actualidad, este fichero se rige por lo establecido en el primer párrafo del citado artículo, siendo su finalidad declarada la "*colaboración estadístico-actuarial para la selección y tarificación de riesgos que recoge datos de contratos de seguros del automóvil suscritos por el tomador del seguro de los cinco últimos años y los siniestros vinculados a dichos contratos."* Según consta en la inscripción del fichero, incluye datos identificativos y datos económico-financieros y de seguros.

En el mes de septiembre de 2000, el Director de la Agencia acordó la inscripción en el Registro General de Protección de Datos (CT00022000) del Código Tipo (CT) creado para regular el funcionamiento del "*FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL"* (FHSA). En este documento se identifica como titular del fichero a la UNIÓN ESPAÑOLA DE ENTIDADES ASEGURADORAS Y REASEGURADORAS (UNESPA), sin perjuicio del régimen de responsabilidad de las entidades aseguradoras adheridas. Por otra parte, se designa a TECNOLOGÍAS DE LA INFORMACIÓN Y REDES PARA LAS ENTIDADES ASEGURADORAS, S.A. (TIREA) como encargado de la "*gestión informática y tratamiento de datos del fichero*", especificando que esta entidad "*se encargará de llevar a cabo las actividades que garanticen la prestación de los servicios informáticos, incluyendo la realización de los controles necesarios para asegurar que no se realiza un uso indebido del fichero.* "

Por acuerdo del Director de la Agencia de Protección de Datos, durante el año 2001 se procedió a realizar, por parte de la Inspección de Datos, un Plan de Inspección de Oficio cuyo objetivo era determinar si el FICHERO HISTÓRICO DE SEGUROS DEL AUTOMÓVIL se ajusta a los principios de la legislación vigente en materia de protección de datos.

Por otra parte, a pesar de concebirse como una inspección de oficio, en el curso de la misma se han revisado las circunstancias en las que se incorporaron al FHSA los datos de las 20 personas que hasta ese momento se habían

dirigido a la Agencia para que ésta tutelase el ejercicio de sus derechos.

* Conclusiones de la Inspección

A continuación se exponen las conclusiones obtenidas a partir de las actuaciones de inspección practicadas, así como una serie de recomendaciones con las que se emplaza a los implicados para que subsanen las deficiencias observadas.

Conclusiones generales

Desde su entrada en funcionamiento, en el mes de octubre de 2000, hasta el momento de realizarse la inspección se habían adherido al FHSA 44 compañías, lo que supone un 60% de las entidades aseguradoras que están autorizadas a operar en el ramo del automóvil. De esa cifra, un 77% ya había comenzado el proceso de envío de datos al fichero.

El CT establece como requisito para la adhesión que la compañía esté inscrita en el Registro Especial de la Dirección General de Seguros, aunque no es preciso ser asociado de UNESPA. Así mismo, se prevé que las altas de nuevas compañías serán comunicadas a la Agencia de Protección de Datos, al objeto de que queden incorporadas al propio CT. A este respecto, se ha comprobado que, antes de iniciarse la inspección, el Registro General de Protección de Datos ya tenía conocimiento del nombre de las compañías actualmente adheridas.

Derecho de información en la recogida de datos

El apartado 1 del artículo 5 de la LOPD especifica la información que es preciso facilitar de modo expreso, preciso e inequívoco a los interesados a los que se soliciten datos personales. Así mismo, el apartado 4 del mismo artículo establece que "*cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo*". Por otra parte, en su apartado 5 se establece que, entre otros supuestos, "*no será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea* ".

Por otra parte, puesto que el FHSA se encuadra en la primera de las modalidades de ficheros contempladas en el artículo 24.3 de la Ley 30/1995, se requiere en este caso que a los interesados se les comunique "*la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley".* Así, la comunicación habrá de ser realizada por cada compañía aseguradora.

En el CT (apartado 7.3) se hace referencia al deber de comunicación al afectado, estableciéndose que "*dicha notificación será uniforme para todas las entidades aseguradoras adheridas*" incluyéndose un modelo de la misma como anexo (pág. 19), el cual tiene la siguiente redacción: "*En virtud de la autorización que concede la ley 30/1995, Unión Española de Entidades Aseguradoras y Reaseguradoras (UNESPA) ha creado el Fichero Histórico de Seguros de Automóviles para la tarificación y selección de riesgos, constituido con la información aportada por las entidades aseguradoras. Le comunicamos que los datos sobre su contrato de seguro del automóvil y los siniestros vinculados a éste, de los últimos cinco años, si los hubiere, serán cedidos al citado fichero común. Si desea ejercitar los derechos de acceso, rectificación, cancelación y oposición puede dirigirse a TIREA, c/ García de Paredes, 55, 28010 Madrid, debiéndose identificar mediante DNI, pasaporte o tarjeta de residencia* ".

Esta obligación de notificar al tomador del seguro también se recoge en el contrato de adhesión al servicio, estableciéndose que "*serán de cuenta de la entidad cuantas sanciones, multas y/o penalizaciones se deriven de dicho incumplimiento* ".

Según consta en Acta, estas notificaciones "*son enviadas entre uno y dos meses antes de la fecha de vencimiento*" y en cualquier caso antes de que los datos se hayan incorporado al FHSA, aunque este extremo no ha podido ser verificado, dado que en el fichero no se guarda constancia de la fecha de envío. Una vez remitida la notificación de vencimiento al asegurado y antes de que venza la póliza, la entidad aseguradora remite los datos correspondientes a TIREA para su inclusión en el *FHSA*, de acuerdo con lo expresado en dicha comunicación. A este respecto, UNESPA y TIREA han declarado que "*no disponen de ningún medio para garantizar que los asegurados han sido previamente informados al respecto por la entidad aseguradora, siendo cada compañía aseguradora la que debe responsabilizarse de cumplir con los procedimientos establecidos"* .

A partir de los documentos que los interesados han aportado a la Agencia junto con sus reclamaciones, se ha comprobado que, en general, las compañías están remitiendo notificaciones que contienen el citado texto. Sin embargo, alguna compañía ha encabezado sus notificaciones con la fecha de vencimiento de la póliza, en lugar de indicar la fecha de envío, lo que puede dar lugar a cierta confusión respecto de la fecha en que se ha realizado la comunicación.

Por otra parte, respecto de las pólizas que se han suscrito con posterioridad a la creación del FHSA, UNESPA ha recomendado a las compañías aseguradoras que incluyan en las Condiciones Generales o Particulares un texto similar

al de las notificaciones. De esta forma, el solicitante del seguro decide si acepta suscribir la póliza con una compañía que incorporará sus datos al FHSA, pudiendo optar, si lo desea, por suscribirla con una compañía que no esté adherida al mismo.

Calidad de los datos

Como norma para garantizar la veracidad de los datos que las entidades deben remitir al *FHSA,* el CT establece que éstos deben provenir en todo caso de los Registros de Pólizas y de Siniestros que, con carácter obligatorio, se establecen en el artículo 65 del Reglamento de la Ley 30/1995 y que están sometidos al control y supervisión de la Dirección General de Seguros. En este sentido, cada compañía asume la total responsabilidad sobre la veracidad de los datos facilitados al fichero. Por otra parte, es obligación de la compañía impedir la utilización de los datos del fichero para otras finalidades.

Dentro de las finalidades previstas por la Ley 30/1995, este fichero tiene por objeto "facilitar, al momento de la suscripción del contrato, información rigurosa y contrastada de los datos de siniestralidad mediante la puesta en común de la información obtenida a través de pólizas y siniestros". En el contrato de prestación de servicios firmado entre UNESPA y TIREA se exponen los siguientes fines: "Promover la transparencia en el mercado del seguro del automóvil, a fin de que las personas que quieran contratar un seguro con otra entidad aseguradora puedan tener fácil acceso a los datos que sobre sus contratos y siniestros disponen las entidades con quienes hayan tenido relaciones contractuales. Las entidades aseguradoras con la información que tiene el fichero podrán ampliar la que el propio tomador facilita al momento de declarar el riesgo, lo que permitirá adecuar los riesgos a los criterios de selección y tarificación de la entidad. La información del fichero, una vez disociados los datos de carácter personal, permitirán a su vez la realización de estudios técnicos y actuariales y la elaboración de estadísticas tan necesarias para el sector."

Sin embargo, aunque la utilidad del *FHSA* es aportar a las entidades información sobre la siniestralidad de los solicitantes de una póliza, el fichero relaciona esta información con el vehículo asegurado. El vehículo se identifica en el *FHSA* mediante tres campos: MATRICULA (que contiene la matrícula completa con formato FIVA), ID_MATRICULA (que indica el tipo de la matrícula: ordinaria, vehículos especiales, remolques, ciclomotores, régimen diplomático, turismo, histórico, temporal, pruebas, ITV, vehículos oficiales, otras) y CO_TIPO_VEHÍCULO (que indica el tipo de vehículo: automóvil, motocicleta, otros). La tipificación de vehículo y matrícula se utiliza como criterio de verificación adicional tanto en el proceso de inclusión del dato en el fichero como en el proceso de consulta.

Los datos que se incorporan al *FHSA* son relativos siempre a tomadores de pólizas. Se ha verificado que, hasta el momento, todos los datos incluidos en el fichero hacen referencia a siniestros cubiertos por la garantía de responsabilidad civil (presente en el seguro obligatorio). Respecto de cada siniestro, se refleja en el fichero si causó daños personales y/o materiales, no guardándose constancia de a quién le correspondió la culpa. Así mismo, se refleja la situación actual del siniestro según la siguiente clasificación: cerrado (87% de los casos), pendiente por reclamación judicial, por reclamación administrativa, por reclamación ante el Defensor del Asegurado o por otro motivo. A este respecto, UNESPA ha declarado que los siniestros incluidos en el *FHSA* con situación "*pendiente*" y cuyo pago no le corresponde a la entidad aseguradora que los ha incorporado al fichero se eliminan de éste, una vez que la entidad aseguradora así lo resuelva. Por otra parte, se ha verificado que, una vez superados los cinco años de antigüedad, se siguen conservando datos de los siniestros (a efectos estadísticos) pero de forma anonimizada.

Respecto del tomador del seguro, se almacena en el fichero la siguiente información: número del documento de identificación (NIF, pasaporte, tarjeta de residencia, CIF), nombre y apellidos. A pesar de que la estructura actual del fichero lo permitiría, hasta el momento no se han incorporado datos relativos a la fecha de nacimiento del tomador. Por otra parte, cada siniestro está asociado a una determinada póliza, según la numeración de la entidad aseguradora, a la que se identifica según el código asignado por la D.G.S. Se comprobó que, para cada persona y cada vehículo, en el fichero se relacionan todas las pólizas que han tenido algún período de vigencia después del 1 de octubre de 2000 y que, a excepción de la hoy vigente, figuran todas marcadas como "*CANCELADA*" (en la actualidad, aproximadamente un 5% del total). Así mismo, se comprobó que no figuraban datos de pólizas con una fecha de vencimiento anterior a la fecha de inclusión.

El Código Tipo prevé que "*TIREA bloqueará automáticamente los datos que tengan más de cinco años de antigüedad*", lo que se aplica tanto a las pólizas que ya no están vigentes como a los siniestros (cubiertos por pólizas vigentes o no). Sin embargo, por el escaso tiempo de vida del *FHSA*, esto no ha podido verificarse respecto de los datos de las pólizas vencidas, puesto que las primeras habrán de bloquearse después de octubre de 2005.

Por otra parte, hasta el momento UNESPA no ha decidido si conservará en el *FHSA* todos los datos de asegurados previamente incorporados por una compañía que deja de estar adherida.

Datos especialmente protegidos

Tras analizar la estructura del *FHSA* no se ha obtenido constancia de que contenga datos de los que el artículo 7 de la LOPD considera especialmente protegidos.

Ejercicio de los derechos de acceso, rectificación, oposición y cancelación

Tal y como se especifica en el contrato firmado entre TIREA y UNESPA, la primera compañía, en representación de la

segunda, "gestionará la solicitudes de acceso, rectificación, cancelación u oposición que en ejercicio de sus derechos realicen los afectados, al objeto de poder cumplir los plazos que prevé la LOPD", según los procedimientos detallados en el CT. Con este objeto, TIREA ha constituido el denominado Centro de Operaciones, en el que se centralizan todas las labores de atención al ejercicio de estos derechos, comunicándose para ello con los respectivos Interlocutores de Protección de Datos que en cada una de las entidades aseguradoras realizan estas labores.

El apartado 8 del CT establece el procedimiento para la atención de estos derechos. Respecto del derecho de acceso, está previsto que "si la solicitud se formula correctamente, TIREA emitirá certificación en la que consten todos los datos que sobre esa persona contiene el Fichero". Se ha comprobado que este tipo de solicitudes se contestan por TIREA indicando, además de los datos incluidos en el fichero, el nombre de las entidades que los han consultado, aunque en la actualidad no se informa de la fecha en que tuvo lugar la consulta.

Respecto de los derechos de rectificación y cancelación, se ha previsto que "si la rectificación o cancelación afecta a datos personales de identificación y con la documentación aportada por el afectado resultare suficientemente probado el error o la inexactitud, se procederá automáticamente a su modificación o cancelación, comunicándolo a la Entidad aseguradora". En cambio, "cuando la solicitud verse sobre la existencia y/o cuantía de los siniestros, el responsable del fichero dará traslado de la solicitud a la entidad aseguradora que haya facilitado el dato, al objeto de que en el plazo de ocho días resuelva de forma motivada sobre su procedencia. Si la entidad no se pronuncia, TIREA mantendrá el bloqueo cautelar del dato, y se comunicará tanto al afectado como a la entidad aseguradora que deberá proceder a su rectificación o cancelación, en los términos de la solicitud, en la primera actualización de información. Realizada la necesaria comprobación por TIREA, si la entidad no hubiera procedido a dicha rectificación o cancelación, el dato quedará definitivamente bloqueado. Si la entidad aseguradora resuelve oponiéndose a la rectificación o cancelación solicitada, deberá motivar su posición ante UNESPA, como responsable del Fichero. La respuesta de la entidad aseguradora será trasladada al afectado, indicándole que la misma puede ser recurrida ante la Comisión de Control en el plazo de quince días desde que recibió la comunicación, mediante presentación de escrito en que razone su petición y los documentos en que fundamenta la misma. Recibido el escrito de recurso, se resolverá por la Comisión de Control en el plazo de quince días".

Respecto de la solicitud de ejercicio del derecho de oposición, el CT prevé que "habrá que atender a la causa de tal solicitud y a los motivos en que fundamenta su pretensión el solicitante. Se seguirá idéntico procedimiento que el descrito para los derechos de rectificación y cancelación. No obstante y, en los casos en que se desestime y acredite por la entidad aseguradora la improcedencia de la oposición, UNESPA podrá, tras comunicarlo al afectado, proceder de oficio al bloqueo de los datos y elevar consulta a la Agencia de Protección de Datos para clarificar la procedencia de tratamiento automatizado de los datos". Aunque en la actualidad no existe ninguna norma al respecto, se ha comprobado que, por sus especiales circunstancias, algunas entidades aseguradoras están estimando las solicitudes de oposición presentadas por personas en las que concurren tales circunstancias.

Se ha verificado que en el momento de recibirse una solicitud de rectificación, cancelación u oposición, TIREA bloquea los registros correspondientes (todos los relativos al tomador o a la póliza en cuestión) mediante la columna ID_BLOQUEO ('S'). En esta situación permanecen hasta que se resuelve la solicitud. En el caso de que la entidad aseguradora resuelva que la solicitud procede porque los siniestros no son imputables a las pólizas del tomador, entonces los datos referidos a éstos se eliminan del fichero. Si la entidad resuelve que procede la oposición/cancelación o bien la entidad no resuelve dentro del plazo, entonces los datos se bloquean definitivamente (es decir, permanecerán ya siempre con el valor 'S'). Se ha comprobado que, hasta el momento de realizarse la inspección, se habían producido 2.355 acciones de bloqueo/desbloqueo en el fichero, como consecuencia de las diversas solicitudes recibidas.

Los datos incluidos en el FHSA referidos a cada tomador pueden presentar 4 situaciones diferentes, que se reflejan con un valor diferente en la columna ID_BLOQUEO. De ellas merece destacarse la relativa al valor 'S', situación de bloqueo, que puede ser cautelar (cuando se ha recibido una solicitud de rectificación/cancelación/oposición, antes de ser tramitada) o bien definitivo. A este respecto se pudo comprobar que ambas situaciones no son directamente distinguibles en el fichero, lo que obliga a considerar simultáneamente la fecha de bloqueo.

A este respecto, UNESPA aún no ha decidido cómo se tratarán los datos que se intenten incorporar al fichero relativos a un tomador que ya figura en situación de bloqueo definitivo.

Por otra parte, se ha observado que en el campo FH_ALTA se hace constar la fecha en que cada dato está siendo incorporado al FHSA, no existiendo ningún otro campo en el fichero en el que se deje constancia del momento en que el dato comienza a estar a disposición de las compañías aseguradoras para su consulta.

Aparte de los datos de las 20 personas que han reclamado ante la Agencia, durante la inspección también se analizaron otros 20 expedientes elegidos al azar (pero distribuidos uniformemente entre diciembre de 2000 y junio de 2001) de entre todos los iniciados como consecuencia de las solicitudes presentadas ante TIREA por los interesados en ejercicio de sus derechos y que permanecían todavía entonces en el FHSA en situación de bloqueo. A este respecto, se pudo comprobar que los escritos de contestación remitidos a los interesados no presentan una redacción uniforme, en especial en lo relativo a la acción que lleva a cabo TIREA, que en unos casos utiliza el término "cancelación", en otros "baja cautelar" o, en otros "cancelación cautelar", cuando en todos los casos el resultado es el "bloqueo definitivo" de los datos en el fichero.

Acceso a los datos por cuenta de terceros

Tal y como prevé el CT, TIREA actúa respecto al FHSA en calidad de encargado del tratamiento, en el sentido de lo que dispone el artículo 3.g de la LOPD, regulándose la prestación de este servicio de acuerdo con lo establecido por el artículo 12 de la misma Ley, mediante el contrato firmado con fecha de 10 de julio de 2000. En este documento se prevé que "TIREA responderá directamente de las sanciones administrativas o de cualquier otro orden que le impusieran por actuaciones que le sean directamente imputables, y de los daños y perjuicios que por estos motivos se irrogase a UNESPA y a las entidades adheridas".

La estipulación Tercera del documento establece que "TIREA deberá implementar todas las medidas de seguridad que requiera el nivel en el que se incluya la información tratada, entre otras: Elaboración de Documento de seguridad; Procedimientos de identificación y autenticación; Controles de acceso; Realización de copias de respaldo y recuperación; Designación de un responsable de seguridad; Realización periódica de Auditorías de Seguridad, al menos cada dos años; Mantener un registro de incidencias".

Comunicación de datos

El apartado 7.2 del CT prevé que "las entidades adheridas podrán realizar consultas al Fichero, según los modelos propuestos en la plataforma tecnológica, que no permite en ningún caso volcar el fichero en su base de datos". Por otra parte, el apartado 5.1.1 del mismo CT prevé que "los datos del fichero no pueden ser objeto de volcado en la base de datos de la entidad, su consulta únicamente puede realizarse caso a caso. La entidad se compromete a no imprimir o grabar los datos a que acceda a través de consulta al fichero". Sin embargo, según se ha comprobado, la configuración actual del servicio *TIRE'arroba'SINCO* sí permite que las propias entidades reciban en sus respectivos sistemas informáticos los ficheros conteniendo el resultado de cada una de las consultas realizadas. En cualquier caso, el artículo 6 del Código Tipo establece que "la entidad impedirá la utilización de la información del Fichero para cualesquiera otras finalidades que no sean las previstas en este Código Tipo así como divulgar información personal o confidencial".

Las entidades aseguradoras disponen de dos vías distintas para acceder al FHSA: on line y en modo diferido (batch). En ambos casos, el sistema devuelve el resultado en un fichero que debe ser posteriormente tratado por el sistema informático de la propia entidad aseguradora.

Para realizar una consulta al fichero es imprescindible que la entidad consultante conozca en todo caso los cinco últimos dígitos del código de la póliza en vigor del solicitante. Además, debe facilitar al sistema uno de los siguientes datos: nombre y apellidos del tomador, número del documento de identificación (D.N.I., pasaporte, tarjeta de residencia) o matrícula del vehículo asegurado. En los dos primeros casos el resultado hará referencia a todas las pólizas suscritas por el interesado (de todos los vehículos). En el último caso hará referencia a los seguros del vehículo referido que han sido contratados por el tomador de la póliza cuyos cinco últimos dígitos se aportan.

Actualmente, en el resultado de la consulta sólo se incluyen datos personales identificativos (número del documento de identificación o nombre y apellidos) si estos datos son aportados por la entidad aseguradora en el momento de realizar la consulta. Aparte de esos datos, según se deduce del Manual de Explotación, el resultado de la consulta incluye:

- Número de pólizas contratadas por el mismo tomador que ha suscrito la póliza cuyos últimos cinco dígitos se han aportado, especificando para cada una de ellas su período de cobertura y la matrícula del vehículo asegurado.

- Número de siniestros cubiertos por cada póliza contratada por ese tomador, especificando su fecha, la existencia o no de daños personales, la existencia o no de daños materiales y la situación actual (cerrado o pendiente, indicando en este último caso si la causa es una reclamación judicial, administrativa, ante el Defensor del asegurado u otra).

Movimiento internacional de datos

No se ha tenido constancia de que en la actualidad se realicen transferencias de datos del FHSA a otros países.

Seguridad de los datos

En el CT (apartado 5) se establece que el FHSA "tiene implementado un sistema de seguridad que garantiza el cumplimiento estricto de la LOPD", el cual está basado en las siguientes medidas, cuyo cumplimiento fue analizado durante la inspección.

- Los datos no podrán volcarse masivamente en las entidades adheridas, las cuales tampoco pueden imprimir o grabar estos datos. No obstante, TIREA ha declarado que no dispone de medios para impedir que las entidades adheridas incorporen tales datos a un fichero.

- Existirá un registro de auditoría que permitirá obtener pistas acerca de cada consulta del FHSA (fecha, hora y entidad consultante). Se ha verificado que junto al fichero existe una tabla en la que se guarda constancia de cada una de las consultas realizadas por cada entidad aseguradora, incluyendo los criterios de búsqueda y el resultado de la misma.

- Sólo se podrá obtener información del fichero cuando medie petición de aseguramiento por el tomador, que debe aportar su número de póliza y un dato identificativo (nombre y apellidos o bien número de DNI o bien matrícula del vehículo). A través de la mencionada tabla, se ha comprobado que no se habían realizado consultas con resultado positivo en las que no se hubiese aportado el número de póliza.

- Existirá una Aplicación de Consulta de Incidencias, en la que se hará constar tipo, momento y persona que la detecta, información que se obtiene de la comunicación entre TIREA y el Responsable de Seguridad de la entidad aseguradora que corresponda. Se ha verificado que TIREA dispone de una aplicación específica para la Consulta de Incidencias.

- Existirá un inventario de soportes de almacenamiento, así como un registro de entrada y salida de soportes. Por otra parte, existirán Procedimientos de borrado o inutilización, para impedir la legibilidad o reutilización de los soportes que se desechan. A este respecto, TIREA ha declarado que los ficheros de datos recibidos para su incorporación al FHSA son eliminados del sistema, una vez superados los procesos de carga, destruyéndose así mismo, en su caso, los soportes (CDROM o DAT) que se hubiesen recibido.

- Los datos se bloquearán cuando se ejerce el derecho de rectificación, cancelación u oposición. A este respecto se han realizado las comprobaciones ya mencionadas.

- Las entidades aseguradoras deben adoptar medidas de seguridad de nivel medio e incluir en el Documento de Seguridad un capítulo específico sobre los medios empleados garantizar para seguridad de los datos del FHSA, especialmente la relativa a funciones y obligaciones de las personas autorizadas por la entidad para acceder al fichero.

Por otra parte, TIREA ha aportado copia de su Documento de Seguridad, con fecha de última actualización del mes de junio de 2000. En relación con este documento genérico de la compañía se realizaron las siguientes verificaciones:

- Existe un documento que contiene las normas de seguridad para el personal con acceso a *TIRE'arroba'SINCO*. Así mismo, en el Anexo I al contrato laboral de los trabajadores de TIREA se incluye una declaración firmada por éstos en el sentido de conocer "su obligación de guardar secreto de las informaciones que pueda obtener de cualquier fichero automatizado o en relación con la intervención en cualquier tratamiento de datos de carácter personal" y de comprometerse a cumplirla.

- Se verificó la existencia de un documento que contiene las "Normas específicas para la realización de las copias de seguridad de los ordenadores del Centro de Proceso de Datos".

- Se obtuvieron diversos listados conteniendo la relación de usuarios definidos en cada uno de los componentes el sistema informático que permite acceder al FHSA.

- Se verificó la existencia de un Informe de auditoría interna del Sistema de Gestión de la Calidad para la prestación, entre otros, del servicio *TIRE'arroba'SINCO*, de abril de 2001, así como de un Informe de auditoría elaborado por una entidad externa, correspondiente al año 2000.

Notificación e inscripción registral de los ficheros

Durante la inspección realizada se tuvo acceso a la aplicación informática con la que TIREA gestiona las solicitudes recibidas en relación con el ejercicio de derechos, no habiéndose constatado que el fichero correspondiente, en el que se almacenan datos identificativos y del domicilio de los solicitantes a efectos de notificación, haya sido convenientemente inscrito en el Registro General de Protección de Datos.

También ha podido verificarse que en la inscripción del fichero "Registro de Incidencias Pago Mediadores-IPAMED", mencionado en el apartado anterior y cuyo responsable es UNESPA, no consta que la compañía TIREA esté actuando en calidad de "encargado del tratamiento".

* Recomendaciones

En conclusión y teniendo como referencia el resultado de las actuaciones de Inspección llevadas a cabo, el Director de la Agencia de Protección de Datos, en virtud de las potestades que le otorga el art. 5, c) y d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia, dictó las siguientes recomendaciones, que deberán ser observadas por el responsable del fichero, el encargado del tratamiento y todas las entidades adheridas, al objeto de adecuar su actuación a los principios de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, a la normativa que la desarrolla y al Código Tipo que regula el Fichero Histórico de Seguros del Automóvil.

Recomendación Primera

Los escritos de notificación que se remiten en cumplimiento de lo que establece el artículo 24.3 de la Ley 30/1995 se fecharán siempre con el día en que son enviados, en lugar de encabezarlos con la fecha en que vence el contrato de seguro. Así mismo, las compañías aseguradoras deberán adoptar las medidas adecuadas para poder acreditar la fecha en que el asegurado ha sido informado. A este respecto, se considerará una buena práctica la inclusión de dicha fecha en el propio FHSA.

Recomendación Segunda

Las compañías adheridas al FHSA deberán informar previamente a la recogida de datos, conforme establece el artículo 5 de la LOPD, de todos y cada uno de los extremos previstos en dicho precepto.

Recomendación Tercera

La información que se almacene en el fichero relativa a los siniestros pendientes de liquidación o pago deberá ajustarse a lo previsto en el apartado 7.1 del Código Tipo, debiendo excluirse la que se refiere al motivo que origina dicha situación (reclamación judicial, administrativa, ante el Defensor del asegurado u otro).

Recomendación Cuarta

De acuerdo con lo que establece el apartado 10 del Código Tipo, cuando una entidad deje de estar adherida al fichero se procederá a dar de baja en el mismo todas las referencias aportadas en su día por esa entidad. Por otra parte, las compañías que hayan causado baja y pretendan adherirse de nuevo al fichero deberán cumplir todas las obligaciones exigibles a una nueva adhesión.

En este sentido, la información que en su día fue incorporada al fichero no podrá ser reutilizada, ni siquiera en el caso de que alguno de los tomadores que contrataron con ella suscriba un nuevo contrato con otra compañía adherida.

Recomendación Quinta

La utilización de un mismo código ('S') para reflejar dos situaciones claramente diferentes (bloqueo cautelar o definitivo) no se considera apropiada a los efectos de lo previsto en el artículo 16 de la LOPD, por lo que deberán utilizarse códigos diferentes.

El bloqueo definitivo de los datos no permitirá en ningún caso el acceso por parte de las compañías adheridas a los datos de tomadores que figuren en el fichero común y sólo se conservarán en tal situación a efectos del cumplimiento de las correspondientes obligaciones legales.

Recomendación Sexta

Deberán normalizarse los escritos de contestación remitidos a los interesados, que en la actualidad no presentan una redacción uniforme, en especial en lo relativo a los diversos términos utilizados para designar la acción realizada por parte de TIREA como consecuencia de una solicitud de acceso, rectificación, cancelación u oposición.

Recomendación Séptima

En relación con lo que establece el apartado 5.1.1 del Código Tipo, las compañías adheridas deberán asegurarse de que en sus propios sistemas informáticos no se conservan ni se imprimen en ningún caso datos que hayan podido ser obtenidos como consecuencia de las consultas realizadas al FHSA. La Comisión de Control prevista en el apartado 9 del CT deberá adoptar las medidas que permitan comprobar de oficio el cumplimiento de esta recomendación. Así mismo, se reitera la obligación prevista en el apartado 7.2 del citado documento.

Recomendación Octava

Respecto del documento de seguridad aportado por TIREA, en el que se incluyen las medidas de seguridad generales implantadas en su establecimiento, deberá elaborarse un documento específico para el FHSA, en el que se reflejen las medidas particulares adoptadas para este fichero, incluyendo ya las acciones llevadas a cabo a partir de las propuestas sugeridas en aquel documento, que en ciertos aspectos ha quedado obsoleto.

Recomendación Novena

Dada la coexistencia de diversos ficheros con datos de carácter personal en el establecimiento de TIREA, los cuales tienen a su vez diversa procedencia y finalidad, el documento de seguridad deberá especificar las medidas adoptadas, tanto técnicas como organizativas, para evitar un posible cruce de la información almacenada en todos ellos.

Recomendación Décima

Deberá notificarse a la Agencia el fichero utilizado por TIREA para la gestión de las solicitudes de ejercicio de los derechos de los ciudadanos, cuya estructura difiere de la del propio FHSA, con objeto de que sea oportunamente inscrito en el Registro General de Protección de Datos.

Recomendación Décima Primera

Respecto del fichero "*REGISTRO DE INCIDENCIAS PAGO MEDIADORES-IPAMED*", deberán notificarse a la Agencia las oportunas modificaciones habidas en su inscripción, en particular, la relativa a la compañía que actúa en calidad de "*encargado del tratamiento*", con objeto de que sean oportunamente reflejadas en el Registro General de Protección de Datos.

Así mismo, con independencia de la observancia de las anteriores recomendaciones, se considera una buena práctica que en el propio fichero se deje constancia de los sucesivos períodos en que cada registro es consultable por las entidades adheridas, circunstancia ésta que en la actualidad es imposible determinar.

2.2.3. Europol

Por acuerdo del Director de la Agencia, se inició un plan de inspección para determinar el funcionamiento y los métodos de trabajo de la Unidad Nacional de Europol española y de la Oficina de Enlace adscrita a la misma, en relación con el tratamiento de los datos de carácter personal.

El funcionamiento de estos dos órganos se regula en los artículos 4 y 5 del Convenio de Europol, recogiéndose también en el mismo el marco legal de los tres componentes del Sistema Informatizado de Recogida de Datos de Europol: Sistema de Información, Ficheros de análisis y Sistema de Índices. Según dicho Convenio, las Unidades Nacionales son el único órgano de enlace entre Europol y los servicios competentes de los Estados miembros, encargándose los funcionarios de enlace del intercambio de información entre esas Unidades Nacionales y Europol.

En la inspección se verificó si los procedimientos implantados en dichos órganos, se adecuaban a lo regulado en el Derecho español en materia de protección de datos, así como lo específicamente estipulado en el Convenio de Europol.

A tal efecto, se inspeccionó tanto la Oficina de Enlace de Europol española ubicada en los Países Bajos, como la Unidad Nacional ubicada en España.

Como resultado de la inspección se apreció que los tratamientos cumplen, en términos generales, las previsiones de la LOPD si bien, se detectaron algunos aspectos susceptibles de mejora que se han trasladado a los responsables de los ficheros de los mismos.

Dada la naturaleza de la entidad inspeccionada y los hechos que se ponían de manifiesto en la inspección practicada, cuya publicidad pudiera afectar al carácter reservado de esa institución, la información contenida en la presente Memoria se limita a señalar la realización de la inspección.

2.2.4. Plan de Oficio al Sector de la Banca a Distancia.

Durante el año 2001 se procedió a realizar un Plan de Inspección de oficio al sector de la Banca a Distancia con objeto de comprobar el grado de adecuación de los ficheros automatizados del sector a las prescripciones de la legalidad vigente sobre protección de datos de carácter personal.

El objetivo principal perseguido en la realización del plan ha sido no tanto el auditar los tratamientos de datos personales en la actividad bancaria tradicional, como el auditar aquellos tratamientos que son específicos y que derivan precisamente de una relación entre entidades y ciudadanos en la que no es necesaria una presencia física.

Es esta especial relación la que impone una serie de procedimientos que no existían en la banca tradicional y en los que las nuevas tecnologías juegan un papel fundamental, al tiempo que presentan una serie de implicaciones en materia de protección de datos y, especialmente, en los aspectos de seguridad, donde conseguir un equilibrio entre la necesidad de establecer procedimientos sencillos para el acceso del usuario a los servicios y la imprescindible seguridad en las transacciones, no resulta trivial.

No obstante lo anterior, también se recogen en la presente inspección conclusiones sobre algunos tratamientos de los que se ha tenido conocimiento en el transcurso de las auditorías y que no siendo específicos de la banca a distancia, se ha considerado que necesitan una adecuación a lo establecido en la normativa de protección de datos.

Para la consecución de este objetivo se ha seleccionado una muestra de entidades con la idea de exponer las conclusiones obtenidas de forma anónima, ya que lo que interesa es que el resultado de la inspección sirva al sector en su conjunto para adecuar su funcionamiento a la normativa de protección de datos.

Finalmente debe puntualizarse que en las conclusiones se recogen fundamentalmente aquellos aspectos que son susceptibles de mejoras. Bien entendido que se trata de aspectos concretos obtenidos de entre todas las entidades analizadas, sin que pueda deducirse por ello que ninguna en particular presenta un funcionamiento deficiente así como tampoco el sector en su conjunto.

* Conclusiones respecto de la ley orgánica 15/1999 y normativa de desarrollo.

Las conclusiones relativas a los ficheros de clientes son las siguientes:

Origen de la información.

Atendiendo al origen de la información se han detectado tres fuentes básicas de datos personales:

a) Datos personales procedentes de fuentes externas mediante alquiler y/o compra de ficheros con fines de publicidad directa.

b) Datos facilitados a la entidad directamente por los afectados con el fin de solicitar algún tipo de información o participar en alguna iniciativa de aquella (simulador de bolsa, agregador financiero, etc.), pero que no llegan a disponer de

un Código de Cuenta de Cliente (CCC) con la entidad.

c) Datos de personas que tienen al menos un Código de Cuenta de Cliente (CCC) con la entidad.

Los datos personales obtenidos en base a la casuística anterior pueden ser ampliados con información procedente de otras fuentes:

a) Información facilitada por el propio cliente cuando solicita la contratación de productos y servicios ofrecidos por la entidad (ej.: solicitud de un crédito hipotecario, etc.)

b) Información recabada por los propios agentes comerciales de la entidad bancaria.

c) Información financiera de productos contratados, así como movimientos en las cuentas.

d) Información procedente de otras entidades financieras (por ejemplo, la obtenida como consecuencia de los agregadores financieros).

e) Información sobre incumplimiento de obligaciones dinerarias obtenida de ficheros constituidos al amparo del artículo 29 de la LOPD.

f) Información relativa al comportamiento de pago en los productos de activo contratados con la propia entidad.

Calidad de datos (artículo 4).

* Respecto de la finalidad de los tratamientos:

De la información recabada de los ficheros de gestión de clientes se desprende que los datos personales tratados en cada uno de ellos son, en general, adecuados, pertinentes y no excesivos con las correspondientes finalidades.

Se ha detectado también la existencia de sistemas de información del tipo DataWarehouse especializados en tratamientos complejos y masivos de la información de los usuarios. No se ha detectado que los usuarios que utilizan este tipo de sistemas tengan acceso a los datos de clientes de forma individualizada, sino a datos agregados, ya que la finalidad de dichos tratamientos es la de diseñar nuevos productos y servicios mediante la definición de campañas comerciales y la selección de los colectivos de clientes a los que dirigir dichas campañas.

* Respecto de la exactitud de los datos:

En general, los datos de los usuarios son exactos y se encuentran actualizados.

No obstante, se ha detectado el caso de alguna entidad que almacena en el sistema de análisis de riesgos asociado a las solicitudes de créditos, el resultado de las consultas a ficheros de incumplimiento de obligaciones dinerarias constituidos al amparo del artículo 29 de la LOPD. En el caso encontrado, la entidad no procede a actualizar dicha información ni a borrarla una vez se finaliza la tramitación de dicha solicitud, por lo que se corre el riesgo de que con el paso del tiempo la información recabada no responda con veracidad a la situación actual del afectado, pudiendo incurrir en un incumplimiento del artículo 4.3 de la LOPD.

* Respecto de la cancelaciones de datos:

El procedimiento establecido en la práctica en las entidades analizadas consiste en que cuando un cliente procede a la cancelación de todas sus cuentas sin que haya solicitado explícitamente la cancelación de sus datos personales, la entidad procede a cancelar dichas cuentas pero conservando aquellos con el fin de acreditar la existencia de la relación contractual durante los plazos legales previstos. En algunos casos la entidad procede de forma adicional a excluirle de futuras promociones comerciales, no así en otros casos, al considerar que puede seguir realizando esta actividad.

En el caso de que el cliente haya solicitado además la cancelación de sus datos personales, la entidades proceden a bloquear dichos datos mediante su marcado, restringiendo, en todo caso, su futura inclusión en campañas comerciales.

Durante el proceso de alta como cliente no siempre llega a producirse un alta efectiva del mismo, quedando el proceso interrumpido, cuando no paralizado indefinidamente, sin que quede activada la cuenta del cliente. En este sentido, se ha detectado que algunas entidades no cancelan en ningún momento los datos de aquellos solicitantes para los cuales no se completó el proceso.

Derecho de información en la recogida de datos y consentimiento del afectado (artículos 5 y 6).

En general, la persona que se dirige a una entidad del sector recibe información acerca del tratamiento de sus datos por distintas vías: Internet, teléfono y a través del contrato en papel de apertura de cuenta.

La información facilitada a través de Internet y de los contratos recoge que los datos recabados van a ser incorporados a un fichero, indicando la denominación social y dirección del responsable del mismo, así como de la posibilidad que tiene la persona de ejercer sus derechos de acceso, rectificación y cancelación en consonancia con la LOPD.

Se ha detectado, en alguna ocasión, que la información facilitada difiere dependiendo del medio consultado o que se encuentra diseminada en diferentes ubicaciones sin que ninguna de ellas la recoja en su totalidad. En un caso concreto figura incluso información que puede ser contradictoria: a través de Internet se informa de posibles cesiones a un grupo de empresas y a través de los contratos en papel de posibles cesiones a otro grupo de empresas diferente.

Así mismo, y en relación con lo anterior, también se ha detectado que la información no siempre resulta fácilmente accesible para el usuario por no estar integrada en el proceso de recogida de los datos personales.

En general, la información que se ofrece a clientes y potenciales clientes recoge que se van a utilizar sus datos con fines comerciales para ofrecer productos financieros. No obstante, dicha información no va, por lo general, acompañada de un mecanismo que permita oponerse a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

Así mismo, se ha detectado la práctica de incluir cláusulas que informan de forma genérica sobre cesiones a "empresas del grupo" para "la oferta y contratación de otros productos y servicios" sin que se concrete con mayor detalle la información aportada y sin que se recoja en el propio contrato ningún procedimiento que permita expresar dicha oposición mediante una casilla como la mencionada anteriormente.

Otro aspecto a señalar es que no siempre se especifican cuales de los datos recabados son obligatorios y cuales no. Así, por ejemplo, una entidad recoge el dato del número de hijos sin especificar si es voluntario o no y cual es la finalidad de recabar dicha información.

Se ha detectado también la realización de tratamientos donde se evalúa la solvencia del cliente mediante el acceso a ficheros comunes de terceros de incumplimiento de obligaciones dinerarias constituidos al amparo del artículo 29 de la LOPD. En el caso de una entidad la información que se aporta es que se realiza un "proceso de evaluación patrimonial o crediticio o scoring para lo cual se le solicitarán una serie de datos que ayudarán a determinar el alcance de su solvencia".

También, se ha detectado la realización de segmentaciones o perfiles de clientes con fines comerciales, a partir de la información personal y comercial que consta en los ficheros de la entidad, sin que se informe de ello a los clientes y sin que éstos puedan, por lo tanto, oponerse a dicho tratamiento.

Las entidades analizadas utilizan como práctica habitual grabar las conversaciones que se producen en los accesos a través de los servicios telefónicos. Es práctica general que se informe de ello a los clientes a través de las condiciones contractuales.

Finalmente, cabe señalar la prestación, por parte del algunas entidades, del servicio denominado agregador financiero por el cual la entidad ofrece al usuario la posibilidad de acceder a través de una única consulta a todas las posiciones que el usuario pueda tener con diferentes entidades financieras. Para ello, el usuario debe de facilitar a la entidad prestataria del servicio las claves de acceso a las restantes entidades.

Datos especialmente protegidos (artículos 7 y 8).

No se ha constatado la existencia de datos especialmente protegidos en los ficheros de clientes y potenciales clientes de las entidades analizadas.

Seguridad de los datos (artículo 9 y RD 994/1999)

Uno de los aspectos esenciales y más significativos de la banca a distancia es precisamente la identificación y autenticación de los clientes dado que no existe presencia física de los mismos. Por esta razón, se habilitan procedimientos técnicos para que de forma remota los clientes puedan consultar sus posiciones e incluso realizar transacciones económicas y contratar productos financieros.

En este sentido, se han analizado dos situaciones consideradas especialmente relevantes: el proceso de contratación a distancia de la cuenta de cliente y el acceso a distancia del cliente a los productos y servicios que le ofrece la entidad.

Respecto del proceso de alta como cliente, se inicia básicamente mediante una petición realizada por el solicitante ya sea por teléfono o por Internet, donde tras aportar ciertos datos básicos iniciales la entidad asigna ya un Código de Cuenta de Cliente en estado de preactivado, así como las claves de identificación y autenticación en los casos en los que el usuario puede elegirlas, desencadenándose a continuación un proceso de remisión de documentación y de las claves al titular o titulares.

Para la remisión de las claves se utilizan, en general, servicios de mensajería con acuse de recibo e identificación fehaciente de destinatario, o, en su defecto, correo ordinario con mecanismos posteriores de activación dirigidos a identificar inequívocamente al cliente.

Seguidamente, se inicia un proceso de recogida y seguimiento de la documentación que debe remitir el cliente a la entidad (contrato firmado, fotocopia del NIF, etc.). Si este proceso no llega a completarse no se activa la cuenta del cliente.

Respecto del acceso a distancia del cliente a los productos y servicios que le ofrece la entidad, se constata la existencia de tres estadios distintos: la identificación, la autenticación y la firma.

La identificación permite a la entidad saber quien es el cliente que se pone en contacto con ella y se produce mediante la aportación (telefónica o por Internet) de un código de usuario o secuencia alfanumérica de entre 6 y 15 caracteres que es única para cada cliente (en ocasiones se utiliza como código de usuario el NIF de la persona e incluso, en algún caso y por teléfono, basta con aportar el número de teléfono del cliente y su nombre). Siempre que se facilita el código de identificación a través del teléfono queda registrado en las grabaciones de las conversaciones de los operadores.

La autenticación es el primer control que realiza la entidad para garantizar que la persona que se ha identificado es quien dice ser. La autenticación se produce mediante la aportación de una parte o de la totalidad de una clave de autenticación formada por entre 4 y 12 caracteres alfanuméricos y que, en principio, únicamente debiera conocer el cliente y el sistema de gestión de claves de la entidad. Cuando se elige a través de teléfono queda registrada en las grabaciones de las conversaciones con los operadores.

Una vez superada la identificación y autenticación, es práctica general que la entidad permita al cliente consultar sus posiciones, así como solicitar la realización de operaciones que suponen movimientos de capital: transferencias, contratación de otros productos, etc. Para poder culminar estas operaciones, en las que se produce un cambio en las posiciones del cliente, la entidad exige además un control adicional o firma.

La firma se produce mediante la aportación de una parte si no la totalidad de una clave de firma que únicamente debe de conocer el cliente y el sistema de gestión de claves de la entidad. La clave de firma suele formarse por una secuencia alfanumérica de entre 8 y 12 caracteres o bien mediante una tarjeta que contiene impresos una serie de secuencias numéricas. A través del teléfono se puede solicitar su emisión e incluso su cambio pero no asignarla de viva voz a través de un operador que conozca la identificación del cliente.

El procedimiento descrito puede presentar, en la práctica, algunos riesgos respecto de la identificación inequívoca del cliente, no tanto por la tecnología utilizada como por los procedimientos establecidos sobre dicha tecnología, así como, por la información facilitada a los usuarios en algún caso, o por la conducta de los propios usuarios en otros.

Finalmente, no se ha detectado en las entidades analizadas la utilización de esquemas de certificación y firma electrónica tipo PKI (Infraestructura de Clave Pública) para el acceso de los clientes a los servicios ofrecidos por las entidades analizadas. Estos esquemas de seguridad, aun no siendo legalmente exigibles, ofrecen la garantía de disponer de certificados realizados por terceros, distintos de los fabricantes, garantizando determinados niveles de seguridad.

Deber de secreto (artículo 10).

En las relaciones contractuales que rigen las prestaciones de servicios para las entidades analizadas y que implican el acceso por parte de las empresas prestatarias a los datos personales de clientes de las entidades, se recogen cláusulas que exigen la debida confidencialidad sobre los datos a los que se accede.

No obstante, se han detectado entidades que no recogen en los contratos con su personal cláusulas que les obliguen a guardar el deber de secreto respecto de los datos personales a los que tengan acceso como consecuencia de su trabajo en la entidad.

También se ha detectado el caso de una entidad donde en la página web que se utiliza para el alta del cliente si se facilita al menos el NIF de una persona que ya es cliente, e independientemente de los datos adicionales que se aporten, ofrece los datos identificativos que en el fichero de clientes figuran asociados a dicho NIF.

Cesiones de datos (artículo 11).

Si bien no se han detectado en las entidades inspeccionadas cesiones de datos a terceros, sí se ha constatado, como ya se ha indicado anteriormente, algunos contratos con cláusulas que informan de forma genérica sobre cesiones a "empresas del grupo" para "la oferta y contratación de otros productos y servicios", sin que se concrete más la información aportada haciendo referencia a las finalidades de la cesión y sin que se recoja en el propio contrato ningún procedimiento que permita expresar la oposición a dicha cesión, como por ejemplo la inclusión de una casilla al efecto.

Acceso a los datos por cuenta de terceros (artículo 12).

En general, la mayoría de las prestaciones de servicios analizadas se encuentran plasmadas en contratos por escrito que recogen la finalidad de la prestación, siendo habitual que incorporen lo estipulado en el artículo 12 de la LOPD.

No obstante, se han detectado algunos contratos que no recogen todos los requisitos exigidos en el artículo 12 como por ejemplo las medidas de seguridad a que se refiere dicho artículo y que el encargado del tratamiento está obligado a implementar, o el destino final de los datos personales una vez ha finalizado la prestación contractual, entre otros.

Impugnación de valoraciones (artículo 13).

No se han detectado en las entidades estudiadas que se tomen decisiones con efectos jurídicos que afecten a personas físicas y que tengan como fundamento únicamente un tratamiento de datos destinado a evaluar determinados

aspectos de la personalidad del individuo.

No obstante, conviene señalar que algunos de los tratamientos analizados, como por ejemplo los de scoring, si que podrían, en determinadas circunstancias, llevar a tomar decisiones automáticas teniendo como fundamento únicamente un tratamiento sobre aspectos de la personalidad. En este sentido, dichos tratamientos quedarían plenamente sujetos a lo prevenido en el citado artículo.

Derecho de las personas: acceso, rectificación, cancelación y oposición. (artículos 15 y 16).

Las entidades inspeccionadas informan a los usuarios de la posibilidad de ejercer estos derechos al tiempo que cuentan con procedimientos definidos para su ejercicio, siendo habitual que dichos procedimientos recojan lo dispuesto en la Instrucción 1/1998 de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Se ha constatado que el derecho ejercido mayoritariamente por los usuarios de estos servicios de manera formal es el derecho de oposición al tratamiento de sus datos personales con fines de promoción comercial.

Creación, notificación e inscripción en el Registro de la APD (artículos 25 y 26).

Las entidades analizadas han procedido a la inscripción en el Registro General Protección de Datos de la APD de sus ficheros de clientes y potenciales clientes.

Datos incluidos en fuentes accesibles al público (artículo 28).

Si bien las entidades analizadas no publican ningún repertorio susceptible de considerarse fuente accesible al público, sí se ha constatado la realización, por parte de aquellas, de compras o alquileres de datos personales suministrados por terceros y cuyo origen último resultan fuentes accesibles al público, siendo utilizados dichos datos con fines de publicidad y de prospección comercial.

En este sentido se han detectado dos modalidades de actuación bien diferenciadas:

a) En unos casos, la entidad financiera procede al alquiler de listados para usos concretos a empresas especializadas en suministrar direcciones procedentes de fuentes accesibles al público. La solicitud de datos se realiza en base a diferentes criterios socioeconómicos y demográficos facilitados por las empresas suministradoras y que obtienen del cruce de los datos personales básicos que figuran en diferentes fuentes de acceso público con datos socioeconómicos agregados en función de datos geográficos.

En estos casos, la entidad recibe un listado que contiene básicamente nombre, apellidos, sexo y domicilio, a partir del cual se confecciona un envío promocional, procediendo posteriormente al borrado de dicho listado, no quedando datos personales del listado en los ficheros de la entidad.

b) En otros casos, la entidad financiera procede a la constitución de un fichero propio con un gran volumen de registros mediante la acumulación de diferentes compras de ficheros a lo largo del tiempo. La finalidad de este fichero no es la de realizar una campaña concreta sino la de servir de base para la realización de diferentes campañas, como por ejemplo envíos promocionales nominativos a los domicilios del área de influencia de una sucursal bancaria, etc.

Dentro de esta última modalidad se ha detectado una entidad cuyo fichero presenta una doble problemática:

En primer lugar, y relacionado con la antigüedad de los datos, cabe señalar que la LOPD introduce respecto de las fuentes accesibles al público una limitación temporal. En este sentido, el artículo 28.3 establece que "Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique. En el caso de que se obtenga por vía telemática una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.".

Por lo expuesto, el citado fichero corre el riesgo de recoger actualmente datos que si bien originariamente quedaban amparados por proceder de fuentes accesibles al público, en la actualidad pueden haber perdido dicho amparo, ya sea por haber sido cancelados de las mismas o por haber perdido éstas dicho carácter.

En segundo lugar, y relacionado con la estructura de datos del fichero, cabe señalar que la estructura diseñada es mucho más amplia que la necesaria para albergar aquel, lo que ha propiciado un enriquecimiento de los datos en algunos registros en los que, si bien en un porcentaje mínimo, se recogen datos que difícilmente tienen su origen en fuentes accesibles al público y sobre los que pudiera no existir el correspondiente consentimiento dado que no existe relación contractual con dichas personas. Entre estos datos se encuentran por ejemplo el DNI, tipo de vivienda, estado civil, número de hijos, tipo de actividad particular, profesión, país de nacimiento, país de residencia, nivel académico, indicador de fallecido, etc.

Prestación de servicios de información sobre solvencia patrimonial y crédito (artículo 29).

En general, la mayoría de las entidades disponen de acceso a ficheros comunes relativos al incumplimiento de obliga-

ciones dinerarias, comunicando al fichero común los impagos producidos y consultando en el mismo las posibles deudas de sus clientes. En general, las entidades consultan estos ficheros como parte de un tratamiento de análisis de la solvencia del cliente cuando se produce la contratación de algún producto financiero con riesgo económico para la entidad (contratación de productos de activo, emisión de tarjetas, etc.).

Así por ejemplo, se ha detectado el caso de una entidad donde la apertura de la primera cuenta va asociada a la emisión de una tarjeta de débito al primer titular, por lo que la entidad procede de forma sistemática a realizar un análisis de solvencia de todos los primeros titulares. Dicho análisis es repetido es ocasiones con el fin de excluir a clientes de determinadas campañas comerciales en las que se promocionan determinados productos de activo.

Tratamientos con fines de publicidad y de prospección comercial (artículo 30).

En las entidades analizadas se ha detectado que existe un procedimiento establecido para excluir de la remisión de publicidad a aquellos clientes que han ejercido su derecho de oposición. Se constata además, que la oposición a este tratamiento es el principal derecho ejercido por los usuarios de los servicios bancarios.

Como ya se ha señalado anteriormente, en general se informa que los datos recabados se van a utilizar con fines comerciales para promociones de productos financieros. No obstante, dicha información no va por lo general acompañada de un mecanismo que permita oponerse a dicho tratamiento en el momento de la recogida de datos, como por ejemplo la inclusión de una casilla al efecto.

Movimiento internacional de datos: Norma general y Excepciones (artículos 33 y 34).

No se ha detectado que se realicen transferencias internacionales de datos en las entidades bancarias inspeccionadas que no estén amparadas por la excepción d) del artículo 34.

Al cierre de la presente memoria no se ha finalizado la elaboración de las correspondientes recomendaciones, por lo que de las mismas se dará cuenta en la próxima memoria.

2.2.5. Registro de Aceptaciones Impagadas (R.A.I.)

Dentro de los Planes Sectoriales de Oficio, se procedió a analizar el grado de adecuación a la Ley Orgánica 15/1999, de 13 de diciembre (LOPD), y normativa que la desarrolla, del fichero RAI (Registro de Aceptaciones Impagadas), cuyo responsable es el CENTRO DE COOPERACIÓN INTERBANCARIA, en adelante CCI.

CCI es una asociación sin ánimo de lucro que tiene por objeto el cumplimiento de, entre otros, el siguiente fin: *"Servir como medio para la cooperación interbancaria con el fin de agilizar el intercambio y liquidación de operaciones del sector, mediante la utilización de los medios que en cada caso resulten más convenientes con vistas a aumentar al máximo la eficacia y reducir al mínimo los costes".*

CCI es la entidad responsable del fichero RAI cuya finalidad es la de proporcionar información sobre la solvencia de las personas. Está constituido como fichero común en el que se consolidan los datos personales de los ficheros propios de los acreedores que contienen aquellos datos que se generan como consecuencia de las relaciones económicas mantenidas con el afectado.

Las normas de funcionamiento del fichero RAI se encuentran descritas en el anexo a su Circular 2/2000, por la que se actualiza funcional y operativamente la circular 84/91 del extinguido Consejo Superior Bancario, en cuyo capítulo II, se indica que *"el Sistema tiene como objetivo fundamental constituir y poner a disposición de todas las entidades de crédito participantes la información relativa al RAI, a nivel nacional, facilitada por el conjunto de entidades de crédito participantes, a través de tratamientos informáticos centralizados"* .

El fichero RAI contiene datos relativos a deudas derivadas del impago de documentos como letras de cambio, recibos aceptados, pagarés cambiarios, pagarés de cuenta corriente y cheques de cuenta corriente que han sido previamente aceptados por personas físicas o jurídicas, en una proporción del 22% y 78%, respectivamente.

Los datos incluidos en el fichero RAI son obtenidos únicamente a partir de las entidades informantes asociadas a CCI, y son facilitados a dicha entidad a través de entidades presentadoras / receptoras, aunque en ocasiones CCI actúa como entidad presentadora. A este respecto se entiende por:

a) Entidad informante:

Es la entidad bancaria que aporta los datos para su incorporación al RAI, siendo la responsable de la validez y calidad de los mismos, así como de su actualización cuando proceda.

b) Entidad presentadora / receptora:

Es la entidad bancaria que transmite al centro de proceso, la información que aporta ella misma como entidad informante y del resto de entidades informantes representadas por ella en el sistema. Así mismo, es la entidad que recibe del centro de proceso, la información facilitada por todas las entidades informantes, para su utilización exclusiva por

ella misma y el resto de entidades a las que representa.

Existen dos modalidades distintas para que las entidades informantes puedan consultar los datos incluidos en el RAI. Dichas modalidades son:

a) Acceso a la copia del fichero RAI disponible en cada entidad presentadora / receptora.

b) Acceso on-line al fichero completo desde entidades informantes.

Finalmente, se ha constatado que CCI tiene suscrito un contrato de prestación de servicios con una empresa que realiza la gestión informática del fichero RAI, (en adelante el encargado del tratamiento), actuando, por tanto, como encargado del tratamiento de dicho fichero, motivo por el cual se han realizado inspecciones en ambas entidades.

* Conclusiones de la inspección

De las actuaciones efectuadas por la Inspección de Datos en las dos entidades, se desprenden las siguientes conclusiones:

* *Respecto a la calidad de datos*

CCI dispone de un sistema de actualización de los datos que garantiza que, tanto el fichero RAI central como las diversas copias existentes en las entidades presentadoras / receptoras, sean exactamente iguales.

En cuanto a la cancelación de datos se refiere, en el fichero RAI no se ha detectado la existencia de deudas con fecha de vencimiento superior a 30 meses. Sin embargo, dicho fichero puede contener datos relativos a deudas ya satisfechas por el deudor. Este hecho puede darse cuando los pagos se realizan de forma directa entre el deudor y el acreedor, y ninguno de ellos lo comunica al RAI ni a la entidad informante, que no tiene conocimiento del pago.

Además, CCI dispone de un fichero para gestionar el ejercicio de los derechos de los afectados.

Por otra parte, los datos relativos a deudas que se dan de baja por diversos motivos, aunque son borrados del fichero RAI, son incluidos de forma permanente desde 1994 en dos ficheros Históricos (uno relativo a bajas dadas por las entidades informantes y el otro relativo a bajas automáticas por tiempo de permanencia en RAI superior a 30 meses), cuyo objetivo es atender requerimientos legales.

Así mismo, dispone de un fichero de Facturación que contiene datos de nombre y apellidos de personas físicas sobre los que se ha realizado una consulta de forma on-line por las entidades asociadas. En ocasiones podría contener también el DNI de los afectados así como la provincia. Los datos permanecen en este fichero durante el año en curso más el año anterior. En este fichero se pueden encontrar datos relativos a personas físicas que no hayan formado parte en ningún momento del fichero RAI.

* *Respecto a la información facilitada al interesado*

El encargado del tratamiento dispone de un procedimiento que garantiza el envío de las correspondientes notificaciones de inclusión en el fichero RAI a los interesados, incluso en un plazo inferior al máximo de 30 días legalmente establecido. Dicho procedimiento controla también las devoluciones habidas, así como el motivo de la devolución.

* *Deber de secreto*

La entidad encargada del tratamiento en el contrato que suscribe con sus empleados, contempla la confidencialidad con la que debe tratarse la información a la que acceden en el desempeño de sus funciones.

Sin embargo, las personas que prestan sus servicios en CCI no han firmado ningún compromiso de confidencialidad, lo que no es necesario según el representante de la entidad por ser poco numerosas.

* *Comunicación de datos*

Dado el funcionamiento del fichero RAI, los datos incluidos en el mismo por cada entidad informante, son conocidos al menos por las entidades presentadoras / receptoras y por las entidades informantes adheridas al sistema de acceso on-line.

Los afectados no conocen la cesión de datos habida entre CCI y las entidades presentadoras / receptoras en el momento en que se produce. Únicamente conocen este hecho cuando ejercen su derecho de acceso ante CCI, con cuya respuesta se adjunta la relación de entidades informantes que podrían disponer de sus datos, sin poder precisar cuál de ellas ha accedido finalmente a los mismos para su consulta.

* *Acceso a los datos por cuenta de terceros*

Entre CCI y la entidad encargada del tratamiento existe un contrato de prestación de servicios suscrito en fecha 31/1/95. En dicho contrato, se cita la LORTAD por razón del momento en que se suscribió, y no se hace referencia expresa a lo

indicado en el artículo 12 de la LOPD, que además de referirse a la utilización de los datos de carácter personal por parte del encargado del tratamiento, también establece la obligación de estipular en el contrato las medidas de seguridad que deben observarse conforme a lo indicado en el artículo 9 de la citada Ley Orgánica.

* *Derechos de acceso, rectificación y cancelación*

Como se ha señalada anteriormente, CCI recoge en un fichero independiente del fichero RAI los datos relativos a las personas que ejercen sus derechos de acceso, rectificación y cancelación, conteniendo datos de reclamante, población y provincia correspondientes a personas físicas que pueden no haber estado nunca incluidos en el fichero RAI.

Ante el ejercicio del derecho de acceso de los afectados, el único fichero consultado es el RAI, no informando de la posible existencia de sus datos en el fichero independiente arriba referido, ni en los dos ficheros históricos también mencionados.

Tampoco se informa de la posible existencia de datos en el fichero de facturación, en el que también se pueden encontrar datos de personas físicas (nombre y apellidos y, en ocasiones, incluso su DNI) cuyos datos nunca hayan estado incluidos en el RAI. A este respecto debe señalarse que cuando una entidad realiza una búsqueda por nombre y apellidos de algún afectado de forma on-line en el RAI central, el sistema devuelve los registros coincidentes con los parámetros de búsqueda indicados por la entidad, desconociendo CCI incluso si alguno de ellos es el buscado ya que no queda constancia de la consulta específica que realiza la entidad. Podría darse el caso de que ninguno de los registros ofrecidos por CCI sea el buscado por la entidad.

Debido al sistema de distribución en cascada de la información contenida en el fichero RAI, CCI no está en disposición de precisar qué entidades determinadas han consultado los datos de un afectado concreto.

* *Registro General de Protección de Datos*

CCI únicamente tiene inscrito en el Registro General de Protección de Datos su fichero RAI, el cual tiene asignado el código de inscripción 1942261580.

El resto de los ficheros citados no se encuentran inscritos.

* *Movimiento Internacional de datos*

No se ha constatado que se produzcan movimientos internacionales de datos.

* *Medidas de seguridad*

La transmisión electrónica de datos entre el encargado del tratamiento y las entidades asociadas al sistema se realiza de forma cifrada, siendo distinto para cada entidad el algoritmo utilizado.

Desde diciembre de 2000 y al objeto de controlar la posible circulación de copias ilegales del fichero RAI, CCI ha establecido un sistema de control que, en el supuesto de darse aquella circunstancia, permitiría detectar la entidad de la que procede la copia ilegal.

Conforme a la tipología de datos contenida en el fichero RAI, el nivel de seguridad asignado al mismo es el medio, por lo que la empresa encargada del tratamiento dispone de un Documento de Seguridad que, según se ha comprobado, se ajusta a lo indicado en los artículos 8 y 15 del Reglamento de Medidas de Seguridad respecto a las medidas de nivel básico y medio, respectivamente.

En relación con las medidas de seguridad de nivel básico y medio especificadas en el citado Reglamento, se ha designado un responsable de seguridad, las funciones y obligaciones del personal se encuentran definidas, se dispone de una auditoría de seguridad, existe una relación de perfiles de acceso de usuarios así como normas respecto a la utilización de contraseñas, se controla el acceso físico al Centro de proceso de datos, existe normativa para la gestión de soportes y la realización de copias de respaldo, disponen de un registro de incidencias.

Al finalizar el año 2001 estaban elaborándose las correspondientes recomendaciones de la inspección realizada, de las que se dará cuenta en la Memoria del año 2002.

2.2.6. Otros ficheros de información sobre solvencia patrimonial y crédito

Durante el año 2001 se han presentado ante la Agencia de Protección de Datos un número significativo de denuncias relativas la inclusión de datos personales en un nuevo fichero común que se ha puesto en marcha, de información sobre solvencia patrimonial e incumplimiento de obligaciones dinerarias. Ante esta circunstancia, y manteniendo el criterio que ha llevado a la APD a realizar en el pasado inspecciones sectoriales sobre otros ficheros de características semejante, se procedió a realizar una inspección de oficio sobre el mismo. A continuación, se exponen las principales conclusiones de las actuaciones de inspección realizadas.

Inscripción en el Registro General de Protección de Datos

La entidad responsable tiene dos ficheros inscritos en el Registro General de Protección de Datos: El fichero común multisectorial para la prestación de servicios sobre solvencia patrimonial y crédito y el fichero de gestión del servicio de protección al consumidor.

En la inscripción del primero consta una transferencia internacional de datos, siendo su destinatario una sociedad ubicada en Francia.

Comunicaciones de datos

La actividad fundamental del responsable del fichero se centra en facilitar información sobre solvencia patrimonial y crédito, relativa al incumplimiento de obligaciones dinerarias, tanto de personas físicas como jurídicas.

Para adherirse al servicio no es necesario que la sociedad pertenezca a un determinado sector de actividad, pero sí debe estar dispuesta a facilitar la información que disponga relativa a las operaciones que hayan resultado impagadas. Asimismo, debe tener como principal actividad la financiación de bienes y servicios o de operaciones que permitan la compra de productos a crédito.

Las entidades que se adhieren al servicio, denominadas "entidades suscriptoras", pueden acceder al fichero a través de emulación, mediante conexión directa a los equipos informáticos o bien a través de entregas de soportes magnéticos. Las consultas pueden realizarse utilizando como criterio de búsqueda el número de DNI, no estando disponible la consulta utilizando el nombre y apellidos.

Accesos a los datos por cuenta de terceros

El titular del fichero ha suscrito un acuerdo con una sociedad para que ésta le preste servicios como encargado del tratamiento. En dicho acuerdo se recogen estipulaciones específicas relativas a la confidencialidad de los datos, al deber de guardar secreto y al establecimiento de medidas de seguridad, recogiéndose en las mismas las exigencias del artículo 12 de la Ley de Protección de Datos y especificándose que deberán adoptarse las medidas de seguridad de nivel medio.

Asimismo, han suscrito otros contratos, entre los que se encuentran: uno para la realización de todas las actividades necesarias para la adecuada gestión del Servicio de Protección al Consumidor (gestión de los derechos de acceso, rectificación, oposición y cancelación de los consumidores, así como la atención telefónica de todo tipo de consultas o solicitudes realizadas por los consumidores) y otro para la prestación del servicio de impresión y envío por correo ordinario de las notificaciones de inclusión en el fichero.

El responsable del fichero también ha suscrito un acuerdo de prestación de servicios de alojamiento de ficheros con una entidad, cuyo domicilio social se encuentra en París (Francia). Asimismo, ha suscrito con una entidad, con domicilio social en Inglaterra, un acuerdo de prestación de servicios y mantenimiento del software que utiliza para la gestión del fichero. En cada caso se ha incorporado un anexo al contrato principal, en el que se establecen las condiciones en las que se alojarían o se utilizarían los datos de dicho fichero, recogiéndose estipulaciones relativas al tratamiento de los datos de carácter personal y a la seguridad de los datos, conforme a lo estipulado en la Ley de Protección de Datos de Carácter Personal y al Reglamento de medidas de seguridad. Posteriormente, se ha suscrito un nuevo acuerdo con la sociedad inglesa, tras la publicación de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, con el fin de adecuarse a las prescripciones legales sobre transferencias internacionales de datos.

Calidad de los datos

* Procedimientos de actualización

Las entidades suscriptoras facilitan los datos en soportes magnéticos que pueden ser entregados a través de servicios de mensajería o de transferencia de ficheros. Las entidades suscriptoras están obligadas a comunicar datos, al menos, una vez al mes.

La identificación de los registros para proceder a su alta o actualización se efectúa teniendo en cuenta los siguientes campos: código de suscriptor, código del fichero (código que identifica unívocamente a un producto para un determinado suscriptor) y número de operación.

* Cancelación de los datos

La información se mantiene en el fichero durante un plazo no superior al establecido legalmente, valor que es configurable a través de un parámetro disponible en el aplicativo. La fecha que se tiene en cuenta para dicho cálculo es la del último vencimiento impagado.

Los datos de aquellos incumplimientos que hayan sido satisfechos por el deudor (anotaciones de "saldo cero") son eliminados del fichero, a través de un proceso de prevalidación.

Las bajas de operaciones o intervinientes registrados en el fichero tienen que ser comunicados por las entidades suscriptoras en un fichero diferente, ya que existe un proceso específico para proceder a las cancelaciones.

Envío de notificaciones de inclusión en el fichero

El fichero de notificaciones de inclusión se genera en el propio proceso de actualización. Posteriormente, dicho fichero se envía por vía telemática, generándose un fichero de notificaciones reducido que contiene los datos necesarios para proceder a la impresión de las notificaciones de inclusión.

Las notificaciones se envían utilizando correo ordinario, almacenándose las cartas devueltas durante un plazo de tres años calculado desde la fecha de su devolución.

Las notificaciones de inclusión en el fichero recogen, entre otros, los siguientes datos: nombre del suscriptor, número de DNI o NIF del interviniente, así como su nombre, apellidos y dirección, naturaleza de la intervención, fecha de la inclusión en el fichero, saldo impagado en el alta y fecha de impresión de la carta.

Procedimientos respecto del ejercicio de los derechos regulados en la LOPD

Con el fin de atender las solicitudes de los afectados de ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, se ha creado un Servicio de Protección al Consumidor cuya gestión ha sido contratada a una empresa externa, tal y como ya se ha puesto de manifiesto anteriormente.

El medio utilizado para contestar a los afectados es el mismo que éstos hayan empleado para dirigirse al Servicio de Protección al Consumidor.

Con el fin de dar cumplimiento a lo dispuesto en el apartado 3 del artículo 29 de la Ley de Protección de Datos, se almacena durante dos años información de las consultas previas realizadas por los suscriptores sobre la existencia de datos de los afectados en el fichero. Esta información no se encuentra accesible para las entidades suscriptoras.

Asimismo, el Servicio de Protección al Consumidor tiene habilitada una transacción que permite efectuar de forma inmediata la cancelación de una operación o interviniente del fichero.

Movimientos internacionales de datos

Como se ha puesto de manifiesto anteriormente, el fichero se encuentra ubicado en las instalaciones de una sociedad en Francia, en virtud de un contrato de prestación de servicios de alojamiento de ficheros.

Asimismo, una sociedad, con domicilio social en Inglaterra, tiene acceso al fichero con el fin de dar cumplimiento al contrato por el cual realiza la prestación de servicios y mantenimiento sobre el software que se utiliza para la gestión de este fichero.

Medidas de seguridad

Tanto el responsable del fichero como el encargado del tratamiento disponen de sus respectivos Documentos de Seguridad que, en general, cumplen con lo estipulado para los ficheros de nivel de seguridad medio en el Reglamento de medidas de seguridad.

También se ha verificado que para acceder al fichero es necesario identificarse y autenticarse, mediante la introducción de un nombre de cuenta, usuario y contraseña.

En la inspección también se verificó la existencia de un registro de soportes y de medidas de seguridad física, en las instalaciones del encargado del tratamiento.

A la fecha de cierre de la Memoria no se habían elaborado las oportunas recomendaciones, las cuales se dictarán durante el año 2002.

3. ACTUACIONES MÁS RELEVANTES EN EL ÁMBITO DE LOS FICHEROS DE TITULARIDAD PÚBLICA

3.1. Administración General del Estado

Dentro de las denuncias presentadas por los ciudadanos ante la Agencia de Protección de Datos en el transcurso del año 2001, un cinco por ciento aproximadamente han sido reclamaciones por posibles infracciones de los responsables de ficheros cuya titularidad corresponde a las Administraciones Públicas.

Los Organismos de la Administración General del Estado sobre los que se han realizado investigaciones por parte de la Inspección de Datos han sido los siguientes:

Agencia Estatal de Administración Tributaria.

Tesorería General de la Seguridad Social

Instituto Nacional de la Seguridad Social

Instituto Nacional de Empleo

Dirección General de Tráfico

Museo de América

Entidad Publica Empresarial Correos y Telégrafos

Ministerio de Administraciones Públicas

Boletín Oficial del Estado

Ministerio del Interior

Por todo ello, la Agencia ha procedido a la apertura tanto de tutelas de derecho como de actuaciones previas de inspección cuya tramitación y resolución se han realizado dentro del año 2001. Asimismo, se ha procedido a dictar resoluciones de algunas actuaciones comenzadas el año anterior. La mayor parte de los hechos denunciados hacen referencia a la posible vulneración del deber de secreto previsto en el artículo 10 de la Ley 15/1999.

3.1.1. Resoluciones más relevantes dictadas por el Director de la Agencia de Protección de Datos.

Durante el ejercicio del año 2001, la Agencia de Protección de Datos ha dictado resolución de procedimientos de infracción de Administraciones Públicas, algunos de los cuales se iniciaron en el ejercicio anterior. De todos ellos merecen especial mención las que a continuación se exponen

Entidad Empresarial Correos y Telégrafos

Durante el año 2000 la Agencia procedió a instruir un procedimiento sancionador a la Entidad Publica Empresarial Correos y Telégrafos por posible cesión de datos personales y datos médicos a tres empresas encargadas de la realización de los llamados "servicios médicos concertados" que realizaban funciones relativas a visitas domiciliarias y de control en materia de salud laboral. En la instrucción del procedimiento se ha comprobado que la citada entidad empresarial tiene suscritos contratos para la prestación de un servicio médico de apoyo para la mejora de la atención asistencial al personal de Correos y Telégrafos, concretamente en la gestión de las ausencias laborales por motivos de salud. Para ello, suministra a las empresas una relación de bajas laborales y de altas producidas donde se incluyen datos personales.

Ahora bien, independientemente de la calificación de dichos datos, la infracción imputada es la cesión o comunicación de datos fuera de los casos permitidos. En este sentido, para determinar si tal cesión es o no ajustada a la normativa sobre protección de datos personales, es preciso tener en cuenta no sólo lo específicamente previsto en la LOPD, sino también lo dispuesto en el artículo 20.4 del Estatuto de los Trabajadores, el cual dispone que *el empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones.* Este precepto habilita a la Entidad Publica Empresarial Correos y Telégrafos a controlar el absentismo laboral de sus trabajadores, permitiéndole comprobar la autenticidad de la baja médica. Por ello, la cuestión se reduce a determinar si para realizar las verificaciones, puede encargarse a un tercero la prestación de ese servicio.

En el presente caso, dado que la Entidad Pública Empresarial Correos y Telégrafos ha demostrado que existen varios contratos escritos de prestación de servicios firmados con distintas entidades y que dichos contratos fueron formalizados durante la vigencia de la Ley Orgánica 5/1992, de 29 de octubre y que en los mismos se establece que *los contratistas deberán (.....) adoptar las cautelas necesarias para que la transmisión de los datos médicos y confidenciales se ajusten a la Ley Orgánica 5/92 y que se considerará confidencial frente a terceros cualquier información recibida por ambas partes al amparo de este contrato, incluso después de haberse extinguido el mismo*, debe entenderse que existe una prestación de servicios amparada por el artículo 27 de la LORTAD y por el actual artículo 12 de la LOPD y no una cesión ilegal de datos, habida cuenta de que no se han utilizado los datos para fines distintos de los estipulados en el contrato de servicios y que los datos no han sido cedidos a terceros, habiéndose previsto las garantías adecuadas al establecerse cláusulas de confidencialidad. No obstante la denuncia presentada dio lugar a la tramitación de un expediente sancionador respecto de la entidad privada que prestó el servicio.

Museo de América

También, se procedió a la instrucción de un procedimiento contra el Museo de América adscrito al Ministerio de Educación, Cultura y Deporte por posible vulneración de los artículos 5 y 20 de la Ley Orgánica 15/1999. En el curso del procedimiento se acreditó que el Museo, a través de un formulario, recaba datos cumplimentados por las personas interesadas en recibir información sobre sus actividades que posteriormente son registrados en un fichero automatizado, sin que la creación de este fichero haya sido autorizada por disposición general, publicada en el Boletín Oficial

del Estado. El citado formulario no contiene ninguna información sobre los extremos recogidos en el apartado 1 del artículo 5 de la Ley Orgánica 15/1999, que dispone *"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco..."*, lo que supone una infracción de carácter leve tal y como dispone el artículo 44.2 d) de la citada Ley. Asimismo, el artículo 20 determina que "*la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente",* por lo que el Museo ha incurrido en una infracción cuya tipificación se encuentra en el 44.3 a) de la Ley Orgánica 15/1999.

Agencia Estatal de Administración Tributaria

Se ha instruido un procedimiento a la Agencia Estatal de Administración Tributaria por posible vulneración del deber de secreto al entregar información sobre datos tributarios del año 1998 de un ciudadano a un tercero. De las actuaciones de inspección llevadas a cabo en la A.E.A.T. se pudo acreditar que el documento presentado por el afectado en su denuncia corresponde a una impresión de pantalla de acceso a los datos resumen de la declaración abreviada de la Renta del año 1998. Asimismo, se ha podido comprobar que dicho certificado se ha emitido accediendo a los datos del afectado a través de su excónyuge, sin poder acreditar el motivo por el cual se procedió a realizar dicho acceso. A la vista del resultado de las actuaciones previas, se acordó iniciar procedimiento de infracción de Administraciones Públicas con arreglo a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992, de 29 de octubre. El procedimiento finalizó mediante Resolución en la que se declara que la Agencia Estatal de Administración Tributaria había infringido el deber de secreto (artículo 10 de la LORTAD).

Tesorería General de la Seguridad Social

En el transcurso del año 2001, se ha procedido a la instrucción de dos procedimientos a la Tesorería General de la Seguridad Social por posible infracción al artículo 10 de la Ley 15/1999, al facilitar una certificación en relación a la vida laboral a una persona distinta de la interesada sin contar con su consentimiento. Cabe destacar que uno de los procedimientos se ha resuelto con el archivo de las actuaciones al acreditarse que la persona a la que se hizo entrega de la certificación de vida laboral había incurrido en un presunto delito de falsedad documental, remitiéndose, por parte de la Agencia, al Juzgado correspondiente la totalidad de la documentación recabada. Sin embargo, en el otro procedimiento se pudo verificar que la Tesorería General de la Seguridad Social expidió un certificado sin consentimiento del afectado y sin acreditar, durante la tramitación del mismo, que se hubieran cumplido las exigencias establecidas por el propio Organismo para la emisión de certificados y su entrega a terceras personas.

Resoluciones dictadas en relación a las medidas de seguridad exigibles a las Administraciones Públicas en el tratamiento de datos personales.

Como ya se informó en la memoria del año anterior, en dicho ejercicio se incoaron procedimientos de infracción de Administraciones Públicas relacionados con el cumplimiento de las medidas de seguridad a la Agencia Estatal de Administración Tributaria (A.E.A.T.) y al Instituto Nacional de Seguridad Social (I.N.S.S.).

Las actuaciones realizadas por la Inspección de datos se circunscribieron a constatar si los documentos desechados procedían de sistemas informáticos y si la información encontrada en los mismos era de uso interno de la Administración imputada.

En el marco de estas actuaciones se comprobó que los documentos encontrados con información de la A.E.A.T. consistentes en impresiones de pantalla, listados impresos y documentación diversa eran copia de documentos generados por los sistemas de información de dicho Organismo. En ellos constaban datos relativos a identificación de contribuyentes, bienes, situación tributaria, datos bancarios, avales e información sobre fianza personal solidaria.

Los documentos provenientes del I.N.S.S. que han podido ser objeto de acceso y consulta de terceras personas ajenas al citado Organismo y a los interesados, contenían datos personales tales como: nombre, apellidos, domicilio, cuenta bancaria y número de afiliación de Seguridad Social, entre otros.

A la vista de las actuaciones descritas se procedió a la apertura de procedimientos de infracción de Administraciones Públicas. De la resolución que puso fin a estos procedimientos, destacan los siguientes aspectos.

La primera cuestión que se aborda es la de si la exigencia de medidas de seguridad (art. 9 de la LOPD) es aplicable a datos que figuran en soporte papel. Para ello es preciso delimitar cuales serian los acceso que la Ley pretende evitar mediante la exigencia de medidas de seguridad. A tal efecto es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

En lo que respecta a los ficheros, el art. 3.a) los define como "todo conjunto organizado de datos de carácter personal" con independencia de la modalidad de acceso al mismo.

Por su parte, la letra c) del mismo artículo permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita la "comunicación" o "consulta" de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros "...que contengan datos de carácter personal sin las debidas condiciones de segu-

ridad que por vía reglamentaria se determinen".

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca, están también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Partiendo de tales premisas deben analizarse a continuación las previsiones que el Real Decreto 994/1999 prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El art. 2.10 del Reglamento considera "soporte" al objeto físico susceptible de ser tratado en su sistema de información sobre el cual se pueden gravar o recuperar datos. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprensivo de todos ellos en congruencia con los preceptos de la LOPD ya expuestos, que tratan de evitar accesos no autorizados a los datos cualquiera que sea el procedimiento u operación para llevarlos a cabo.

El artículo 20 incorpora las previsiones específicas que han de aplicarse en la gestión de soportes. Sus dos primeros apartados se refieren específicamente a soportes informáticos, calificativo que no aparece en el apartado 3, debiendo, por ello, acudirse a la definición general de soporte antes citada. Conforme a dicho apartado, *"cuando un soporte vaya a ser desechado ... se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él ..."*. Por otra parte este mismo criterio ha sido el adoptado para la Orden del Ministerio de Trabajo y Seguridad Social de 17 de enero de 1996, sobre Control de Accesos al Sistema Informático de la Seguridad Social, en su artículo 8, dispone: *"Por los responsables de las distintas entidades y organismos incluidos en el sistema de seguridad se implantarán las medidas que eviten la salida no autorizada de soporte de datos (listados, soportes magnéticos u otros) fuera de las dependencias de la entidad, así como se supervisará periódicamente su efectivo cumplimiento."*

Igualmente, la propia AEAT tal y como consta en su documento "Manual de Seguridad General de la Agencia Tributaria" establece respecto de la documentación en soporte papel generada para uso interno que "*durante el tiempo que la documentación permanezca en la unidad responsable de su utilización, el destinatario de la misma velará de su correcto manejo, así como de su custodia una vez concluida la jornada laboral en armarios cerrados al efecto*", que "*la destrucción de los listados se hará constar en una diligencia que se capturará informáticamente junto con la recepción de los mismos*" y que "*la destrucción del resto de documentación se hará constar así mismo en diligencia expedida al efecto*".

En los casos expuestos resultó acreditado que la información desechada en papel procedía de soportes informáticos internos y que ambos Organismos deberían haber adoptado las medidas necesarias para impedir cualquier recuperación posterior de la información que contenían. Tales medidas no fueron adoptadas, incurriendo por ello en infracción del art. 9 de la LOPD.

3.1.2. Resoluciones de archivo

Entre las reclamaciones presentadas ante la Agencia que han finalizado con una resolución de archivo cabe destacar las relativas a posibles infracciones por comunicación de datos entre Administraciones Públicas, en algunos casos de datos especialmente protegidos, tratamiento sin consentimiento y vulneración de deber de secreto.

En este contexto se recibieron dos reclamaciones en relación al acceso indebido a la información sobre la vida laboral que posee la Tesorería General de la Seguridad Social. En una de las reclamaciones, el afectado denuncia que la empresa en que prestaba sus servicios le envió un pliego de cargos con motivo de la supuesta comisión de incumplimientos que pudieran ser motivo de sanción, en el que consta información relativa a vulneración de la exclusividad del contrato de trabajo debido a que "... permanece dado de alta en la Seguridad Social por la mercantil...". Sin embargo, y después de realizar las actuaciones de Inspección, se pudo constatar que la información sobre la vida laboral había sido suministrada por el propio afectado.

En otra reclamación, el afectado plantea que entre la documentación presentada a un Juzgado figura un informe de su vida laboral emitido por la citada Tesorería General de la Seguridad Social. En este caso se resolvió el archivo de actuaciones al acreditarse que el informe había sido elaborado por el propio Organismo, el cual ha acreditado, que pese a haber sido solicitado por persona distinta del titular, se habían cumplido todos los requisitos necesarios para la elaboración del certificado de vida laboral y su entrega a terceras personas, con autorización del afectado.

En relación a la posible cesión entre Administraciones Públicas, se recibió un escrito donde el afectado consideraba que se había vulnerado el artículo 7 de la LOPD al haber sido trasladado el expediente disciplinario incoado por el Ministerio de Administraciones Públicas a un Ayuntamiento, lugar donde actualmente está prestando servicio. La cuestión planteada exigía analizar si los traslados del expediente disciplinario que se han producido con motivo del cambio de destino del afectado, vulneran la intimidad del mismo o están amparados por una Ley. En este sentido, la Agencia acordó el archivo de las actuaciones al considerar que en las disposiciones legales vigentes en materia de régimen local, se establece: *"Las sanciones disciplinarias que se impongan a los funcionarios se anotarán en sus hojas de servicios y, en todo caso, en el Registro de Personal, con indicación de las faltas que la motivaron...."* (art. 152.1 del Texto Refundido) . El hecho de que la Resolución del expediente disciplinario incoado al afectado sea dictada por el Ayuntamiento que propuso su iniciación o por el Ayuntamiento en qué presta sus servicios en este momento, no afecta a que los datos relativos a la sanción disciplinaria se incluyan en un fichero, cuyo responsable es el Ministerio de Administraciones Públicas, y en la hoja de servicios del propio afectado.

Por último, y como novedoso en el campo de las tecnologías de la información realizadas a través de Internet, se recibió una reclamación en la que se indicaba que el Ministerio del Interior había publicado un informe sobre violencia callejera del año 1999, que contenía datos personales. Sin embargo, aunque dicho informe efectivamente estaba publicado en Internet se pudo constatar que solo hacia referencia al número de detenidos sin especificar datos de carácter personal, por lo cual no resulta de aplicación la Ley Orgánica 15/1999.

3.1.3. Tutela de Derechos.

Durante este año se han tramitado ocho tutelas de derecho por denegación del ejercicio de los derechos de los ciudadanos, de las cuales solo una de ellas ha sido desestimada al considerarse por parte de la Agencia, que la petición de rectificación solicitada por el afectado de un informe médico emitido por el Instituto Nacional de Seguridad Social, fue elaborado según los dispuesto en la normativa reguladora de las incapacidades laborales del sistema de la Seguridad Social. Al ser ratificado dicho informe y dada respuesta al afectado en el plazo establecido reglamentariamente se desestimó su reclamación.

De las restantes Tutelas de derecho tramitadas, que fueron estimadas por parte de la Agencia, cuatro de ellas se iniciaron por reclamación fundada en la denegación del derecho de acceso, otras dos estaban relacionadas con el ejercicio del derecho de rectificación y la última de ellas se fundamentaba en la denegación del derecho de cancelación de los datos del afectado contenidos en el Registro Central de Penados y Rebeldes.

3.1.4. Otras actuaciones de la Inspección de Datos

A finales del año 2001, como consecuencia de denuncias presentadas en la Agencia por ciudadanos, se han realizado actuaciones de Inspección a distintos Organismos dependientes de la Administración General del Estado que actualmente se encuentran en fase de actuaciones previas de inspección o de Acuerdo de Inicio de Procedimiento de Infracción de Administraciones Públicas. La mayor parte de las mismas se refieren a posible vulneración de artículo 10, de la Ley Orgánica 15/1999 relativo al deber de secreto.

En el momento de finalizar el ejercicio, todas las actuaciones referidas anteriormente se encuentran en fase de tramitación.

3.2. Administración Autonómica

El número de actuaciones de inspección que se han practicado durante el año 2001, en relación con ficheros cuya titularidad es una Administración Autonómica, se ha mantenido en términos equivalentes al de años anteriores. No obstante es significativa la reducción en el número de expedientes sancionadores iniciados.

Respecto de las actuaciones de inspección tramitadas cabe señalar las tres siguientes, iniciadas todas ellas tras recibirse escritos de denuncia:

* La primera se refería a la denuncia de un acuerdo que había suscrito la Consejería de Industria, Comercio y Turismo de la Generalitat de Catalunya con la Cámara Oficial de Comercio, Industria y Navegación de Girona, por el que ésta última tenía acceso a los ficheros automatizados de la primera, con el fin de que le facilitara la gestión de los servicios de información y tramitación que afectan a la puesta en marcha, ampliación o traslado de actividades industriales. Tras la realización de las pertinentes actuaciones de investigación el Director de la Agencia procedió a su archivo, entendiendo que la firma de dicho acuerdo estaría amparado por el artículo 12 de la Ley 15/1999 y por el artículo 1.2 de la Ley 3/1993, de 22 de marzo, de las Cámaras Oficiales de Comercio, Industria y Navegación, que dispone que dentro de las competencias que las Cámaras pueden ejercer se encuentran las que les puedan encomendar y delegar las Administraciones Públicas.

* En la segunda, se denunciaba a la Dirección General de Recursos Humanos de la Consejería de Economía y Hacienda de la Comunidad Autónoma de Murcia, tras haber ordenado su Director General, sin autorización judicial, la intervención de las comunicaciones de correo electrónico de diferentes funcionarios de esa Comunidad Autónoma. Durante las actuaciones de investigación se puso de manifiesto que el Director General había dictado instrucciones

específicas con el fin de destruir un mensaje electrónico que había sido remitido a varias direcciones pertenecientes a funcionarios de la Comunidad Autónoma, al entender que este mensaje presentaba un contenido malicioso y que suponía una flagrante suplantación de su propia identidad. En este caso también se procedió al archivo de las actuaciones, al no apreciarse la comisión de ninguna infracción a la normativa sobre protección de datos de carácter personal y, considerando que la actuación del Director General era una decisión que se encuadraba dentro del ámbito de sus competencias, así como que no había accedido al contenido de los mensajes ni revelado el mismo.

* En la tercera se ponía en conocimiento del Director de la Agencia un incidente que se produjo en una Oficina de Empleo, dependiente de la Generalitat Valenciana, y que supuso la aparición en el interior del contenedor de basura de numerosos contratos de trabajo del año 1997. Durante las actuaciones de investigación se puso de manifiesto que empleados de esa oficina habían depositado un archivador de cartón que contenía documentos en una papelera para su destrucción, siendo posteriormente evacuado su contenido por error a un contenedor ubicado en la vía pública. Asimismo, se acreditó que las Diligencias de Investigación Penal incoadas por la fiscalía del Tribunal Superior de Justicia de la Comunidad Valenciana, por presunto acto de negligencia por hechos relacionados con la Oficina de Empleo mencionada, habían sido archivadas por estimarse que los hechos denunciados no eran constitutivos de infracción penal. El Director de la Agencia archivó finalmente las actuaciones al no ser aplicable la LOPD a los archivos manuales hasta el 24 de octubre de 2007, a excepción de los derechos de acceso, cancelación y rectificación, ya que no pudo acreditarse que los documentos que aparecieron en el contenedor de la basura procedieran de algún tratamiento automatizado realizado por los sistemas informáticos.

Respecto de los procedimientos sancionadores, cabe señalar el que se inició contra el Centro de Informática de Gestión Tributaria, Económico-Financiero y Contable dependiente de la Xunta de Galicia, por comunicación de datos a dos entidades bancarias con el fin de que emitieran los justificantes de haberes de sus empleados públicos.

Durante la tramitación del procedimiento quedó acreditado que pese a que las competencias de emisión de los justificantes de haberes las tenía atribuidas ese Centro de Informática, el 50% de los justificantes de haberes eran emitidos por dos entidades bancarias. Para ello, el Centro de Informática generaba y entregaba mensualmente a dichas entidades sendas cintas magnéticas conteniendo la información necesaria para que emitieran el recibo de nómina correspondiente, procediendo después a remitir los justificantes de haberes a los domicilios de los trabajadores que eran clientes de la entidad, o a las entidades bancarias designadas por el perceptor. Además, quedó acreditado que no existía un contrato formal de prestación de servicios suscrito entre el Centro de Informática y las dos entidades bancarias para la prestación del mismo.

Iniciado el procedimiento, se resolvió declarando la existencia de infracción al estimarse que, para que exista una prestación de servicios encuadrable dentro del actual artículo 12 de la Ley 15/1999, es necesaria la constancia de la suscripción de un contrato de servicios entre las partes, en el que se haga expresa mención de las previsiones contenidas en dicho artículo, no siendo admisible una mera referencia a la prestación del servicio. Y ello, porque el aludido artículo exige expresamente que el contrato de prestación de servicios conste en alguna forma que permita acreditar su celebración y contenido y que en él, se establezcan expresamente: que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento; que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas y que se recojan las medidas de seguridad que el encargado del tratamiento esté obligado a implementar.

3.3. Administración Local

Durante el año 2001, se han recibido en la Agencia cinco reclamaciones de Tutela de derechos y dieciséis denuncias en relación al posible incumplimiento de lo establecido en la Ley Orgánica 15/1999 por parte de los responsables de los ficheros gestionados por la Administración Local, que dieron lugar a las correspondientes actuaciones de investigación por la Inspección de Datos.

De los procedimientos de Tutela de derecho tramitados, dos de ellos se iniciaron por reclamación fundamentada en la denegación del derecho de acceso, otras dos estaban relacionadas con el ejercicio del derecho de rectificación y la última de ellas se basaba en la denegación del derecho de cancelación de los datos del reclamante.

Dos de las reclamaciones fueron desestimadas, una de ellas relacionada con el ejercicio del derecho de rectificación, por quedar fuera de la competencia de la APD la cuestión planteada por el denunciante y la segunda, relativa al ejercicio del derecho de acceso, fue desestimada por ser competencia su resolución, de la Agencia de Protección de Datos de la Comunidad de Madrid.

Seis de las denuncias presentadas se referían a la cesión de datos personales por parte de Entidades Locales a otras entidades públicas o privadas sin el consentimiento de los afectados, cuatro de ellas hacían referencia al Padrón de Habitantes como el origen de los datos cedidos, otra de las denuncias se basaba en la cesión de los datos personales de los trabajadores de una Diputación Provincial a una entidad privada para realizar envíos de cartas personales con fines publicitarios, y la última de ellas denunciaba la comunicación a un Órgano judicial de antecedentes policiales de un ciudadano, cuya anotación databa del año 1975.

De las restantes denuncias presentadas, dos ellas hacían referencia a posible vulneración del deber de secreto y siete a posibles infracciones del artículo 4.2 y 5.1 de la LOPD, relativos al tratamiento de datos personales sin consentimiento del afectado y al derecho de información en la recogida de los datos, respectivamente.

Asimismo, tras la aparición en los medios de comunicación de una noticia relativa a la posible utilización por parte de la Policía Local del Ayuntamiento de Ecija, de expedientes sobre datos policiales de los ciudadanos que pudieran afectar a las derogadas legislaciones de Vagos y Maleantes y de Peligrosidad Social, el Director de la Agencia ordenó a la Inspección de Datos la apertura de actuaciones de investigación.

El número de procedimientos de infracción de Administraciones Públicas por vulneración de la Ley Orgánica 15/1999, incoados a entidades integrantes de la Administración Local durante 2001, derivados de las denuncias presentadas por los ciudadanos, fueron seis. De ellos, dos se debieron a infracción del artículo 11 de dicha Ley Orgánica, relativo a la comunicación de datos personales a terceros sin consentimiento de los afectados, infracción tipificada como muy grave en el artículo 44.4.b) de dicha norma.

En otras dos ocasiones se inició el procedimiento por infracción del artículo 10 de la LOPD, relativo a la obligatoriedad del deber de secreto por parte del responsable del fichero y de quienes intervengan en su tratamiento, tipificada como grave en el artículo 44.3.g) de la citada norma, y en las dos ocasiones restantes las causas fueron infracción al artículo 4.2 de la LOPD, relativo al tratamiento de los datos de carácter personal para finalidad distinta de la que hubieran sido recogidos, y por infracción al artículo 6.1 relativo al consentimiento inequívoco del afectado para el tratamiento de sus datos, tipificadas ambas como graves.

En este ámbito de actuaciones cabe destacar la incoación del procedimiento de infracción de Administraciones Públicas al Ayuntamiento de la Seu D'Urgell, por haber realizado un acuerdo verbal con una entidad privada para la prestación de un servicio, consistente en la creación de un portal de Internet, con objeto de facilitar una dirección de correo electrónico gratuito a sus habitantes.

A tal efecto, dicho Ayuntamiento facilitó a la entidad privada un fichero automatizado, generado a partir del Padrón de habitantes, con datos relativos a aproximadamente 44.000 cuentas de correo electrónico (dirección de correo, usuario y contraseña). Por su parte la entidad cesionaria procedió a realizar el alta de dichas cuentas en su propio servidor de correo electrónico. El Ayuntamiento de La Seu D'Urgell no había solicitado a los vecinos el consentimiento para la cesión de sus datos.

El acuerdo de inicio del procedimiento de infracción de Administraciones Públicas, establece que el Ayuntamiento puede incurrir en falta tipificada como muy grave, al infringir lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999, en el que se establece que, *los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado* .

Asimismo, cabe reseñar el acuerdo de inicio de procedimiento de infracción de Administraciones Públicas al Ayuntamiento de El Ferrol, por un error informático detectado en el funcionamiento de una página Web, cuyo diseño y mantenimiento había sido adjudicado a una entidad privada.

La finalidad de la página web era la promoción turística de El Ferrol, siendo una de las opciones contempladas en dicha página, el envío de postales gráficas a través de internet, en las que se podía incorporar un texto por parte del remitente. Por un fallo de seguridad desapareció el control que impedía el acceso a la relación de mensajes de otros usuarios, así como el contenido de los mismos, por lo que dicha información quedó accesible públicamente.

El Acuerdo de inicio de procedimiento de infracción, establece que estos hechos podrían suponer una infracción del artículo 10 de la LOPD, en el que se establece que, *el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo* .

Por otra parte, y también en fase de tramitación, se ha producido un acuerdo de inicio de procedimiento de infracción contra el Ayuntamiento de Osuna por posible infracción al artículo 6.1 de la LOPD, tratamiento de datos inconsentidos, con relación a la disposición adicional tercera de la misma relativa al *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.* El citado Ayuntamiento cuenta con un fichero manual, en el que constan datos del afectado relativos a antecedentes policiales desde el año 1975, que fueron remitidos a un Juzgado de Instrucción.

Asimismo, entre los procedimientos de infracción de Administraciones Publicas iniciados durante el año 2001 hay que reseñar los incoados a sesenta Ayuntamientos por posible infracción del artículo 20 de la LOPD, tipificada como grave en el artículo 44.3.k) de dicha norma.

La causa del inicio de dichos procedimientos de infracción fue la no contestación a los reiterados requerimientos realizados por la Agencia de Protección de Datos a todos los Ayuntamientos del territorio nacional de más de cuatro mil habitantes que no los habían inscrito, para el cumplimiento de la obligación de notificación de los ficheros que contengan datos personales de los cuales fueran responsables.

A la fecha de cierre de la Memoria, todos los procedimientos de infracción mencionados a lo largo de este apartado, se encuentran en fase de tramitación.

3.4. Fuerzas y Cuerpos de Seguridad

Entre las actuaciones de inspección efectuadas, figuran las que se iniciaron a raíz de peticiones de colaboración del Presidente de la Commission Nationale de L'Informatique et des Libertés (CNIL), autoridad competente en materia de protección de datos en Francia. Estas solicitudes se realizaron al amparo del artículo 114.2 del Convenio de Schengen, en relación con peticiones de acceso a los ficheros del Sistema de Información Schengen (SIS) y en, su caso, de cancelación, recibidas por dicha autoridad y que habían sido realizadas por personas que figuraban incluidas en el SIS como personas no admisibles a territorio Schengen y cuyos datos habían sido introducidos por las autoridades españolas.

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

En el año 2001 la Dirección General de la Policía puso en marcha la Operación LUDECO. Dicha operación se inició con el fin de dar una respuesta policial eficaz al incremento de los hechos perpetrados por grupos criminales o individuos procedentes de Colombia y Ecuador, mejorando la coordinación de las distintas Unidades y Servicios con competencia en la materia, a nivel central y periférico.
En la comparecencia del Director de la Agencia ante la Comisión Constitucional del Congreso de los Diputados que tuvo lugar el 7/11/2001, se suscitó un amplio debate sobre la conformidad de dicha operación con las previsiones de la LOPD. Como resultado del mismo el Director de la Agencia asumió el compromiso de verificar tal adecuación, dando instrucciones para que se iniciara una actuación inspectora de oficio cuyas conclusiones se producirán en el 2002.

4. ACTUACIONES MÁS RELEVANTES EN EL ÁMBITO DE LOS FICHEROS DE TITULARIDAD PRIVADA

Se describen a continuación los casos más significativos que se han producido durante el ejercicio en relación con los ficheros de titularidad privada. La información se agrupa por sectores de actividad con el fin de facilitar una perspectiva omnicompresiva de las cuestiones suscitadas en cada uno de ellos. Esta circunstancia determina que, en ocasiones se incluyan también, referencias a ficheros de titularidad pública en los que se han planteado temas relevantes respecto de cada sector de actividad.

4.1. Entidades financieras

La mayoría de las denuncias interpuestas por los ciudadanos contra entidades financieras son consecuencia de la inclusión de sus datos en ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito. Sin embargo, también es considerable el número de reclamaciones contra dichas entidades basadas en posibles infracciones a la Ley Orgánica 15/1999, en lo relativo a vulneración del deber de secreto, tratamiento de datos de carácter personal sin consentimiento o comunicación de datos fuera de los casos permitidos.

Al margen de las reclamaciones relacionadas con ficheros a los que se refiere el artículo 29 de la LOPD, durante el año 2001 se iniciaron 51 actuaciones previas de investigación que implican a entidades bancarias y financieras, así como 52 tutelas de los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos que los han ejercido ante estas entidades sin obtener resultados satisfactorios. De las 51 actuaciones de investigación iniciadas, 21 concluyeron con el archivo de las actuaciones y 10 dieron lugar a la apertura de un procedimiento sancionador, continuando el resto en fase de investigación al finalizar el año 2001. Merece destacar que la mayor parte de éstas, se referían a incumplimientos relativos al deber de guardar secreto que establece el artículo 10 de la LOPD.

Así mismo, la mayoría de los procedimientos sancionadores finalizados durante el año 2001 se han resuelto con la imposición de sanciones a las entidades financieras. La infracción a los artículos 9 (seguridad de los datos) y 10 (deber de secreto) de la LOPD han sido los hechos mayoritariamente sancionados, y en menor frecuencia, la infracción al artículo 4.3 (calidad de datos).

Entre las resoluciones dictadas por el Director de la Agencia de Protección de Datos durante el año 2001, en relación con ficheros de los que son responsables las entidades financieras, cabe destacar las resoluciones de sendos procedimientos incoados contra tres entidades bancarias como consecuencia de la aparición en medios de comunicación de una noticia relativa a que diversa documentación que contenía datos personales se encontraba en los contenedores de basura en la vía pública.

En dos de dichos procedimiento, el Director de la Agencia resuelve imponer sanción por infracción al artículo 9 de la LOPD, al constatarse que los documentos en los cuales se fundamenta la imputación de las infracciones, proceden de ficheros de los que es responsable la entidad bancaria y contiene información interna de la misma relativa a personas físicas. Al encontrarse en un supuesto en el que de un mismo hecho derivaban dos infracciones, se entendía que una de ellas, la de deber de secreto, estaba subsumida dentro de las exigencias de medidas de seguridad y por ello solo se sancionó por esta última. Los fundamentos de estas resoluciones coinciden básicamente, con las de similares procedimientos iniciados a Administraciones públicas que se detallan en los apartados correspondientes de esta memoria

Así mismo, el tercer procedimiento concluye mediante resolución de archivo al no acreditarse infracción de la Ley de protección de datos, toda vez que la documentación aparecida era de la que habitualmente manejan los ciudadanos, no conteniendo datos personales el único documento de uso interno de la entidad que había aparecido.

También cabe citar entre las resoluciones dictadas durante el año 2001, la Resolución R/23/2001 del Procedimiento incoado contra una entidad bancaria por vulneración del deber de secreto al facilitar datos sobre saldos y movimientos de una cuenta a una tercera persona no titular de la misma.

Durante la tramitación del procedimiento quedó acreditado que la entidad bancaria facilitó datos sobre saldos y movimientos de una cuenta corriente a una tercera persona ajena a la relación contractual entre los contratantes de dicha cuenta, sin que conste autorización para ello por los titulares.

En las alegaciones presentadas, la entidad bancaria aduce que los hechos han prescrito, al considerar que la vigente LOPD califica como leve la infracción de incumplir el deber de guardar secreto establecido en el artículo 10 de la citada Ley, estableciéndose un plazo de prescripción de un año a contar desde el día en que se cometió la presunta infracción.

La Resolución fundamenta la imposibilidad de que pueda prosperar la citada alegación, ya que los hechos imputados se produjeron durante la vigencia de la Ley Orgánica 5/1992, que tipifica como grave la infracción de vulneración del deber de guardar secreto en su art. 43.3.g), estableciendo un plazo de prescripción de dos años según el art. 46.1 de dicha Ley.

Por otra parte, incluso en el caso de considerarse aplicable al presente caso la vigente LOPD, en ella se tipifica la infracción de vulneración del deber de guardar secreto en el art. 44 con tres grados diferentes en sus epígrafes 2.e), 3. g) y 4.g), calificándola como leve, grave y muy grave respectivamente, encontrándose explícitamente definida la infracción imputada a la entidad bancaria, en el epígrafe 3.g) del citado artículo 44, como grave, al disponer :

" g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, **servicios financieros**, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. "

Finalmente, el Director de la Agencia de Protección de Datos resolvió imponer una sanción a la entidad bancaria por infracción del artículo 10 de la Ley Orgánica 5/1992 tipificada como grave.

4.2. Solvencia patrimonial y crédito

Durante el año 2001, las reclamaciones en relación a ficheros de información sobre solvencia patrimonial y crédito se incrementaron considerablemente respecto al año anterior. Así, si durante el año 2000 se iniciaron 63 actuaciones previas de investigación, en el año 2001 éstas prácticamente se duplicaron, ascendiendo a 120.

Además del notable aumento producido en el número de actuaciones, éstas se han visto incrementadas en complejidad, debido a la cada vez mas frecuente interposición por los ciudadanos de denuncias en las cuales se ven implicados varios ficheros de solvencia de titularidad diversa, en vez de uno solo como era habitual hasta la fecha.

Cabe indicar también el enorme incremento de reclamaciones en las que se ven implicadas entidades del sector de las telecomunicaciones, como entidades informantes, testimoniando el explosivo crecimiento que han alcanzado, entre otras operadoras, las de telefonía móvil. En este sentido, de las 120 actuaciones mencionadas, 39 correspondían a informaciones suministradas por entidades de este sector de las telecomunicaciones.

Estas consideraciones, sumadas al hecho de que durante el año 2001 ha aparecido un nuevo fichero de solvencia patrimonial y crédito, de carácter multisectorial y ámbito nacional, así como el cese de la distribución a las entidades financieras de otro que ofrecía información de fuentes accesibles al publico, reflejan la actividad existente en el sector de los servicios de información sobre solvencia y crédito.

Por otro lado, en la memoria del año 2000 se informó sobre el inicio de varios Procedimientos Sancionadores por infracción del artículo 29.4 de la LOPD, en relación con el articulo 4.3 de esta. Se trata del denominado "Saldo 0", con el cual podían figurar, durante la vigencia de la derogada LORTAD, deudas en los ficheros de Solvencia Patrimonial y Crédito, una vez pagadas éstas y hasta el transcurso de los seis años preceptuados. Los mencionados procedimientos finalizaron durante el año 2001, por lo que se informa a continuación del contenido de las resoluciones dictadas.

La situación de "saldo 0" era admitida al amparo de la LORTAD, como se ilustra en las citadas resoluciones, debido fundamentalmente a que la aplicación del principio de exactitud de datos para estos ficheros se regulaba mediante la aplicación del principio general de "calidad de datos", contenido en el art. 4.3. de la referida ley, que dispone que los *"datos serán exactos y puestos al día de forma que respondan con veracidad a la situación* **real** del afectado". Una deuda informada con "Saldo 0" en un fichero de cumplimiento e incumplimiento de obligaciones dinerarias respondía a la situación real de "haber sido deudor y haber dejado de serlo".

Ahora bien, el legislador introduce en la LOPD un cambio trascendental en este sentido, al exigir esta nueva norma, también en su artículo 4.3, que los datos deben responder con veracidad a la situación **actual** del afectado. El legisla-

dor vuelve a insistir a este respecto, y en concreto para el tipo de ficheros que estamos tratando, con el cambio producido en el artículo 29.4 de la LOPD respecto a lo dispuesto en el anterior artículo 28.3 de la LORTAD. Así, no cabe, con el texto vigente, el que una persona continúe figurando en un fichero común de solvencia patrimonial y crédito con deudas ya pagadas, ni aún figurando con el saldo impagado nulo o cero, pues ello implicaría reconocer como deudor a alguien que ya no lo es, no siendo por tanto la situación actual la reflejada por el fichero.

Como se explica en las resoluciones dictadas a este respecto, no puede olvidarse que la información sobre "Saldo 0" en un fichero relativo al cumplimiento o incumplimiento de obligaciones dinerarias es un dato adverso y no un dato neutral, puesto que esa consideración adversa es la que acredita la práctica de las entidades consultantes de dichos ficheros. En definitiva, el deudor que cumplió, conforme a la LOPD, debe ser excluido del fichero mediante la cancelación de sus datos. No cabrá, por tanto, ni que las entidades informantes notifiquen tales datos, ni que el responsable del fichero común los registre, trate y haga accesible a terceros. Así, el legislador ha venido a corregir una situación que bajo la vigencia de la LORTAD, producía graves quebrantos a los ciudadanos, y en la que éstos, después de pagar sus deudas, se veían condenados a permanecer en el fichero de morosos, aunque con "Saldo 0", por un tiempo máximo de 6 años. Además refuerza el criterio restrictivo de que, respecto de las limitaciones al contenido esencial de un derecho fundamental, han establecido las sentencias del Tribunal Constitucional y, específicamente sobre el derecho a la protección de datos, la STC 292/2000, de 30 de noviembre.

Por todo lo anterior, el Director de la Agencia de Protección de Datos dictó resoluciones por infracción del artículo 29.4 en relación con el 4.3 de la LOPD, tipificada como grave en el artículo 44.3 f) de dicha norma. No obstante, se apreció una cualificada disminución de culpabilidad de los imputados, procediendo por tanto la aplicación del art. 45.5 de la LOPD, por lo que las sanciones fueron rebajadas a 601,01 euros (100.000 ptas.).

Entre las restantes resoluciones dictadas por el Director de la Agencia de Protección de Datos durante el año 2001, en relación con los ficheros a los que se refiere el artículo 29 de la LOPD, cabe destacar la relativa al procedimiento sancionador incoado a la entidad responsable de uno de estos ficheros en relación a la inclusión de datos personales de cuatro menores de edad en un fichero común de morosidad. La inclusión de los datos de los menores fue realizada a instancias de un colegio, que por error facilitó los nombres de sus alumnos, menores de edad, en lugar de los nombres de los padres, auténticos deudores.

Durante las actuaciones previas de investigación correspondientes a este procedimiento sancionador, se pudo constatar la existencia de un contrato entre el colegio y una tercera entidad al objeto de gestionar la recuperación de deudas, por el cual esta tercera entidad quedaba obligada a la inclusión en el fichero de morosidad de los datos económico-financieros relativos al incumplimiento de obligaciones pecuniarias o económicas objeto del contrato, viniendo, por tanto, la citada inclusión ordenada por el colegio, al firmar el contrato.

Este procedimiento finalizó en archivo al exonerar de responsabilidad a la entidad de recobro de deudas a la que se inició el procedimiento. No obstante siendo el colegio la entidad responsable de la inclusión en el fichero, en los términos expuestos, y ser por tanto el colegio la entidad que debió asegurarse de que se cumplían todos los requisitos legales exigidos, según establece la Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, se ha iniciado expediente sancionador al mismo.

4.3. Compañías de telecomunicaciones

Como en años anteriores, la Agencia de Protección de Datos ha recibido gran cantidad de denuncias en las que se haya implicado algún operador de telecomunicaciones, lo cual pone de manifiesto que continúa latente en los ciudadanos una cierta preocupación por el uso que puedan dar a sus datos personales cualquiera de las empresas que operan en este sector.

De la revisión de las denuncias entrantes a lo largo del año habría que destacar por novedosas, aquellas recibidas desde mediados de año en las que varios ciudadanos ponen de manifiesto una serie de hechos que, resumidos, podrían concretarse en dos: por un lado, el haber recibido en su domicilio facturas emitidas por un operador de telecomunicaciones, las cuales contienen sus datos personales incluidos datos bancarios, cuando no existe ninguna relación contractual entre el denunciante y dicho operador y, por otro lado, el haber recibido una llamada telefónica de una persona que se identifica como empleado de una compañía eléctrica ofertando los servicios del citado operador de telecomunicaciones.

Los hechos descritos en último lugar fueron objeto de actuaciones de investigación por parte de la inspección de la Agencia de Protección de Datos llegándose a las siguientes conclusiones:

Todas las personas que han presentado denuncias mantienen relaciones comerciales con la empresa de suministro eléctrico.

La empresa de suministro eléctrico, a su vez, ha contratado con una tercera empresa, en virtud de un contrato de prestación de servicios, la gestión comercial.

Para que esta última pueda desempeñar los servicios contratados, la empresa de suministro eléctrico le ha facilitado los datos personales de aquellos clientes de la compañía que, en el escrito que la misma les remitió en junio de 1999, no habían manifestado su deseo de "*no recibir información que no esté relacionada con el suministro eléctrico".* El citado escrito comunicaba que "*en la medida en que estas compañas de divulgación de los productos del Grupo .... y de sus*

sociedades participadas se efectuarán a partir de la base de datos de nuestros clientes, queremos asegurar que ninguno de ellos reciba contra su voluntad otra información comercial que la estrictamente relacionada con el suministro eléctrico". Junto con este escrito se incluía un modelo de contestación mediante el cual, el destinatario podía expresar su deseo de "*no recibir información que no esté relacionada con el suministro eléctrico".* Cabe destacar que ninguno de los denunciantes ha manifestado a la Agencia de Protección de Datos haberlo desautorizado.

En marzo de 2000 la empresa de suministro eléctrico firmó un contrato con un operador de telecomunicaciones en virtud del cual, la empresa de suministro eléctrico comercializa los servicios de telefonía que presta el operador.

Desde el mes de octubre de 2000 se han realizado campañas de marketing telefónico para promocionar los servicios del operador de telecomunicaciones a los clientes de la empresa de suministro eléctrico y como consecuencia de dicha campaña, la empresa de gestión comercial ha remitido al operador de telecomunicaciones los datos personales de aquellas personas que en el transcurso de la conversación telefónica aceptaron contratar los servicios del operador.

La empresa de marketing no ha podido acreditar documentalmente el consentimiento otorgado por los denunciantes para la cesión de sus datos al operador de telecomunicaciones. Por otra parte, a pesar de que en el argumentario utilizado por las personas que realizaron las llamadas relativas a la campaña de marketing telefónico, aparece como despedida la frase "con los datos que nos ha facilitado hemos cumplimentado el contrato que recibirá en unos días para firmarlos, junto a un folleto que incluye las tarifas de consumo por días y franjas horarias", no se ha podido acreditar una relación contractual entre los denunciantes y el operador de telecomunicaciones, a excepción de las facturas emitidas por el operador a los mismos.

Las actuaciones de inspección comentadas anteriormente no han concluido en el ejercicio a que se refiere a la presente memoria, por lo que se dará cuenta de su resolución en la memoria correspondiente.

Por otra parte, a lo largo del año 2001 el Director de la Agencia de Protección de Datos ha dictado varias resoluciones en las que se hayan implicadas empresas del sector de las comunicaciones. Doce de estas resoluciones acuerdan el archivo de actuaciones y cinco de ellas son resoluciones de procedimientos sancionadores.

A continuación se expone un breve resumen de ellas:

La primera, resuelve imponer al operador de telecomunicaciones una multa por una infracción tipificada, según la LOPD, como grave al tratar los datos personales de la persona denunciante con conculcación de los principios y garantías establecidos en la ley. Los hechos denunciados y probados hacen referencia a la no atención, por parte del operador, a una solicitud de exclusión de los datos personales del denunciante de los repertorios de abonados públicos al servicio de telefonía.

La segunda, similar a la anterior, impone al operador una multa por una infracción tipificada como grave al tratar los datos personales del denunciante sin su consentimiento ya que, según se ha considerado probado, esta persona solicitó al operador un número de teléfono nuevo con la intención de que el mismo se mantuviese en secreto y por tanto, solicitó que fuese excluido de las guías telefónicas. No obstante, el operador en un momento concreto del tiempo, edita unas nuevas guías en las cuales incorporó el número de teléfono de la persona que había solicitado su no inclusión en las mismas y que hasta ese momento había figurado en los sistemas de información del operador, como no publicable.

La tercera resolución tiene como antecedentes de hecho la solicitud realizada por una persona al operador en el sentido de oponerse al tratamiento de sus datos personales para la remisión de publicidad, tanto de la propia compañía como de otras terceras. Además, se oponía a que sus datos figurasen en los repertorios públicos de abonados al servicio de telefonía. Dicha solicitud no fue atendida por el operador puesto que la persona denunciada recibió publicidad en su domicilio y sus datos personales podían ser extraídos por cualquier empresa de los repertorios públicos de abonados, a través de internet. Este incumplimiento, tipificado según la normativa de protección de datos como tratamiento sin consentimiento, supuso para el operador una sanción tipificada como grave.

Finalmente, la cuarta resolución tipifica la infracción cometida como leve y tiene su origen en varias denuncias presentadas por otras tantas personas al haber recibido en su domicilio una carta remitida por el operador en la que se les comunicaba que su contraseña había sido sustituida por la nueva que adjuntaban en la citada carta. Sin embargo, los datos personales incluidos en las cartas no se correspondían con los datos personales de los destinatarios de las mismas, hecho que pusieron de manifiesto con la correspondientes denuncias ante la Agencia de Protección de Datos. Las investigaciones realizadas por la inspección de la Agencia pusieron de manifiesto que se había tratado de un error en el proceso de impresión utilizado por el operador para imprimir las cartas.

Especial relevancia tienen las dos resoluciones que se van a comentar a continuación ya que los hechos denunciados hacen referencia al cumplimiento de la normativa específica de protección de datos en el sector de las telecomunicaciones, concretamente a diferentes artículos del Real Decreto 1736/98, de 31 de julio, que aprueba el Reglamento de desarrollo del Titulo III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, desarrollando determinados aspectos de la protección de datos personales en la prestación de servicios de telecomunicaciones.

Una de ellas tiene su origen en el escrito de una persona que ponía de manifiesto el hecho de haber recibido en su domicilio un sobre remitido por una empresa del que se deducía que dicha entidad le había dado de alta en un servicio

facilitado a través de internet sin haber manifestado el denunciante su deseo de ser cliente de dicha entidad y su desconocimiento del citado servicio.

Las actuaciones de inspección concluyen, entre otros aspectos, que: a) el operador de telecomunicaciones ha realizado una campaña de telemarketing a sus abonados profesionales ofertando dicho servicio, que es comercializado por otra empresa de su mismo grupo, en virtud de un contrato de Agencia suscrito entre ambas entidades. Para realizar esta campaña el operador utilizó los datos personales y de tráfico y facturación de todas las líneas contratadas por los abonados profesionales (personales y particulares); b) El operador facilitó a una empresa del grupo un fichero con datos personales de sus clientes sin haber podido acreditar que dichas personas estuviesen interesadas en contratar el citado servicio; c) A su vez, la empresa del grupo remitió al operador dos fichero con datos personales de clientes.

Entre los hechos probados y recogidos en dicha resolución se encuentran: 1) Ambas entidades, operador y empresa del grupo, suscribieron un contrato de Agencia por el que la segunda designa a la primera como Agente no exclusivo para la comercialización de sus productos y servicios, en virtud del cual, el operador comercializó para la empresa del grupo, entre otros servicios, un servicio de internet, siendo los destinatarios de la campaña publicitaria aquellos profesionales que, utilizando internet, nunca habían manifestado al operador su deseo de no recibir publicidad. Los datos de los interesados en el servicio se grabaron en un fichero que el operador remitió a la empresa del grupo 2) Para realizar la campaña promocional el operador había tratado datos de sus propios abonados que figuraban como "particular" y no sólo como "no particular" ya que la selección no se realizaba por líneas, sino por clientes. De este modo para seleccionar a un cliente "no particular" se trataban también sus datos como cliente "particular".3) La empresa del grupo remitió posteriormente al operador un fichero con datos de clientes cuyos registros habían sido procesados correctamente y otro con datos de clientes que no habían podido ser procesados.

Las infracciones imputadas en la presente resolución son las siguientes:

Primera. Al operador de telecomunicaciones se le imputa una vulneración del artículo 4.2 de la LOPD. Esta imputación se funda en que el operador ha tratado los datos de tráfico y facturación de sus abonados para seleccionar potenciales clientes y ofrecerles un servicio que no se encuentra entre los suministrados por el propio operador, sino que es prestado por otra empresa del grupo.

Se incumple así el artículo 65.3 del Real Decreto 1736/1998 que sólo permite el tratamiento de tales datos para la promoción comercial de los propios servicios del operador y una infracción del artículo 4.2 de la LOPD que impide el uso de los datos personales para finalidades incompatibles con aquellas para las que fueron recogidos.

Segunda. También se imputa al operador la infracción relativa al tratamiento de datos sin consentimiento del afectado (art. 6 de la LOPD) ya que, pese a haber remitido el denunciante un burofax prohibiendo la utilización de sus datos para funciones distintas de la prestación y facturación del servicio, el operador mantuvo sus datos en un fichero destinado a realizar promociones comerciales.

Tercera. Finalmente se imputa al operador una cesión ilícita de datos (art. 11 de la LOPD) al haber comunicado datos de sus abonados a otra empresa del grupo que prestaba el servicio.

A este respecto la Resolución destaca que, en el caso analizado, los datos personales del profesional que presentó la denuncia están incluidos en el ámbito de aplicación de la LOPD

Cuarta. A la empresa del grupo prestadora del servicio se le imputa la vulneración del artículo 6 de la LOPD al haber tratado sin consentimiento del afectado los datos que le había cedido el operador de telecomunicaciones.

Quinta. La segunda infracción imputada a la empresa del grupo fue la cesión ilícita de datos (art. 11 de la LOPD) ya que, a su vez, remitió al operador los datos de clientes después de haberlos tratado para determinar si se habían procesado correctamente o presentaban incidencias.

Sexta. Por último se declaró una infracción del art. 16 de la LOPD fundada en que la empresa del grupo no atendió el derecho de cancelación ejercitado por el denunciante

La segunda resolución tiene su origen en la denuncia formulada por una persona que ponía de manifiesto que había recibido una llamada telefónica por parte de un operador haciéndole ofertas publicitarias con fines de venta directa, cuando previamente había solicitado a dicho operador *"rechazar las llamadas no solicitadas con fines de venta directa".*

Los hechos probados recogidos en la resolución se concretan en que el denunciante es titular de un número de teléfono, que solicitó al operador en tres ocasiones "*rechazar las llamadas no solicitadas con fines de venta directa"* y que recibió una llamada en su número de teléfono por parte del operador realizándole ofertas publicitarias con fines de venta directa. El contenido de la llamada consistió en informar a sus abonados sobre la posibilidad de realizar 30 minutos diarios de llamadas a otras provincias por 1.500 pesetas al mes.

El Real Decreto 1736/1998 indica en su artículo 65.3 lo siguiente:

"Asimismo, los operadores podrán tratar los datos a los que se refiere el apartado anterior para la promoción comercial de sus propios servicios de telecomunicaciones, siempre y cuando el abonado haya dado su consentimiento previo".

El artículo 68 del mismo Real Decreto, se refiere, expresamente, a las llamadas no solicitadas con fines de venta directa:

"Las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas de llamada automática, a través de servicios de telecomunicaciones, sin intervención humana o facsimil, sólo podrán realizarse a aquellos que hayan dado su consentimiento previo".

La Resolución estima que el operador había obtenido el consentimiento tácito del abonado conforme al artículo 65 del Real Decreto 1736/1998.

En efecto, aunque la denunciante solicitó que su línea telefónica rechazara las llamadas con fines de venta directa (art. 68 Real Decreto 1736/1998), no manifestó su negativa a recibir llamadas del propio operador relacionadas con la promoción comercial de sus servicios al no haber contestado la carta que a tal efecto le había remitido previamente el operador (art. 65 del R.D. 1736/1998).

En base a lo anterior, se resolvió archivar el procedimiento incoado al operador al no suponer los hechos imputados vulneración a lo establecido en la LOPD.

4.4. Servicios de Internet

Durante el año 2001 se dictaron distintas Resoluciones relacionadas con la realización de actividades a través de Internet. Entre éstas, por su especial relevancia cabe destacar las que se reseñan a continuación.

Difusión de datos de usuarios de un portal de Internet

Como ya se mencionó en la Memoria correspondiente al año 2000, se iniciaron en dicho ejercicio actuaciones de inspección como consecuencia de un soporte informático que un medio de comunicación remitió a la Agencia. Dicho soporte, contenía más de doce mil códigos de usuarios, con sus respectivas contraseñas, supuestamente pertenecientes todos ellos a clientes de un proveedor de servicios de acceso a Internet.

Las citadas actuaciones, en las que se constató que haciendo uso de los códigos de usuario y contraseñas podía accederse a los datos personales de los clientes, así como al contenido de sus buzones personales de correo electrónico, dieron lugar a la apertura de un procedimiento sancionador al proveedor de servicios, resuelto en el año 2001 en base a dos hechos de especial relevancia:

El primero de ellos relativo a la obligación impuesta en el artículo 11 del Real Decreto 994/99 por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros que contengan datos de carácter personal y que establece que las contraseñas se almacenarán de forma ininteligible. A este respecto, el proveedor de servicios utilizaba un sistema de control de acceso para sus clientes que almacenaba de forma claramente legible las contraseñas, dando lugar a una falta de las garantías de seguridad respecto de la confidencialidad de dichas claves. Este hecho ha dado lugar a una sanción al proveedor de servicios por incumplimiento de las medidas de seguridad (artículo 9 de la LOPD).

El segundo hecho se refiere a que como consecuencia de las actuaciones practicadas se constató que el proveedor de servicios mantenía en su fichero información de clientes que se habían dado de baja desde el año 1996. Entre la información mantenida se encontraban, además de los datos identificativos, datos de fecha de nacimiento, teléfono, profesión, código de identificación de usuario, contraseña, etc. Estos datos, que no son necesarios para la finalidad del fichero (facturación del servicio prestado), deberían haber sido cancelados como consecuencia de la baja, de acuerdo con lo establecido en el propio Pliego de Condiciones Generales del contrato suscrito entre cliente y proveedor de servicios. La Agencia ha considerado que este hecho ha supuesto un incumplimiento, por parte del proveedor de servicios, de la obligación de cancelar los datos una vez han dejado de ser necesarios para la finalidad para la cual fueron recabados (artículo 4.5 de la LOPD), por lo que ha impuesto al proveedor de servicios la correspondiente sanción.

Difusión de datos relativos a participantes en un concurso organizado por una compañía automovilística

En el pasado año 2000 la Agencia recibió una denuncia presentada por un estudiante universitario que manifestaba que, tras haber participado en un concurso organizado a través de Internet por una importante firma automovilística, pudo conectarse a un servidor público de ficheros descargando sobre su propio ordenador personal un fichero que contenía sus datos personales (nombre, apellidos, domicilio completo, dos números de teléfono, fecha de nacimiento, centro y curso académico) así como los correspondientes a otras 4.810 personas.

Como consecuencia de las actuaciones practicadas por la Inspección a raíz de la denuncia, el Director de la Agencia acordó el inicio de un Procedimiento Sancionador que fue resuelto en el mes de julio de 2001. Durante el mismo, quedó probada la participación en los hechos de varias compañías especializadas en los sectores de comunicación y servicios informáticos, una de las cuales había facilitado su propio servidor, ubicado en EEUU, para alojar el fichero que contenía los datos de los concursantes que resultaron difundidos públicamente a través de Internet. En la Resolución se constataba la inexistencia de las medidas de seguridad adecuadas, así como la falta de regulación contractual de los accesos a los datos por cuenta de terceras compañías, el tratamiento y comunicación inconsentidos de los datos y su

transferencia internacional fuera de los supuestos previstos en la LOPD.

En la Resolución se sancionó a las diversas empresas que intervinieron en el proceso al haber incumplido las exigencias del artículo 12 de la LOPD para la prestación de servicios, incurriendo así en cesiones y tratamientos de datos no amparados legalmente. Adicionalmente, se sancionó la realización de transferencias internacionales de datos a EEUU sin amparo legal, así como el incumplimiento de las medidas de seguridad.

La compañía automovilística (como responsable del fichero o tratamiento, puesto que es quien en definitiva decide sobre la finalidad, contenido y uso del tratamiento, según la definición del artículo 3.d) de la Ley) conocía perfectamente todo el desarrollo del proceso, así como las entidades que habrían de intervenir en el mismo para el buen fin del proyecto con el que se pretendía la creación de una base de datos de estudiantes. Por todo ello, la Resolución declara que la compañía automovilística había participado en la comisión de los hechos constitutivos de infracción y debía responder de las infracciones y sanciones que de ellos se derivaban en calidad de responsable del fichero, siendo esta responsabilidad exigible en forma solidaria en virtud de lo establecido en el artículo 43 de la Ley Orgánica 15/1999 y 130.3 de la Ley 30/1992, de 26 de noviembre.

Publicación de imágenes de los trabajadores de la redacción de un periódico deportivo

Durante el año 2001 se resolvió también el Procedimiento Sancionador iniciado a una compañía editorial, como consecuencia de la denuncia presentada por un sindicato en relación con la instalación de cámaras en la redacción de un periódico, con las que se recogían imágenes de la actividad de los trabajadores, que luego se "*volcaban*" en la web del periódico con una periodicidad de 15 segundos.

En la Resolución se consideró que, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta la cámara concierne a personas y suministra información sobre la imagen personal de éstas, su lugar de trabajo y actividad que en él desarrollan,

En este caso, se estimó que los datos personales que suministra la grabación no sólo hacen referencia al lugar de trabajo de la persona cuya imagen se graba sino que reflejan la identidad de la misma a través de su aspecto físico. Además se entendió que los datos concernientes al puesto de trabajo de una persona son datos de carácter personal a efectos de la LOPD si se refieren a una persona física identificada o identificable, lo que ocurría en este caso en el que las personas físicas que aparecían en las imágenes podían ser claramente identificadas e individualizadas.

Por otro lado, si bien es cierto que existe una relación laboral entre la empresa y las personas cuya imagen capta la cámara, la relación jurídica entre la compañía editorial y sus trabajadores no exige ni requiere la grabación de las imágenes de estos últimos y su exposición pública en Internet para que pueda perfeccionarse entre las partes dicha relación jurídica. La grabación de los trabajadores para difundir sus imágenes a través de Internet con la finalidad de reflejar el movimiento y la actividad de la redacción no constituye una facultad del empresario, puesto que no figura entre las facultades que le reconoce la legislación vigente, y no puede confundirse con la facultad del empresario de adoptar las medidas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones laborales, pues en el presente caso no es esta la finalidad que se persigue con la instalación de la *webcam* y la difusión pública en Internet.

Por todo ello, en la Resolución se sancionó por una infracción del artículo 6 de la LOPD, al considerarse que la compañía no contaba con el consentimiento inequívoco de los afectados y tampoco se daba ninguna de las causas de exclusión del consentimiento recogidas en el apartado 2 del mencionado artículo.

Publicación de datos sobre accesos a páginas web relativos a usuarios de los servicios prestados por una Universidad

A comienzos del año 2001 se recibió una denuncia presentada por un sindicato en relación con la creación por parte de una Universidad pública de un fichero con información relativa a los sitios de Internet a los que accedía cada uno de los empleados de la Universidad, fichero cuyos datos habían sido difundidos públicamente a través de Internet durante el mes de diciembre de 2000. Una vez realizadas las oportunas actuaciones inspectoras, el Director de la Agencia acordó el inicio del correspondiente Procedimiento de Infracción de las Administraciones Públicas, el cual fue resuelto declarando la comisión por parte de la Universidad de una infracción del artículo 9 de la LOPD.

En la Resolución se consideraba probado que el Área de Informática y Comunicaciones, dependiente de la Gerencia de la Universidad, tenía asignada, entre otras, la competencia de gestionar y administrar el servicio de acceso a Internet, del cual se provee exclusivamente al personal docente y administrativo y a su alumnado. Todas estas personas podían disponer de una cuenta de acceso y una dirección nominativa de correo en el correspondiente dominio de la Universidad. Durante el mes de diciembre de 2000, el citado departamento realizó diversas pruebas en sus servidores con las que se pretendía obtener información estadística sobre los perfiles de acceso a Internet, en cuanto a número medio de páginas visitadas y tiempo medio de conexión. Entre estas pruebas, se ejecutó una aplicación que permite cruzar el fichero de registro de accesos (log de visitas) con la información que figura en el sistema, relativa a la correlación entre dirección IP y dirección del dominio de la Universidad, dirección que coincide con la que tiene asignada el usuario de cada ordenador. Como resultado, se obtuvieron distintos ficheros que contenían, para cada día de la semana anterior, una relación de las páginas visitadas desde cada dirección asignada a los usuarios. Para que esta información pudiese ser analizada, se depositaron los ficheros en una dirección del dominio de la Universidad, la cual es de acceso público, por lo que se encontraba al margen de la seguridad interna del dominio de la Universidad en materia de accesos, pudiendo por tanto ser consultada por cualquier persona.

En la Resolución también se estimaba no sólo que la inexistencia de medidas de seguridad tras el volcado de ficheros conteniendo datos personales a un sitio de acceso público había sido manifiesta, corriéndose el riesgo de que alguien se hiciese con información personal ajena de modo no autorizado e inadvertido por el afectado, sino también que existía el peligro de que se siguiese el rastro que van dejando quienes acceden a distintas páginas de Internet y, a partir de las preferencias, aficiones o intereses que de este itinerario quepa deducir, se acabase elaborando un perfil sobre la personalidad de esos usuarios de la red.

Consideración de la dirección electrónica como dato personal

Durante el año 2001 se recibió en la Agencia una reclamación presentada por un particular que manifestaba haber recibido en su buzón electrónico varios mensajes remitidos por una compañía especializada en seguridad informática, sin que le vinculara ninguna relación comercial con ésta que pudiese justificar el tratamiento de su dirección electrónica.

La Resolución valoraba que la dirección electrónica se forma por un conjunto de signos o palabras que la diferencian de las demás, siendo el titular de la misma quien generalmente decide y elige su formato, con el único límite de que no exista otra dirección idéntica correspondiente a otro titular. En la selección de la dirección electrónica se pueden elegir combinaciones que no contengan significado alguno o, utilizar como combinación el nombre de la persona o algún otro dato identificativo.

El concepto de dato personal, según la definición de la LOPD, comprende: "*cualquier información concerniente a persona física identificada o identificable*", de donde se requiere la concurrencia de un doble elemento: por una parte la existencia de una información o dato y de otra, que dicho dato pueda vincularse a una persona física. En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física la convierten en un dato de carácter personal. Por el contrario, si no puede hacerse tal vinculación no puede ser considerado dato personal. Al concurrir esta última circunstancia en el caso analizado, se procedió al archivo de las actuaciones.

4.5. Publicidad y marketing directo

El envío postal de publicidad no deseada y el marketing directo constituyen una de las actividades comerciales que mas número de denuncias han ocasionado durante el año 2001, al igual que en años anteriores, como viene siendo reflejado en la Memoria de la Agencia. En la mayoría de los casos el objeto de la denuncia tiene relación con el tratamiento de datos personales sin consentimiento del afectado.

Teniendo en cuenta el número de expedientes sancionadores iniciados en el año 2001, se observa que los que tienen relación con este sector suponen un 18% de todos los iniciados por actividades correspondientes al ámbito de los ficheros de titularidad privada, porcentaje que es similar al de los dos ejercicios anteriores. En cuanto a las infracciones detectadas, cabe señalar que, fundamentalmente, están tipificadas como graves por incumplimiento de lo estipulado en el art. 6 de la LOPD, es decir, el tratamiento de datos de carácter personal sin consentimiento del afectado.

De las sanciones por infracciones tipificadas como graves cabe destacar las impuestas a dos empresas editoriales por infracción del artículo 6.1 (tratamiento sin consentimiento) en relación con el art. 3.d de la LOPD. En cada caso el denunciante había recibido en su domicilio un envío publicitario de una de las empresas, figurando en ambos envíos una dirección postal errónea y coincidente con la registrada en el censo electoral.

Las entidades editoriales argumentan que no son responsables de la conducta que se les imputa, pues no han tratado dato alguno, ni son responsables de los ficheros de donde se obtuvieron los datos de los destinatarios. No obstante, en los dos casos, ha quedado acreditado que la entidad beneficiaria de la publicidad es la que decide sobre la finalidad, contenido y uso del tratamiento, y por tanto, según la definición del art. 3. d) de la LOPD, se identifica como responsable del tratamiento de los datos y beneficiaria de la publicidad y, en consecuencia es responsable del mismo.

Como fundamento de estas resoluciones, en ellas se señala que "*La vigente LOPD se aplica no solo cuando existe un conjunto organizado (fichero) de datos, sino también cuando se realizan operaciones y procedimientos que permitan la recogida, grabación, conservación, elaboración, bloqueo y cancelación de aquellos, aunque el Responsable de ese tratamiento carezca de bases de datos de su titularidad que, en los términos legales, se incluyan en la definición del fichero. De este modo, cabe que el sistema de protección de la LOPD se exija a los responsables del tratamiento, aunque carezcan de ficheros, e incluso a los meros encargados de aquel, a los que la nueva Ley hace también responsables. Esta configuración legal se adecua perfectamente a la realidad en la que cada vez es mas frecuente la externalización de los servicios informáticos, que no son prestados por las propias empresas responsables de los ficheros sino por terceros* .

Dentro de este marco, en los casos resueltos, el beneficiario de la publicidad es "*quien decide sobre el contenido y uso de la campaña publicitaria*", ya que es "*quien ha decidido que se realice una campaña publicitaria, ha delimitado el colectivo de personas físicas identificadas o identificables a las que debía realizarse el envío publicitario al contratar la selección de personas (…) determinando la finalidad y uso del tratamiento de los datos de las personas seleccionadas al contratar el envío de una comunicación publicitaria de sus productos (…) El artículo 3.d) de la LOPD considera como*

responsable del tratamiento no solo al titular o responsable del fichero, sino también a la persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento". Pudiendo imputarsele la infracción de la LOPD (en estos casos del artículo 44.3.d) y declarasele responsable de aquella.

Por otra parte, cabe señalar que del total de las resoluciones sancionadoras, un gran porcentaje ha recaído sobre una misma entidad, debido, en su mayoría, a tratamiento de datos personales existentes en los ficheros históricos de la entidad, sin que dicha empresa determinará el origen de los mismos, ni acreditará el consentimiento de los interesados para dicho tratamiento, quedando acreditado en todos ellos que dichos datos no provenían de fuentes accesibles al público, ni existe una Ley que ampare ese tratamiento ni una relación contractual o negocial entre los titulares de los datos y la empresa. En este caso el Director de la Agencia, iniciado el procedimiento sancionador acordó "*la medida de carácter provisional consistente en que por parte de S.M.I., se cese de inmediato en el tratamiento de los datos contenidos en sus ficheros históricos"*. Finalmente, mediante acuerdo posterior el Director de la Agencia confirmó la medida cautelar.

Es también destacable la resolución del Director de la Agencia de Protección de Datos relativa a la comisión de una infracción tipificada como muy grave por parte de una Universidad Pública, al quedar probado que "*la Universidad, proporciona a otras entidades, a cambio de una compensación económica, datos personales de estudiantes matriculados y de titulados en los diferentes estudios académicos"* sin haber acreditado la Universidad que disponía de consentimiento de los interesados para realizar la cesión de sus datos.

La Universidad en el formulario de solicitud de matrícula , solicitaba el consentimiento de los alumnos con la frase *"autorizas a que la Universidad proporcione tu dirección a empresas solventes que desean enviarte información escrita".* Sin embargo, no se informa que se van a facilitar datos identificativos de sus estudios (curso, centro, titulación etc..).

La resolución se fundamenta en que según establece el art. 11.1 de la LOPD, *"Los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario".* El citado precepto exige, como requisito primordial para que la comunicación o cesión de datos se ajuste a la Ley, que exista el consentimiento previo del interesado. El art. 3 h) de la Ley define el consentimiento del interesado como "Toda manifestación de voluntad, libre inequívoca, especifica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". Por tanto, si el consentimiento otorgado carece de algunas de las exigencias que especifica la propia definición nos encontraríamos ante un consentimiento viciado. El mismo art. 11, en referencia a la comunicación de datos, dispone en su apartado 3 *"Sera nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretendan comunicar."* Si el interesado a quien se solicita el consentimiento para la comunicación de sus datos desconoce el tipo de actividad de aquel a quien se pretenden comunicar y la finalidad para la que van a ser utilizados sus datos, nos encontramos ante una nulidad del consentimiento en virtud del transcrito artículo 11.3.

Varias entidades utilizaron los datos personales obtenidos de la Universidad, para la realización de envíos publicitarios, lo que ha ocasionado la sanción a las mismas por infracción del artículo 6.1 de la Ley Orgánica. Asimismo se declaró la existencia de una infracción muy grave por parte de la Universidad que cedió los datos.

Por otra parte, son también varias las sanciones impuestas a empresas que, a pesar de haber recibido solicitudes de cancelación por parte de los interesados, no han procedido a su cancelación y han continuado tratando sus datos con fines publicitarios.

4.6. Sanidad

El tratamiento de los datos de salud es objeto de especial protección por el legislador y tema de especial sensibilidad para la generalidad de la colectividad. De ahí la vigilante y constante preocupación de la APD por su adecuación a las prescripciones legales. A continuación se exponen las denuncias más significativas habidas en los sectores público y privado respecto al tratamiento de datos de salud.

Sector público

* En el año 2000 se recibió una reclamación en la que se denunció a un determinado Centro de Salud del INSALUD y concretamente a un médico que prestaba sus servicios en el mismo, por haber sido requerida la denunciante por un Juzgado de Instrucción en relación con una denuncia presentada por el citado médico, quien había aportado datos relativos al domicilio y número de teléfono de la misma, tras haberlos obtenido de la Administración del Centro de Salud.

Por los servicios de inspección se comprobó que el médico interpuso una denuncia en la que manifestaba que fue insultado y difamado por la usuaria de un vehículo con una determinada matrícula, *"madre de una paciente infantil"* con determinado domicilio y número de teléfono. Así mismo manifestó que sus datos fueron facilitados por la Administración del Centro de Salud *"ya que imperiosamente tenía que entrar a su despacho para pasar consulta médica"* .

Durante la inspección realizada en el Centro de Salud se comprobó que dicho centro disponía de un ordenador desde

el que se podía acceder a los datos administrativos de los usuarios adscritos al centro, entre ellos los de la denunciante.

Por razón de las funciones que tienen atribuidas, los médicos que forman parte del Equipo de Atención primaria del centro (como era el caso del médico denunciado) tienen acceso a los datos administrativos de los pacientes adscritos al mismo, especialmente para la realización de visitas domiciliarias.

Una Circular del INSALUD, en la que se detallan las instrucciones generales sobre seguridad y protección de datos, recoge el compromiso que adquieren los usuarios de los sistemas informáticos para utilizar la información con fines exclusivos de gestión, estando obligados a guardar recato de la misma y secreto de los datos de carácter personal.

Sin embargo el médico denunciado obtuvo, en su calidad de miembro del equipo médico del centro de salud, los datos de la denunciante contenidos en un fichero automatizado del centro, utilizando los datos del domicilio y teléfono de la denunciante para la interposición de una denuncia contra ella.

A la vista de los hechos el Director de la Agencia acordó el inicio de un Procedimiento de Infracción de Administraciones Públicas a la Gerencia de Atención Primaria de la cual dependía el Centro de Salud por infracción del artículo 10 de la LOPD relativo a la vulneración del deber de secreto.

De la Resolución de dicho procedimiento se dará información en la Memoria del próximo año.

Sector privado

* Mención especial merece una denuncia relativa a la entrega de documentos médicos oficiales a terceras personas, realizada por el médico responsable del tratamiento.

En este caso el denunciante manifestó que en la Demanda Civil que se seguía contra su hija, se acompañaban como prueba documentos relativos a la salud de la misma provenientes de una determinada clínica privada y de un determinado Centro de Salud. El denunciante también manifestaba que algunos de los informes entregados habían sido manipulados.

Tras realizar una inspección en la clínica privada del médico denunciado, se constató que la historia clínica de la hija del denunciante se encontraba archivada tanto en papel como en un fichero informático, comprobándose que ambas historias eran diferentes. La original entregada a la titular contenía diferente información que la historia clínica obtenida del fichero informático.

La historia clínica en formato electrónico fue manipulada y posteriormente impresa, no pudiéndose acreditar a quién fue entregada. No obstante, el médico denunciado no había sido requerido judicialmente para entregar la historia clínica de la hija del denunciante a terceras personas.

A la vista de los hechos, el Director de la Agencia acordó el inicio de un procedimiento sancionador al médico denunciado, que gira bajo el nombre de su clínica privada, por infracción grave al no adoptar las medidas necesarias para mantener la seguridad de los datos de carácter personal y por infracción muy grave por la vulneración del deber de secreto sobre datos de salud.

Dado que los documentos aportados como prueba en el procedimiento de Menor Cuantía se correspondían con copias de certificación relativa al parto de la hija del denunciante expedida por un determinado Hospital y copias de su historial clínico del mismo Hospital, el Director de la Agencia también acordó el inicio de un procedimiento de infracción de Administraciones Públicas al citado Hospital por infracción del artículo 9 de la LOPD, relativo a la seguridad de los datos, tipificada como grave por dicha norma.

De la resolución de ambos procedimientos se dará información en la Memoria del próximo año.

* Una de las denuncias recibidas se refiere a la utilización de los datos de un donante de sangre por una determinada Hermandad de Donantes de Sangre, hecho del cual tuvo conocimiento el denunciante al recibir un escrito remitido por dicha Hermandad en la que se le informaba de que sus datos habían sido facilitados por el Banco de Sangre correspondiente.

Tras realizar visita de inspección tanto en la Hermandad de Donantes de Sangre como en el Banco de Sangre, se constató que el Banco de Sangre, tras realizar las extracciones, permitía a la Hermandad de Donantes de Sangre el acceso a datos de los donantes dado que compartían un único fichero, no siendo los donantes conocedores del hecho.

A la vista de los hechos el Director de la Agencia ha iniciado un procedimiento sancionador al Banco de Sangre y a la Hermandad de Donantes de Sangre por cesión de datos de salud entre ambas entidades, que al finalizar el año 2001 se encuentra en tramitación.

* Otra de las denuncias se refería a la falta de atención de los derechos de acceso y cancelación de la denunciante por parte de una determinada Clínica. Se añadía en la denuncia que dicha Clínica facilitó los datos relativos a los ingresos de la denunciante a su ex marido ya que en respuesta a la solicitud de acceso que éste realizó a los datos de su esposa, la Clínica le comunicó que en cuanto a los internamientos de su esposa no se le podía facilitar ninguna información. Lo que sin embargo sí revelaba esta información era la estancia de la denunciante en la mencionada Clínica, teniendo en cuenta, además, que se trataba de una Clínica de salud mental.

Tras realizar una inspección en la citada Clínica se comprobó que las historias clínicas no se encontraban informatizadas y que el contenido de la historia clínica de la interesada se correspondía con la totalidad de la información que le fue facilitada a la propia interesada. Dado que la LOPD no es de aplicación a los ficheros y tratamientos no automatizados hasta el 24 de octubre del año 2007, sin perjuicio de los derechos de acceso y cancelación de la interesada, se concluyó que no se apreciaba en este caso ninguna vulneración a la LOPD. En lo relativo a la cancelación de los datos correspondientes al segundo ingreso de la interesada, que según la misma no se produjo, ha sido igualmente constatado por la Inspección de Datos que las fechas de ingreso coincidían con los datos registrados en el Libro de Sanidad, sin que existiera ninguna prueba o indicio del que pudiera deducirse la inexactitud de dichos datos, acordando por tanto el Director de la Agencia el archivo de las actuaciones.

* Se presentó una denuncia sobre la posible utilización de los datos de pacientes atendidos en una Consulta médica por parte de una determinada Clínica de cirugía estética, hecho del cual la denunciante tuvo conocimiento tras ejercer su derecho de acceso en la clínica como consecuencia de una llamada telefónica recibida por ella en la que, en nombre de un determinado doctor, se le informaba que las consultas se pasaban en la nueva Clínica. Además, el acuse de recibo de la clínica relativo al ejercicio del derecho de acceso de la denunciante, fue firmado por la misma persona que trabajaba en la Consulta.

Se realizó una visita de inspección a la Clínica de cirugía estética en la que no se encontraron ficheros con datos de carácter personal dado que la apertura de la misma era reciente y aún no disponía de sistema informático. Sí se encontró un fichero con fichas de cartulina que contenían los datos de sus clientes entre las cuales no se encontraban los datos de la denunciante.

Ante el requerimiento de los inspectores de la Agencia en relación con el origen de los datos de la denunciante, el representante de la Clínica de cirugía estética manifestó que uno de los médicos que trabajan en la misma, anteriormente trabajaba en otra consulta y que al trasladarse a la citada Clínica de cirugía estética envió un escrito a los pacientes que figuraban en su agenda manuscrita informándoles de la apertura de la clínica.

Dado que en la inspección realizada no se encontraron ficheros automatizados con datos de carácter personal, el Director de la Agencia resolvió archivar las actuaciones, al no resultar exigible lo dispuesto en la LOPD hasta octubre de 2007.

* Se presentó una denuncia sobre la posible cesión de datos de salud relativos a los trabajadores de un Consorcio Sanitario realizada por el mismo a una determinada Mutua y por ésta a la empresa de visitadores médicos subcontratada a tal efecto.

Tras realizar una inspección en la Mutua se constató que ésta se ampara en los conciertos que suscribe con las empresas a las que prestan sus servicios y que recibe datos de las mismas para realizar la prestación económica relativa a las bajas por accidentes de trabajo y enfermedades profesionales de la Seguridad Social. La posibilidad de que las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social contraten, mediante conciertos, con medios privados para hacer efectivas las prestaciones sanitarias, está prevista legalmente.

A tal efecto y en determinadas poblaciones en las que no existe presencia física de personal de la Mutua, ésta contrata con diversas entidades para realizar orientación diagnóstica y visitas domiciliarias, entre otros servicios.

Por su parte, el Consorcio no facilita datos relativos a los diagnósticos de los trabajadores que se encuentran en situación de baja laboral, sino que son obtenidos por la Mutua en el desempeño de sus funciones, incorporándolos después a sus propios ficheros.

Dado que en el supuesto examinado quedó acreditado que el tratamiento de datos de los trabajadores del Consorcio por la Mutua se encontraba amparado en la Ley General de la Seguridad Social y normativa de desarrollo, el Director de la Agencia resolvió archivar las actuaciones, no apreciándose vulneración de la LOPD.

* En otra de las denuncias se exponía que tras haber sufrido un accidente de tráfico, las denunciantes fueron examinadas por un determinado Gabinete de Médicos, el cual elaboró, a petición de una empresa de seguros, sendos informes relativos a su estado de salud. Estos informes fueron presentados por la empresa de seguros en los autos del Juicio Verbal pertinente que se seguían en un determinado Juzgado de Primera Instancia, sin que ellas dieran su consentimiento para la utilización, tratamiento y difusión de tales datos.

Con la documentación facilitada por la empresa de seguros, el Gabinete Médico elaboraba los informes médicos relativos a las lesiones de las denunciantes, que según se constató en la inspección realizada en el mismo, se encontraban registrados en el fichero de la entidad y los remitía a la empresa de seguros para su presentación al Juzgado, todo ello sin que constara el consentimiento de las afectadas para la cesión de sus datos personales y sin que existiera contrato de prestación de servicios entre la empresa de seguros y el Gabinete Médico.

A la vista de los hechos el Director de la Agencia acordó el inicio de un procedimiento sancionador al Gabinete Médico por infracción del artículo 11 de la LOPD, que al término del ejercicio aún no había finalizado.

4.7. Colegios profesionales

Los principales problemas que se han planteado hacen referencia a la cesión de datos de colegiados a otras entidades y al tratamiento que éstas realizan sin el consentimiento de aquéllos. De entre las resoluciones más importantes o significativas dictadas durante el año 2001, cabe destacar la siguiente:

* Un determinado Colegio Oficial de Odontólogos y Estomatólogos puso de manifiesto ante la Agencia el haber recibido denuncias de colegiados relativas a determinadas actuaciones llevadas a cabo por una Mutua de Accidentes de Trabajo consistentes en el envío a los colegiados que tienen concertados los servicios médicos del personal de sus clínicas con ellos, de publicidad de una determinada Entidad ofreciéndoles prestación de servicios odontológicos en condiciones económicas especiales, tanto para el personal como para su familia.

Tras realizar una inspección en la Mutua, el representante de la misma manifestó que la entidad solicitó a los servicios centrales de la Mutua que se enviara una oferta a las empresas y trabajadores autónomos que tenían concertados servicios médicos con dicha Mutua, siendo ésta la que realizó el mailing, seleccionando de su base de datos a los destinatarios así como las direcciones e imprimió la carta de presentación del servicio que se quería difundir, limitándose la Entidad a proporcionar a la Mutua la publicidad a enviar.

Tras realizar inspección en la Entidad, el representante de la misma manifestó que firmaron un acuerdo de colaboración con la Mutua para que ésta ofertara a sus mutualistas los servicios de la entidad. Finalmente señalaron que cuando envían publicidad de sus propios servicios a empresas o profesionales, utilizan direcciones que figuran en catálogos, como, por ejemplo, el editado por una determinada Empresa.

Tras realizar inspección en esta Empresa, los representantes de la misma expusieron que su actividad era la de edición de libros, anuarios y revistas técnicas. Los datos de los profesionales que figuran en las mismas son facilitados por Colegios y asociaciones profesionales.

El Colegio Oficial de Odontólogos y Estomatólogos denunciante comunicó a la Agencia que *"no edita ni ha editado nunca anuario alguno conteniendo datos relativos a los profesionales colegiados"*. Sin embargo, dicho Colegio facilitó a la Empresa un listado de nombres, apellidos, dirección profesional, teléfono, fax y e-mail de los colegiados.

A la vista de los hechos, el Director de la Agencia acordó el inicio de un procedimiento sancionador al mismo Colegio Oficial de Odontólogos y Estomatólogos por infracción del artículo 11 de la LOPD relativo a la cesión de datos de carácter personal, tipificada como muy grave, y a la Empresa por infracción del artículo 6 de la misma Ley relativo al tratamiento de datos personales sin consentimiento de los afectados, tipificada como grave.

Durante la tramitación de dicho procedimiento sancionador, la Empresa alegó, entre otras cosas, que al solicitar al Colegio un listado de sus colegiados, éste les contestó *"Tal y como solicitaron, adjuntamos la relación actualizada de colegiados que permiten la divulgación de sus datos ..."*. La Empresa, después de recibir dicho listado, vuelve a pedir el consentimiento a los colegiados para tratar sus datos, incluirles en la Guía que editan, etc. Si algún colegiado no autoriza el tratamiento de sus datos, éstos se mantienen en el fichero para evitar el solicitar de nuevo su consentimiento.

Finalmente, tras el estudio y valoración de las alegaciones presentadas por los infractores, el Director de la Agencia resolvió imponer al Colegio Oficial de Odontólogos y Estomatólogos una multa de 10.000.000 de pesetas (60.101,21 euros) y exonerar de responsabilidad a la Empresa por la infracción del artículo 6 de la LOPD.

4.8. Asociaciones

Entre los procedimientos más significativos tramitados durante el año 2001, cabe destacar la siguiente:

* Una Asociación gallega puso de manifiesto ante la Agencia que con motivo de la celebración de una Feria, se realizó un envío publicitario que fue recibido por todos los socios de la Asociación. La Feria fue organizada por un grupo cuyo órgano gestor era un determinado Instituto. Los datos de los destinatarios fueron extraídos de una base de datos respecto de la cual los citados destinatarios no habían autorizado ni su inclusión, ni su tratamiento. Así mismo manifiestan haber ejercido el derecho de acceso ante el Ayuntamiento correspondiente y ante el Instituto, no habiendo obtenido respuesta.

Como consecuencia de los hechos denunciados se realizó una inspección en la sede del Instituto, en la que su representante informó que el mismo forma parte de un grupo local de desarrollo rural al que le fue encomendada la gestión de un programa de iniciativa comunitaria, motivo por el cual se celebró la Feria.

Para promocionar la mencionada Feria, se realizaron una serie de envíos publicitarios a personas residentes en la autonomía de Galicia relacionadas con el tema tratado por la Asociación. Las etiquetas con los nombres y dirección de los destinatarios del citado envío, fueron confeccionadas por una Entidad determinada.

Aunque el Instituto no participó en el envío de la publicidad de la Feria, contaba con un fichero automatizado que contenía datos de carácter personal entre los que se encontraban gran parte de los relativos a los denunciantes sin que los representantes del Instituto pudieran determinar su origen. Además, el Instituto recibió 39 solicitudes de ejercicio de derecho de acceso las cuales no fueron contestadas.

Por otra parte, se realizó inspección en la citada Entidad, cuyos representantes declararon que el fichero con los datos

personales de los destinatarios del envío objeto de la denuncia, fue creado a partir de un fichero manual existente en la Asociación. La confección de las etiquetas fue realizada por la misma Entidad, colaborando el Ayuntamiento en el ensobrado y etiquetado del mismo.

Como consecuencia de las actuaciones realizadas, el Director de la Agencia acordó el inicio de un procedimiento sancionador al Instituto por infracción del artículo 6.1 de la LOPD, relativa al tratamiento de datos sin consentimiento de los afectados, y por infracción del artículo 15 de la misma Ley, relativo a la atención de los derechos de acceso, ambas infracciones tipificadas como graves por dicha norma; y de un procedimiento sancionador a la Entidad por infracción del ya descrito artículo 6.1 de la citada Ley Orgánica. Dichos procedimientos sancionadores al finalizar el año 2001 se encuentran en tramitación.

1 Las decisiones de la Comisión Europea 2000/518/CE y 2000/519/CE, de 26 de junio, han considerado adecuado el nivel de protección de datos personales en Suiza y Hungría. Así mismo, la Decisión 2000/520/CE, de igual fecha, ha efectuado la misma declaración respecto de las empresas de los Estados Unidos de América acogidas al sistema de "puerto seguro".

IV. SECRETARIA GENERAL

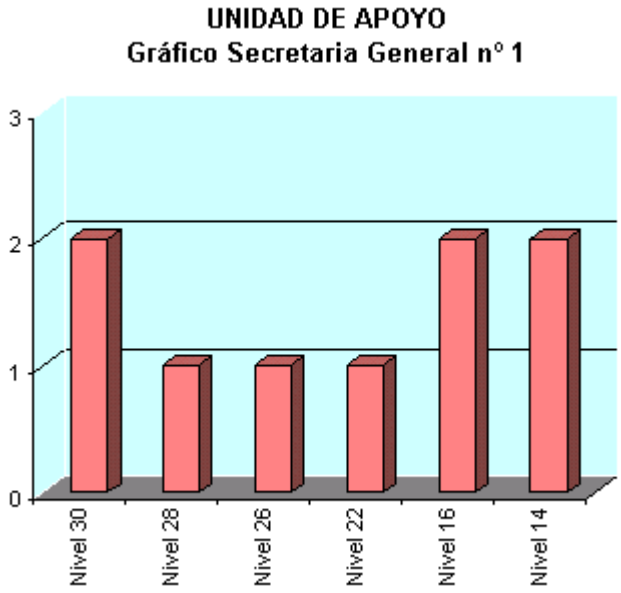
Las actividades conducentes a proporcionar y administrar los medios personales, materiales y técnicos para el funcionamiento del Ente, así como las competencias relativas a la atención al ciudadano, las atribuye el Estatuto de la Agencia (R.D. 428/93, de 26 de marzo) a la Secretaría General.

1. PLANIFICACIÓN, ORGANIZACIÓN Y GESTIÓN DE RECURSOS HUMANOS

La estructura orgánica de la Agencia de Protección de Datos se configura, de conformidad con lo dispuesto en el artículo 11 del citado Real Decreto 428/93, en los siguientes órganos:

* El Director de la Agencia, asistido por su Secretaría Particular, por la Unidad de Apoyo y el Gabinete Jurídico, que suponen un total de 10 funcionarios.
* El Consejo Consultivo.
* El Registro General de Protección de Datos, integrado por 14 funcionarios.
* La Inspección de Datos, constituida por 29 funcionarios.
* La Secretaría General, integrada por 16 funcionarios y 2 laborales.

El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General con categoría de Subdirecciones Generales, se constituyen como órganos jerárquicamente dependientes del Director de la Agencia.



REGISTRO GENERAL DE PROTECCIÓN DE DATOS
Gráfico Secretaría General nº 2

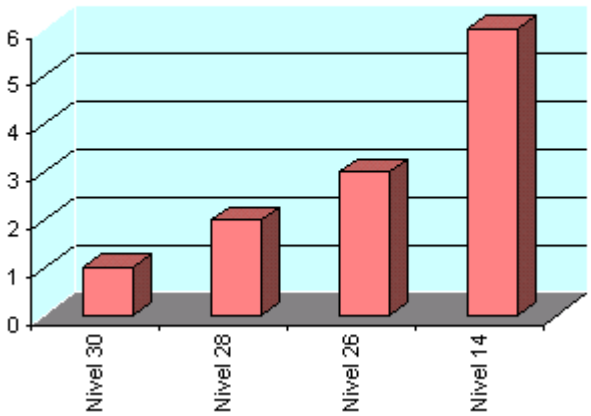
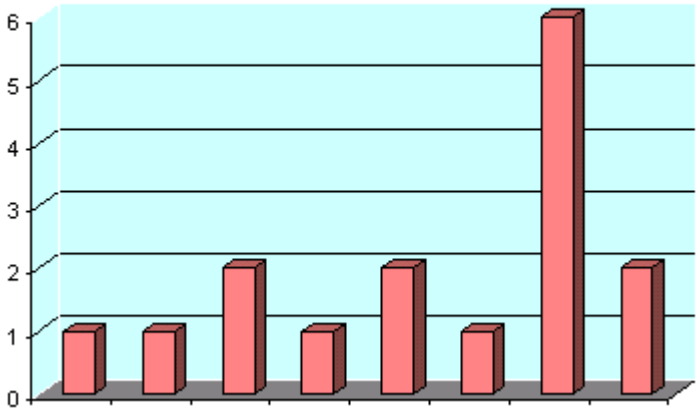
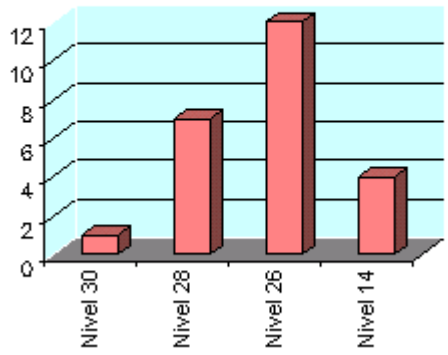


Gráfico S.G. Núm. 3
SECRETARIA GENERAL



INSPECCIÓN DE DATOS
Gráfico Secretaria General num. 4



En materia de Planificación, Organización y Gestión de Recursos Humanos se han realizado las siguientes actuaciones:

* Gestión y administración del personal funcionario y laboral destinado en la Agencia, y Gestión de retribuciones y habilitación.

Entre las actividades llevadas a cabo a este respecto, la gestión y administración ordinaria, destaca la continuación en la tramitación ante la Comisión Ejecutiva de la Comisión Interministerial de Retribuciones de un expediente de aumento de puestos de trabajo. Comenzado el expediente en el año 2000, como consecuencia de la necesidad de atender a las crecientes tareas de la Agencia, que se pusieron claramente de manifiesto en el citado expediente, y se concretaban en la solicitud de 42 funcionarios de perfiles y niveles diversos, quedó concluso con un acuerdo de la CECIR de 26 de septiembre de 2001, con otro posterior de corrección de errores en los que, autorizaban la modificación de la Relación de Puestos de Trabajo, con un aumento de los siguientes puestos de trabajo:

* 1 Consejero técnico, N.28, para la Unidad de Apoyo.
* 1 Inspector de Datos, N.28, para la Subdirección General de Inspección de Datos.
* 1 Subinspector N. 26, para la Subdirección General de la Inspección de Datos.
* 1 Jefe de Servicio de Gestión Presupuestaria N. 26 para la Secretaría General.
* 2 Jefes de Negociado N. 18 para la Subdirección General del Registro General de Protección de Datos.
* 1 Jefe de Negociado N. 18 para la Secretaría General.

Es evidente que la concesión de estos 7 funcionarios no satisface las necesidades (puestas de manifiesto en la Memoria anterior) en relación con los elementos personales necesarios para un normal desenvolvimiento de las competencias y tareas propias de la Agencia dada la tendencia creciente de carga de trabajo que se mantiene en aumento constante.

* Como consecuencia de la concesión indicada y para cubrir las bajas que se han ido produciendo a lo largo del año se han realizado seis convocatorias para la provisión de puestos de trabajo.

Para la provisión de las plazas contenidas en esas seis convocatorias se han llevado a cabo las comisiones de valoración oportunas.

* Así mismo, dentro del proceso de consolidación del empleo laboral llevado a cabo en el 2001 en la Administración General del Estado, por Resolución de 15 de junio (BOE del 28) se convocaron dos plazas de personal laboral, mediante contratación laboral fija.

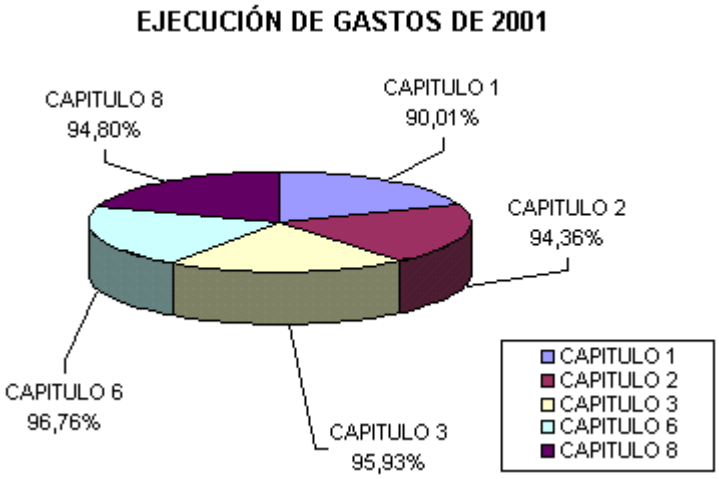
La fase de oposición se celebró (coincidiendo en el mismo día con el resto de la Administración Central) el 25 de noviembre, estando al finalizar el año pendiente de concluir el proceso de contratación.

* Ejecución del Plan de Acción Social de la Agencia de Protección de Datos para 2001, siguiendo las recomendaciones previstas en el Acuerdo Administración-Sindicatos sobre condiciones de trabajo de la Función Pública.

2. GESTIÓN ECONÓMICA Y PRESUPUESTARIA

En cumplimiento de lo dispuesto en el artículo 34 de la Ley Orgánica 15/99 y en los artículos 30 e), 32, 33, 34, 35 y 36 del Real Decreto 428/93 de 26 de marzo por el que se aprueba el Estatuto de la Agencia se han llevado a cabo, como cada año, las siguientes tareas y funciones:

* Ejecución y seguimiento presupuestario



* Modificaciones presupuestarias.
* Contratación y la gestión presupuestaria del gasto.
* Gestión de los ingresos de la Agencia de Protección de Datos que han tenido su procedencia de transferencias establecidas en los Presupuestos Generales del Estado, intereses de cuentas corrientes, así como el pago de las sanciones impuestas por la Agencia en el ejercicio de la postestad sancionadora.
* Contrato de arrendamiento:

Durante el año 2000 se llevó a cabo la operación de localizar para la Agencia unos locales acorde con sus necesidades y con previsión de futuro, dado que los que se tenían en su momento ya no respondían a los requerimientos existentes y por otro lado el arrendamiento finalizaba al término del año.

El 24 de julio de 2000 se firmó un contrato de arrendamiento de un edificio sito en la calle Sagasta 22 de Madrid.

Durante el mes de enero de 2001 se llevó a cabo la mudanza de la primitiva sede a la actual. Este nuevo edificio cuenta con una entreplanta especialmente dedicada a la Atención al Ciudadano y cinco plantas más en los que se distribuyen las distintas dependencias de la Agencia.

Así mismo, se mantiene contrato de arrendamiento de un pequeño local destinado a almacén del Ente Público.

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

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

3. OTRAS FUNCIONES Y TAREAS

* Notificación de las resoluciones del Director en cumplimiento de lo establecido en el artículo 30, b) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Total de Notificaciones efectuadas: 2.091

* De Procedimientos a Administraciones Públicas: 144
* De Actuaciones Varias: 543
* De Procedimientos Sancionadores: 666
* De Tutela de Derechos: 738

Estas cifras no tienen porqué coincidir necesariamente con las de expedientes, procedimientos y actuaciones de la Inspección (ver el apartado de la Memoria dedicado a la Inspección de Datos), toda vez que una actuación inspectora habitualmente da lugar a diversas notificaciones por la existencia de una pluralidad de personas que legalmente deber ser notificadas.

* Registro de Entrada y Salida de documentos en la Agencia:

* Registros de Entrada: 26.062 (incremento del 21,51% respecto al 2000).
* Registros de Salida: 47.330 (incremento del 18,93% respecto al 2000).

En cumplimiento del mandato establecido en el artículo 22 del Estatuto de la Agencia la Secretaría General ha actuado

como Secretaría del Consejo Consultivo en las 4 reuniones celebradas durante el año 2001. El contenido de las reuniones se concreta en el apartado de la memoria relativo al Consejo Consultivo.

Ha sido también competencia de la Secretaría General la organización, en colaboración con el Gobierno de La Rioja, de unas Jornadas sobre "Protección de Datos Personales por las Administraciones Públicas" celebradas en Logroño los días 5 y 6 de julio.

Así mismo, se ha llevado a cabo las convocatorias, fallos y entrega de los galardones de los Premios "Protección de Datos Personales" y Periodismo "Protección de Datos Personales", Convocatoria 2001.

De estas dos últimas acciones se da extensa información en el epígrafe de esta Memoria "OTRAS ACTIVIDADES"

4. EL ÁREA DE ATENCIÓN AL CIUDADANO

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD) dentro de su artículo 37.e), establece como una de las funciones de la Agencia de Protección de Datos la de proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos de carácter personal. Esta función viene atribuida a la Secretaría General de la Agencia por el artículo 31.d) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia y se ejerce a través del Área de Atención al Ciudadano.

Esta área constituye en la mayoría de las ocasiones, la primera aproximación que tiene a su disposición el ciudadano para poder informarse y plantear aquellas consultas que considere necesarias en orden a la aplicación de la LOPD a su caso concreto. Ello implica, como ya se ha venido poniendo de relieve en memorias anteriores, que una de las funciones primordiales de esta Unidad, es la de tratar de informar a los ciudadanos de la forma más sencilla posible sobre aquellas cuestiones que les preocupan directamente, facilitándoles la orientación y ayuda que precisen para una mejor defensa de sus derechos, e indicándoles los diferentes aspectos que se regulan en la LOPD y en el resto del ordenamiento jurídico de aplicación en esta materia.

Seguidamente y dando cuenta de las diferentes formas en que se presta la atención al ciudadano, se puede distinguir de una parte, la atención personalizada que a lo largo del año 2001 ha representado un total de 19.925 consultas, y de otra parte, la información que se obtiene directamente a través de la página Web de la Agencia cuyo desglose se analiza más adelante.

Por lo que se refiere a la atención personalizada se indica que la misma se viene realizando, al igual que en cualquier otro órgano de la Administración Pública, de tres formas, y así se distingue: la atención telefónica, la atención presencial y la atención por escrito. En el siguiente cuadro se detalla el número total de consultas atendidas en el año 2001 en las tres modalidades.

Atención telefónica	Atención presencial	Atención por escrito	Total
15.634	1.890	2.416	19.940

Durante el año 2000 el número de consultas fue:

Atención telefónica	Atención presencial	Atención por escrito	Total
14.420	1.878	2.964	19.262

Por lo que se refiere a la información obtenida a través de la página Web se destaca que, a través de ella se pueden consultar los siguientes apartados: una guía informativa acerca de los principios de la LOPD; los modelos para ejercer los derechos de acceso, rectificación y cancelación; las recomendaciones a usuarios de Internet; las recomendaciones al sector de comercio electrónico, que se ha incluido como novedad en el año 2001 fruto de una inspección de oficio al sector; la legislación en la materia de protección de datos; los modelos de cuestionarios para notificar la inscripción de ficheros tanto de titularidad pública como privada al Registro General de Protección de Datos; el programa informático para la declaración de ficheros a través de Internet y el catálogo actualizado de ficheros inscritos en la Agencia. También se puede acceder al apartado de consultas más frecuentes que ya se incorporó como novedad en el año 2000 y que como se detallará más adelante ha supuesto una importante fuente de información para el ciudadano.

En el siguiente cuadro se concreta el número total de accesos que ha tenido la Web durante el año 2001

Número total de accesos a la página Web durante el año 2001

Enero	113.102
Febrero	128.580
Marzo	149.894
Abril	117.723
Mayo	167.037
Junio	164.122
Julio	127.913
Agosto	92.697
Septiembre	113.359
Octubre	143.277
Noviembre	147.043
Diciembre	107.991
Total	**1.572.738**

En el siguiente cuadro se refleja la evolución de los accesos a la Web de la Agencia de Protección de Datos desde el año en que se implantó, que fue 1998, y se ve el considerable incremento que ha tenido esta forma de obtener información, pasando de un total de 216.000 accesos a un total de 1.572.738 accesos, es decir un incremento de un 728 %.

Evolución del número de accesos a la Web de la Agencia

Año	**Nº de accesos**
1998	216.000
1999	506.362
2000	1.173.056
2001	1.572.738

Respecto al acceso al apartado de consultas más frecuentes de la Web, se pone de relieve que el objetivo de la inclusión de este apartado en el año 2000, era el de facilitar el acceso directo a aquellas consultas que eran solicitadas con mayor frecuencia por los ciudadanos, y dicho objetivo se ha visto cumplido a lo largo del año 2001 de forma considerable tal y como se desprende del siguiente cuadro, en el que se recoge el número total de accesos que se han realizado a cada una de las consultas concretas, abarcando los meses comprendidos entre julio y diciembre de 2001 dado que esta información hasta el mes de julio no estaba disponible.

Consulta 1	Publicidad	2.852
Consulta 2	Facturación Telefónica	1.745
Consulta 3	Guías Telefónicas	1.496
Consulta 4	Ámbito de la LOPD	2.056
Consulta 5	Derecho de acceso	1.544
Consulta 6	Derecho de acceso ante la APD	1.820
Consulta 7	Ficheros de Morosos	2.469
Consulta 8	Ficheros de Morosos con datos de fuentes públicas	1.061
Consulta 9	Direcciones Ficheros Morosos	733
Consulta 10	Inscripción ficheros	2.727
Consulta 11	Como se deben declarar ficheros	2.967
Consulta 12	Presentación documento seguridad	2.544
Consulta 13	Seguridad (fichero nóminas)	2.706
Consulta 14	Seguridad (datos de hacienda pública)	1.279
Consulta 15	Seguridad (servicios financieros)	1.302
Consulta 16	Implantación medidas seguridad de nivel medio	2.142
Consulta 17	Sentencia Tribunal Constitucional sobre LOPD	2.545
Total		33.988

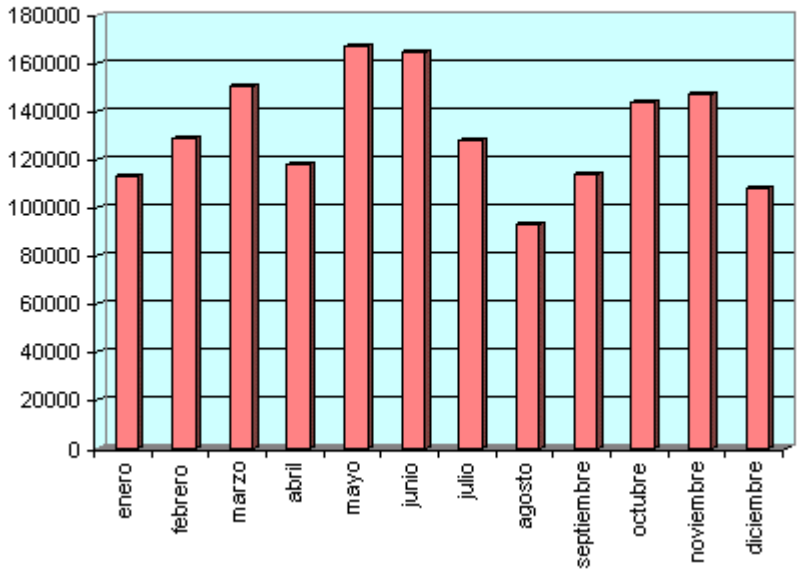
A la vista de todos los cuadros anteriores se pueden obtener unos criterios de valoración respecto a la evolución de las prioridades que el ciudadano va teniendo para obtener información de la Agencia.

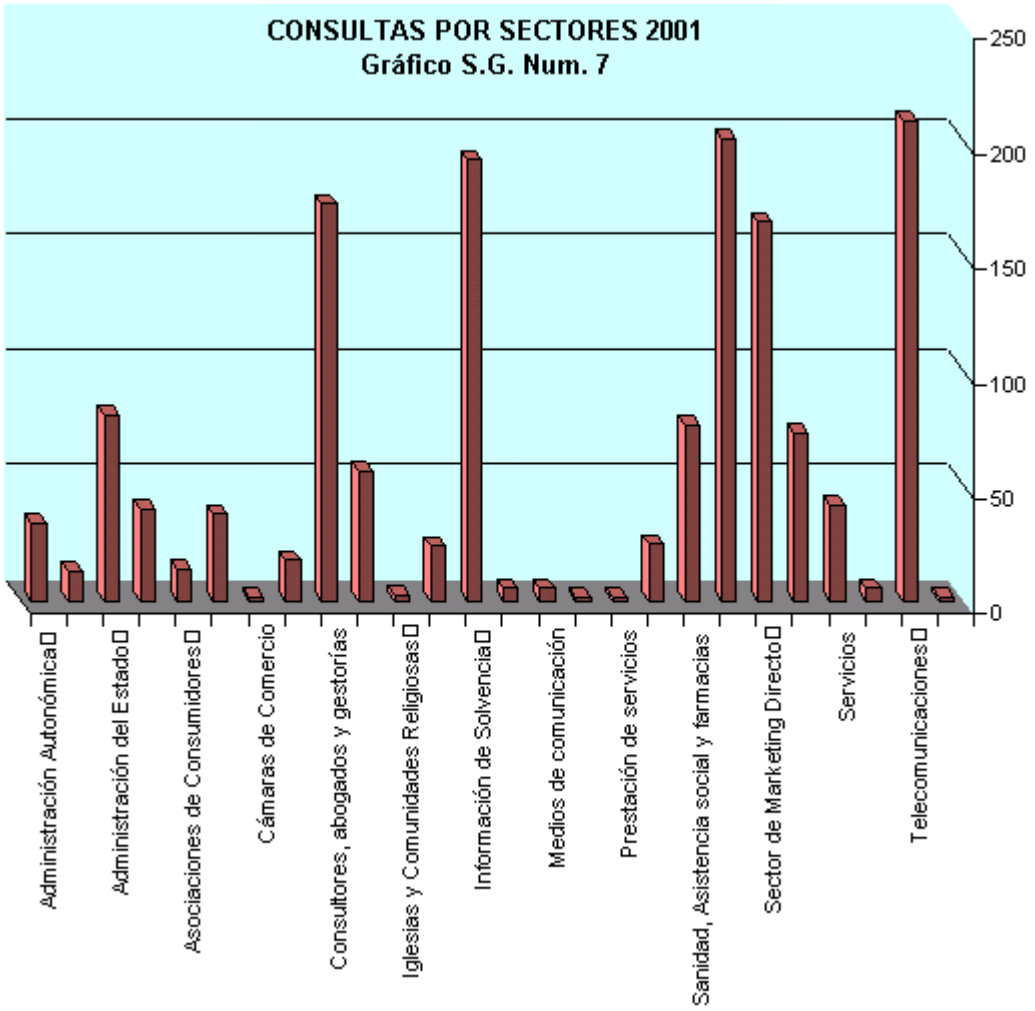
Así, se puede señalar que la atención personalizada en sus tres modalidades, está en la línea del año 2000, con un número total de 19.940 consultas, que representa un incremento de un 3,32%. No obstante existen algunas variaciones que se indican a continuación. Respecto de la atención telefónica se señala que sigue en una línea creciente pasando de 14.420 consultas en el año 2000 a 15.634 en el año 2001, lo que implica que, si se dispusiera de más recursos humanos esta forma de atención seguiría creciendo. La atención presencial en la sede de la Agencia se mantiene en los mismos valores, habiendo decrecido sin embargo las consultas escritas, que han pasado de 2.964 a 2.416

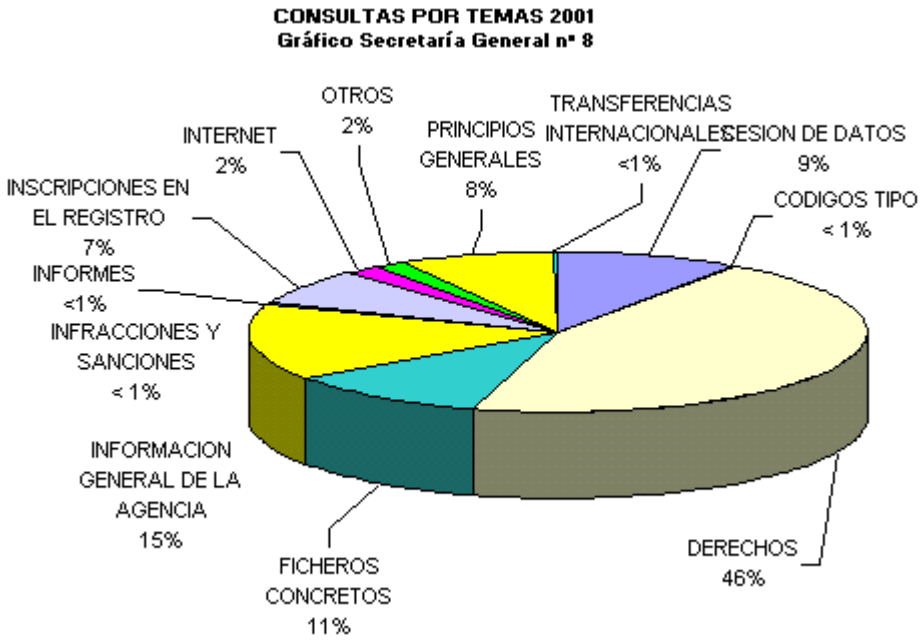
Este decrecimiento anterior tiene su reflejo y es consecuencia del crecimiento que ha experimentado el acceso a las consultas más frecuentes de la Web y ello derivado por la rapidez que representa el acceso a la información a través de Internet. En concreto estas consultas han supuesto en seis meses un total de 33.988, que supone, si lo extrapolamos proporcionalmente al resto del año, un total de 67.000 accesos, que implicaría aproximadamente un 336% de incremento respecto a la forma de atención personalizada, por lo que esta información debe ser potenciada.

Seguidamente, se procede a insertar una serie de gráficos, en donde queda reflejada la distribución por sectores y temas del global de las consultas planteadas durante el año 2001.

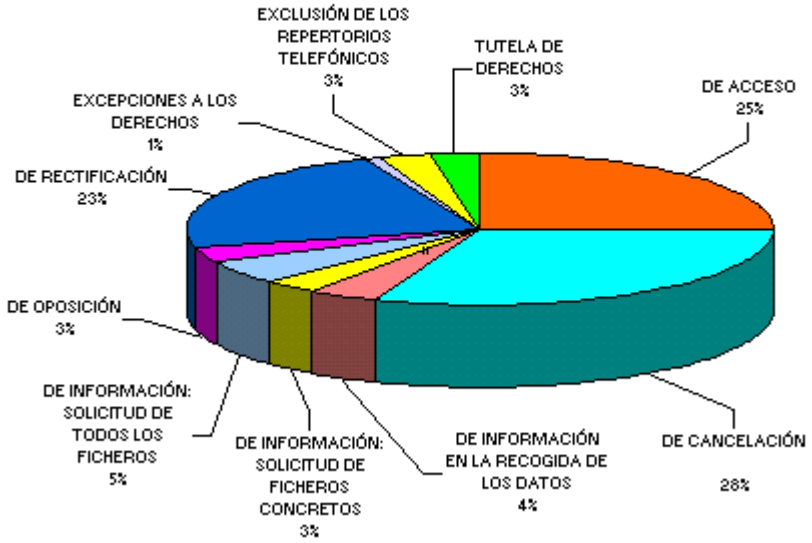
NUMERO TOTAL DE ACCESOS A LAS PÁGINAS WEB DE LA AGENCIA DE PROTECCIÓN DE DATOS
Gráfico Secretaría General nº 6



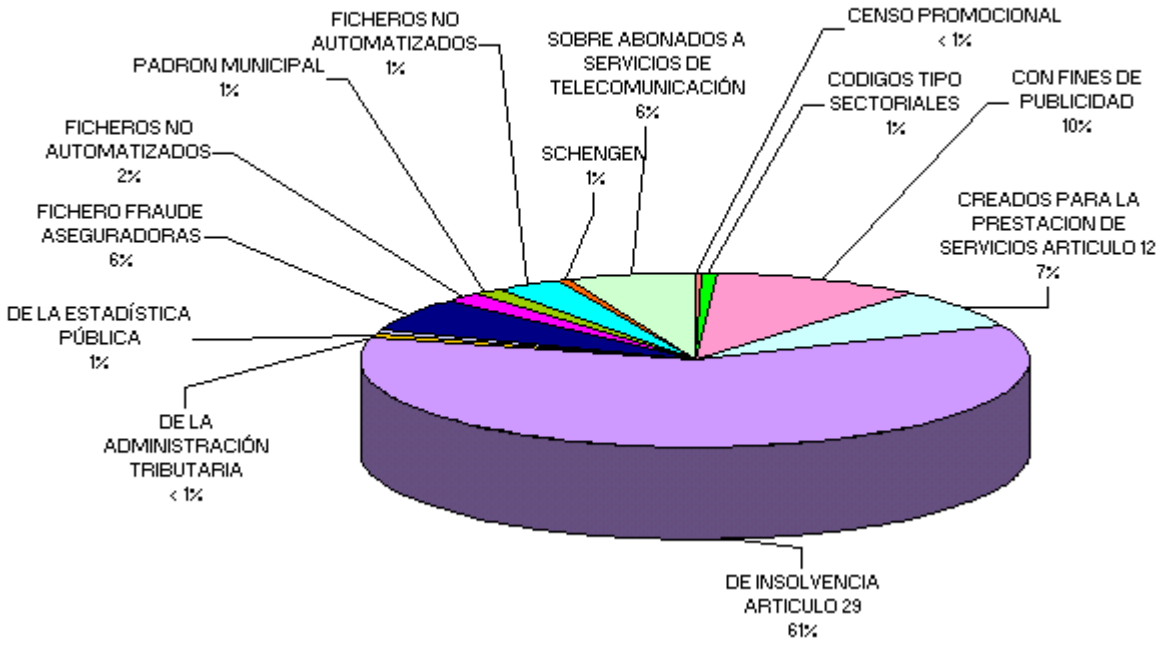

CONSULTAS POR SECTORES 2001
Gráfico S.G. Num. 7
250
200
150
100
50
0
Administración Autonómica
Administración del Estado
Asociaciones de Consumidores
Cámaras de Comercio
Consultores, abogados y gestorías
Iglesias y Comunidades Religiosas
Información de Solvencia
Medios de comunicación
Prestación de servicios
Sanidad, Asistencia social y farmacias
Sector de Marketing Directo
Servicios
Telecomunicaciones

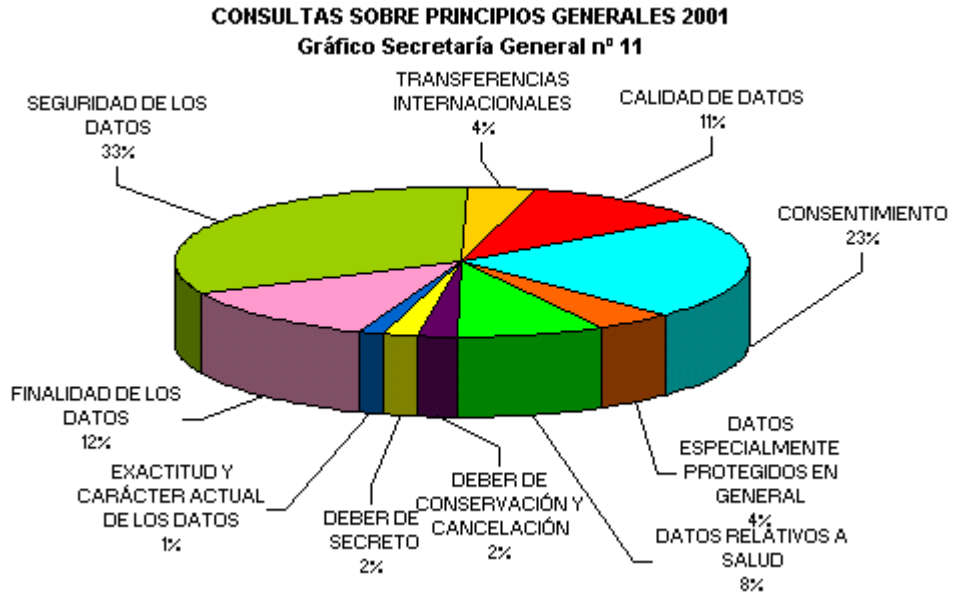

CONSULTAS POR TEMAS 2001
Gráfico Secretaría General nº 8
OTROS 2%
INTERNET 2%
PRINCIPIOS GENERALES 8%
TRANSFERENCIAS INTERNACIONALES <1%
CESION DE DATOS 9%
CODIGOS TIPO < 1%
INSCRIPCIONES EN EL REGISTRO 7%
INFORMES <1%
INFRACCIONES Y SANCIONES < 1%
INFORMACION GENERAL DE LA AGENCIA 15%
FICHEROS CONCRETOS 11%
DERECHOS 46%

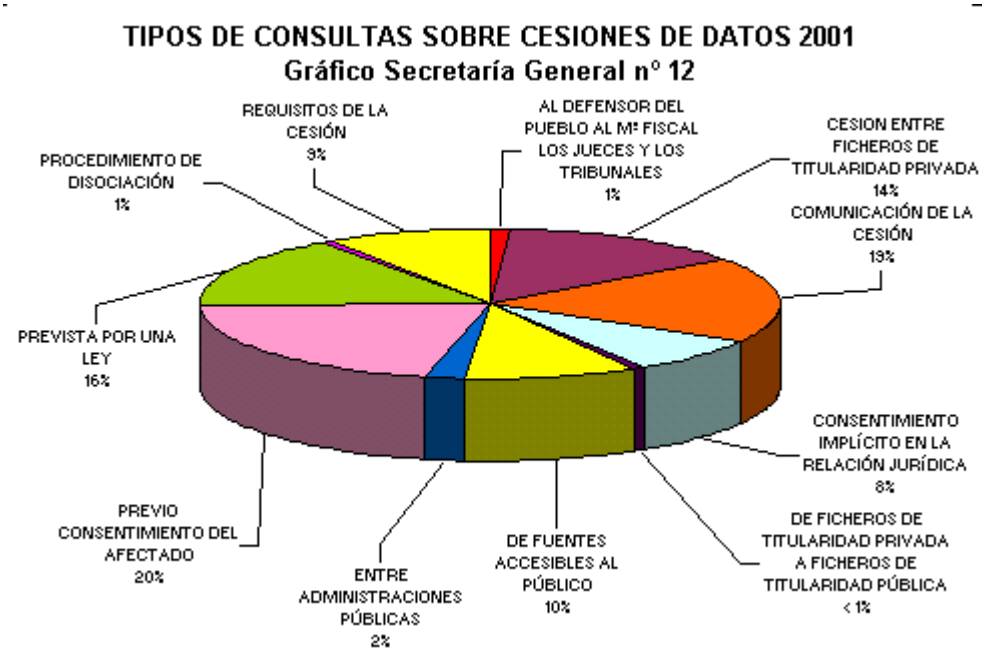
TIPOS DE CONSULTAS SOBRE DERECHOS 2001
Gráfico Secretaría General nº 9



FICHEROS CONCRETOS 2001
Gráfico Secretaria General nº 10







A continuación, y de la misma forma que en las memorias de los años anteriores, dado el interés que las consultas de los ciudadanos pueden presentar, se procede a publicar en esta memoria aquellas consultas que se ha considerado de mayor importancia por la cuestión planteada, distribuyéndolas en los siguientes apartados:

* INTERNET Y PÁGINAS WEB
* TELECOMUNICACIONES
* VIDEOVIGILANCIA
* RELACIONES LABORALES
* DATOS DE SALUD/ DATOS BIOMETRICOS
* SEGUROS
* REGLAMENTO DE SEGURIDAD
* FICHEROS PÚBLICOS
* EXCEPCIONES A LOS DERECHOS DE ACCESO

4.1. Internet y Páginas Web

Dentro de este apartado, sobre el que hay que indicar que las consultas han sido muy diversas, se incluye en primer lugar una consulta que ha sido varias veces realizada y que va referida a la forma en que se deben de declarar los ficheros en los que se están tratando y recogiendo datos a través de páginas Web. Se recogen otras dos consultas en las que se pregunta sobre cómo se puede ejercitar el derecho de cancelación ante un periódico digital y ante el responsable de una Web de subastas. También se incluye otra consulta sobre si sería correcta la publicación de una lista de admitidos a un proceso selectivo, y finalmente otra sobre la forma de acceso a una Web con contenido pornográfico ubicada en Estados Unidos de América.

4.1.1. Como se deben de declarar los ficheros con datos procedentes de una Web.

Se han planteado varias consultas exponiendo las dudas sobre la recogida y tratamiento de datos a través de páginas Web y si se tenían que declarar o no los ficheros creados con esa información.

En contestación a estas consultas se ha puesto de relieve que, el tratamiento de datos a través de una página Web, en principio, no se diferencia en nada de cualquier otro tratamiento y en este sentido se le aplica en su totalidad la LOPD.

La LOPD establece la necesidad del consentimiento de los ciudadanos para que sus datos puedan ser tratados y cedidos a terceros, exigiendo que el mismo sea libre, inequívoco, específico e informado.

El principio de finalidad viene a establecer que los fines para los que podrán emplearse los datos han de ser, no sólo legítimos como se exigía en la derogada Ley Orgánica 5/1992 Reguladora del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), sino además, determinados y explícitos. Indudablemente viene a concretarse y restringirse el alcance de este principio que junto con el del consentimiento, son principales en toda normativa sobre la protección de la intimidad ante el tratamiento de datos personales, siendo necesario que el afectado conozca en todo caso de forma indubitada las finalidades para las que se procede al tratamiento de sus datos.

En los supuestos planteados en los que se están recogiendo los datos a través de páginas Web, la finalidad concreta y determinada de la recogida y tratamiento deberá venir perfectamente explicada dentro del contenido de la Web.

Se indicó que el derecho a la información previa a la recogida de datos es básico, y la LOPD lo explicita con mayor claridad, al exigirse en todo caso y sin excepción alguna, que se informe al afectado de la existencia del fichero, de la finalidad de la recogida de datos y de los destinatarios de la información, así como de la identidad y dirección del responsable. Esta información deberá facilitarse a las personas que accedan a la Web previamente a que faciliten cualquier tipo de datos de carácter personal.

Por otra parte, y respecto de la declaración del fichero que se cree con los datos recogidos, se indicó que efectivamente dicho fichero quedaría dentro del ámbito de aplicación de la LOPD y en consecuencia tendrían la obligación de proceder a la declaración del mismo al Registro General de Protección de Datos

Se indicó igualmente que la declaración la pueden realizar a través de Internet, o mediante soporte magnético y asimismo se informó de que el formulario en papel para la declaración se puede obtener de la página Web accediendo al apartado Registro General de Protección de Datos o solicitándolo por escrito a la propia Agencia, señalando que tanto el formulario como la inscripción es gratuita.

También se informo de que, de conformidad con el Reglamento aprobado por Real Decreto 994/1999, de 11 de junio (BOE 25-6-1999) deberán de redactar el documento de seguridad regulado en el artículo 8 del referido Reglamento y adaptar las medidas de nivel básico, medio o alto que correspondan. Dicho documento no tiene que ser presentado en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido.

4.1.2. Ejercicio del derecho de cancelación ante un periódico digital

Se planteó una consulta por la que se solicitaba información de cómo se podría hacer efectiva la cancelación de datos personales de la suscripción de un periódico digital.

Se informó de que, accediendo al apartado consultas más frecuentes de nuestra Web, y en concreto a la número 5 "Consulta sobre acceso ante responsable conocido", se podía obtener la información relativa a cómo se ejercitan los derechos de acceso rectificación y cancelación con carácter general.

Por lo que se refiere a la consulta concreta, se indicó que, previamente a contestarla, se ha accedido a la página Web correspondiente del periódico digital, comprobando que figuran al final diferentes apartados entre los que se encuentra el de privacidad.

Accediendo al apartado privacidad se obtiene información respecto a la política de protección de datos, en la que se indica entre otras cuestiones que es miembro de la Asociación Española de Comercio Electrónico y se informa del contenido del artículo 5.1 de la LOPD, identificando igualmente a la empresa administradora de la Web.

En consecuencia, se procedió a informar al solicitante de todo lo anterior, señalándole que para cancelar sus datos, debería dirigirse por correo electrónico a la Central de Usuarios tal y como se específica en la propia página Web, o bien dirigirse por correo postal al responsable de la página anteriormente indicado, acompañando copia de su DNI y utilizando los modelos que tenemos disponibles en nuestra propia Web en el apartado modelos y formularios, proce-

dimiento este último que, para que quede constancia de su petición, es el que habitualmente se recomienda por la Agencia.

4.1.3. Derecho de cancelación ante el responsable de una Web dedicada a subastas

En esta consulta se planteaba la posibilidad de interponer una denuncia ante la Agencia contra la entidad responsable de una página Web, por el tratamiento realizado con los datos personales, dado que no se cancelaban los mismos ante la existencia de una presunta deuda de facturación.

En este caso se procedió a informar que, previamente había que distinguir dos situaciones, que están relacionadas entre si pero que a su vez son independientes. Así de un lado, habrá que distinguir la relación estrictamente comercial derivada del alta realizada en la Web con el objeto de subastar un objeto determinado (en el caso planteado se trataba de un ordenador personal), y de otro lado habrá que diferenciar el tratamiento de los datos personales que, como consecuencia del alta, se ha llevado a efecto por el responsable de la Web.

El artículo 6 de la LOPD establece que, cuando exista una relación negocial, laboral o administrativa, el tratamiento de los datos irá implícito con el consentimiento manifestado para el establecimiento de dicha relación. En consecuencia, el hecho de darse de alta para la subasta, implica que el tratamiento de sus datos personales será lícito y dicho tratamiento durará mientras la relación negocial exista.

En este sentido, el artículo 4.5 de la referida Ley establece que los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Igualmente, el artículo 16 de la LOPD al regular el derecho de rectificación y cancelación establece que, la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

A la vista de esta regulación y enlazándolo con las dos situaciones anteriormente diferenciadas, la entidad responsable de la Web podrá tratar los datos personales en tanto en cuanto subsista la relación negocial, y ésta continuará mientras no se llegue a un acuerdo para solucionar la presunta deuda contraida con el responsable de la Web por la realización de la subasta.

Una vez solucionado el objeto de la reclamación, es cuando sí se podrá exigir del titular de la Web que se cancelen los datos personales, de conformidad con lo previsto en los artículos 6 y 16 de la LOPD y ante la negativa a la cancelación, en el plazo de los diez siguientes a la petición, se podrá denunciar al responsable de la Web ante esta Agencia.

4.1.4. Publicación de una lista de admitidos a un proceso selectivo

En esta consulta se preguntaba sobre si era legal que, introduciendo el nombre del consultante en un buscador de Internet aparecieran sus datos en la Web de la Agencia Tributaria.

En contestación a la consulta se le informó que, precisamente la función de un buscador en Internet es acceder y rastrear, dentro de las páginas Web con las que se conecta, en busca de la información solicitada.

Es por ello que al introducir sus datos en el buscador, la consulta le dirige a donde puedan figurar los datos personales solicitados, y en concreto, en el caso planteado, le dirigió a la página Web de la Agencia Estatal de Administración Tributaria, donde dentro del apartado de recursos humanos se hace pública la lista de admitidos a las pruebas para el cuerpo técnico auxiliar de informática, lista en la cual el consultante se encuentra, al haberse presentado a dichas pruebas.

Se le indicó que la publicación de la lista de admitidos realizada por la Agencia Tributaria forma parte del procedimiento administrativo para la celebración de las oposiciones de acceso al cuerpo técnico auxiliar de informática, por lo que siendo uno de los requisitos administrativos de la convocatoria, todos los aspirantes admitidos deberán figurar en dicha lista y permanecerán en la misma hasta el cumplimiento del plazo correspondiente de exposición que forma parte del procedimiento selectivo.

Respecto de la publicación de dicha lista en Internet se señaló que, en principio no es ilegal, siempre que se haya informado a los aspirantes de que los listados se harían públicos a través de Internet, dado que con ello lo que se pretende es facilitar a las personas esta información de una forma ágil y rápida, evitándoles desplazamientos innecesarios.

4.1.5. Forma de acceso a una Web con contenido pornográfico

Fueron varias las consultas y quejas que se plantearon respecto a la forma de acceso a una página Web con contenido pornográfico, en la que indicando cualquier nombre se entraba en el contenido de la misma.

Se informó al ciudadano que no es que se hubiera creado una página Web con los datos personales de nadie, sino que la forma de acceder a esa página Web era a través de cualquier nombre o clave que se indicase, o simplemente sin poner ningún nombre, completándose la conexión en todas las ocasiones pero accediendo únicamente a la información general de dicha página.

De esta actuación anterior, en principio, no se desprende que exista ningún tratamiento, dado que como se ha indicado es una forma de acceso a dicha página, siendo indiferente el nombre o clave que se indique.

4.2. Sector de telecomunicaciones

4.2.1. Preasignación de operador

Se recibió una consulta exponiendo la queja sobre la actuación llevada a cabo por una empresa operadora de telecomunicaciones, dado que había procedido a realizar con el consultante la preasignación de operador de telecomunicaciones sin su conocimiento, y solicitaba de la Agencia, que se requiriese del operador el contrato de preasignación.

Se procedió a contestarle aclarándole que, de su petición se derivaban dos cuestiones independientes, como son, de un lado, la posible relación comercial derivada de la contratación telefónica con el operador de telecomunicaciones y de otro lado, el tratamiento de sus datos personales por parte de esta empresa en base precisamente a la contratación de la preasignacion de llamadas.

La Agencia únicamente puede centrar la información y posterior actuación en aquel aspecto relacionado con el tratamiento de los datos personales por parte de la empresa de telecomunicaciones, no pudiendo entrar a analizar el procedimiento de preasignación de operador de telefonía, cuya regulación está contenida en el Reglamento sobre Interconexión y Acceso a Redes Públicas y Numeración, aprobado por Real Decreto 1651/1998.

En este sentido se le indicó que el artículo 6 de la LOPD establece la norma general por la que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa, estableciendo también como excepción del consentimiento, precisamente, la existencia de una relación comercial, como podría ser el caso planteado.

Por tanto habrá que saber si el operador tiene una relación comercial con el consultante para su preasignacion.

En este sentido el artículo 19 del Reglamento de Interconexión establece que: " *La preasignación o preselección de operador permite al usuario decidir por adelantado la entidad habilitada que cursará las llamadas, sin necesidad de marcar código de selección de operador antes del número telefónico al que se dirigen dichas llamadas. Cuando se preste la facilidad de preasignación de operador se ofrecerá además la posibilidad de selección de operador llamada a llamada, mediante la marcación del código de selección correspondiente.*

2. El cambio de operador por preselección será coordinado por el operador beneficiario del mismo. Previa solicitud escrita del abonado a dicho operador, éste informará de la misma al operador preseleccionado con anterioridad, comunicándole la fecha de efectividad de tal preselección. El cambio se realizará en un plazo inferior a cinco días, contados desde la recepción de la comunicación....."

A la vista de la regulación anterior es necesario por tanto que el operador preasignado, tenga una solicitud escrita y firmada por el consultante para poder prestarle el servicio, situación que según él no se produce, dado que no les ha enviado ninguna solicitud.

Por tanto se le informó que de existir relación comercial, el tratamiento de los datos personales se podría realizar, por lo que si ejercita el derecho de acceso ante dicha empresa, le deberían de justificar dicho tratamiento, y en caso de no quedar justificado, lo podría poner en conocimiento de la Agencia para que se iniciase un procedimiento de tutela de derechos.

4.2.2. Consultas inversas

Durante el presente año, se han seguido planteando consultas sobre la posibilidad de realizar consultas inversas a los repertorios telefónicos y en este sentido se ha considerado conveniente resaltarlo e insistir en la información facilitada a lo largo del año 2000.

Con carácter general la normativa de aplicación para la consulta de guías telefónicas, tanto en papel como en formato electrónico, está regulada en el artículo 67 del Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones aprobado por R.D. 1736/1998, de 31 de julio, y en él no está prevista la consulta inversa, entendida como el obtener la identidad y/o dirección de una persona a partir de su número de teléfono, fax o dirección de correo electrónico.

Este servicio puede tener importantes efectos negativos para la privacidad, dado que la finalidad de un repertorio con búsqueda inversa es diferente a la de un repertorio tradicional de abonados.

Un directorio telefónico, tal y como está concebido en nuestra legislación específica de telecomunicaciones, permite obtener el número de teléfono de una persona conocida, a partir de su nombre y un criterio geográfico, mientras que la finalidad de una búsqueda inversa es la obtención de la identidad y la dirección de un abonado del que únicamente es necesario conocer su número de teléfono y aunque este recurso de los directorios inversos puede servir a los intereses legítimos en algunos casos especiales de emergencia y seguridad pública, el proporcionar los datos de un usuario a

partir de su número de teléfono, sin disponer del consentimiento del afectado, podría constituir un tratamiento desleal de la información que contravendría el principio de calidad de datos contemplado en el artículo 4 de la LOPD.

A este respecto se puso de manifiesto que este es el criterio de la Autoridad de Control de la Unión Europea según figura en el Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio y cuyo texto fue recogido en la memoria del año 2000 (pags. 707 y siguientes).

4.2.3. Mensajes cortos a teléfonos móviles

Se presentó una consulta por la que interesaba saber si la actuación de una empresa con la que se tiene contratada la prestación del servicio de telefonía móvil, está actuando correctamente respecto al envío de mensajes cortos con noticias de interés general de publicidad.

El artículo 6 de la LOPD establece dentro de su apartado 2, que no será preciso el consentimiento del afectado para el tratamiento de sus datos personales cuando este tratamiento se refiera al mantenimiento de una relación contractual, si bien precisa en su apartado 4 que el afectado, en estos casos, podrá oponerse al tratamiento cuando existan motivos fundados y legítimos a una concreta situación personal.

El artículo 30 LOPD al regular específicamente los tratamientos con fines de publicidad y de prospección comercial, que en principio podría ser de aplicación equiparable a este caso, establece en su apartado 4 que los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciónes que sobre ellos figuren en aquél, a su simple solicitud.

A la vista de dichos preceptos se le señaló que, el tratamiento de los datos personales por parte de la empresa con el objeto de la prestación del servicio de telefonía móvil contratado así como el tratamiento de los datos para el envío de publicidad o noticias a través de mensajes cortos podría ser lícito, siempre que los abonados hubieran sido informados de ello al contratar el servicio y no se opongan al mismo, como parece que sería su caso.

Es por ello, que para el ejercicio del derecho de oposición se le recomienda que lo formalice por escrito, que explique que no desea recibir la publicidad, que acompañe junto con su petición de oposición copia de su DNI para acreditar su personalidad, y que lo envíe con acuse de recibo a la empresa prestadora del servicio.

Si después de ejercitar el derecho de oposición, le siguieran enviando noticias o publicidad, podría solicitar la tutela de derechos ante esta Agencia, acompañando copia de los escritos que haya enviado a la empresa y del acuse de recibo de los mismos.

4.3. Videovigilancia

La consulta iba en el sentido de conocer si la instalación de cámaras de videovigilancia en las estaciones de la red de metro era legal y si debía de procederse a informar a los trabajadores y usuarios de dicha red de su instalación.

Se informó en primer lugar, que había que valorar si las imágenes grabadas se encontrarían sometidas a lo dispuesto en la LOPD, siendo necesario para ello efectuar dos acotaciones previas.

De un lado, se plantea el problema de si dichas imágenes pueden ser consideradas como datos de carácter personal de conformidad a lo establecido en LOPD, debiendo indicarse en este sentido que, los artículos 1 y 2 de la citada Ley, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos personales, siendo definidos éstos en el artículo 3.a) de la Ley Orgánica como "cualquier información concerniente a personas físicas identificadas o identificables".

En consecuencia, las imágenes a las que se refieren sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas imágenes, no encontrándose amparadas en la Ley Orgánica en caso contrario.

De otro lado, y aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el artículo 3 b) de la Ley. Ello supone que en el supuesto de que las imágenes no sean objeto de una organización sistemática, con arreglo a criterios que permitan la búsqueda de las mismas a partir de los datos personales de una determinada persona, el archivo en que se contuvieran las cintas de vídeo referidas a dichas personas no será considerado fichero a los efectos de la Ley.

Las matizaciones anteriormente señaladas resultan especialmente relevantes, dado que del contenido de la consulta no se desprende que la grabación de imágenes se encuentren incorporadas a ningún fichero estructurado en los términos señalados, por lo que la LOPD no sería de aplicación al supuesto planteado.

En consecuencia, la utilización de videocámaras para las actividades a las que se refieren será posible, sin consentimiento de los afectados, siempre que no pueda procederse a la identificación de las personas que aparecen en las imágenes o, en caso de existir, dichas imágenes no sean incorporadas a un fichero, en los términos definidos, ya que en caso contrario sería preciso el consentimiento del afectado, o que una norma con rango de ley formal permitiese dicha grabación.

4.4. Relaciones laborales

4.4.1. Tratamiento y cesión de datos de los empleados por parte de la empresa donde trabajan.

En esta consulta se interesaba conocer si la empresa donde se trabaja podría solicitar de sus empleados datos relativos a su titulación profesional así como si podría ceder esta información a terceras empresas.

En contestación a las preguntas se indicó que, en materia de protección de datos rige como uno de los principios generales el de calidad de los datos, regulado en el artículo 4 LOPD, en virtud del cual, los datos que se deben recoger son aquellos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

En el caso planteado, la empresa podrá disponer de todos aquellos datos personales que les sean necesarios para mantener la relación laboral, y entre dichos datos podrá conocer el nivel de estudios que tiene cada uno de sus trabajadores, dado que dicho dato en principio no cabe considerarlo como excesivo, pues permitirá a la empresa el valorar el nivel de conocimientos de su plantilla a efectos, por ejemplo, de realizar promociones profesionales dentro de la empresa.

Respecto a si la empresa puede requerir a un trabajador concreto para que desarrolle sus funciones en base a la nueva titulación, se informó que era una cuestión que excedía del ámbito de competencias de esta Agencia dado que afecta plenamente al desarrollo de las relaciones laborales en el seno de la empresa.

Por lo que se refiere a si la empresa podría difundir los datos personales de sus empleados, se le indicó que esta sería una cuestión que quedaría afectada por lo dispuesto en el artículo 11 de la LOPD, rigiendo el principio básico de que para poder ceder datos personales a terceros hace falta el consentimiento de las personas afectadas salvo que se dieran alguna de las excepciones previstas en el apartado 2 del referido artículo.

4.4.2. Creación de ficheros con trabajadores conflictivos

Llama la atención que se insista de nuevo en plantear esta cuestión interesándose en conocer si es legal la posibilidad de crear una base de datos a través de una Web, compuesta por datos de trabajadores que han tenido problemas en empresas, con el objeto de que pueda ser consultada por terceros.

En contestación a la consulta se informó que la creación de un fichero común con datos de trabajadores conflictivos suministrado por las empresas que hayan tenido problemas con estos trabajadores, para así dar a conocer estos datos a terceras empresas que pretendan contratar con ellos, no está previsto en la LOPD como una situación especial y excepcional a la regla general del consentimiento prevista en el artículo 11.

Los únicos ficheros comunes que, con carácter singular, se regulan en la Ley Orgánica son los ficheros de información de solvencia patrimonial y crédito regulados en el artículo 29, conocidos popularmente como ficheros de morosos, así como los ficheros comunes para la liquidación de siniestros y prevención del fraude creados por las Compañías Aseguradoras previstos en la disposición adicional sexta de la Ley.

Se puso de relieve por tanto, que la existencia de un fichero común de las características señaladas implicaría, aparte de que dicho fichero debería ser declarado al Registro General de Protección de Datos para su inscripción, el que para la cesión de los datos por parte de las empresas a dicho fichero se necesitaría el consentimiento de los trabajadores afectados, regla general que está prevista en el artículo 11 de la Ley Orgánica que expresamente establece que: "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".

Finalmente se señaló que una actuación contraria a lo previsto en el referido artículo 11, podría ser considerada, de conformidad con el régimen sancionador previsto en la Ley, como una infracción muy grave, pudiendo ser denunciada y en su caso sancionada si queda acreditado el incumplimiento de la LOPD.

4.4.3. Cesión de datos al Comité de Empresa

En contestación a esta consulta en relación a facilitar al Comité de Empresa un censo de trabajadores se informó lo siguiente:

Las competencias de los Comités de Empresa vienen establecidas en el artículo 64 de la Ley del Estatuto de los Trabajadores en donde se regula con carácter específico qué información se les debe de facilitar por parte de la empresa para el ejercicio de sus competencias, no figurando entre dicha información la de la obtención de un censo nominativo de todos los trabajadores de la empresa y los únicos datos personales a los que tienen acceso es a aquellos que consten en la copia básica del contrato, copia que el empresario les debe de facilitar en el plazo de los diez días siguientes a la celebración del mismo.

Es por ello, que el acceso al censo laboral por parte de los representantes de los trabajadores, se limitará al momento de la celebración de las elecciones sindicales de conformidad con lo previsto en el artículo 74 del referido Estatuto.

4.4.4. Tratamiento de datos como consecuencia de un expediente disciplinario

Se planteó por un policía perteneciente al Cuerpo Nacional de Policía, si los datos de su expediente personal podrían tratarse sin su consentimiento como consecuencia de la tramitación de un procedimiento disciplinario.

Se le puso de relieve que la LOPD regula en su artículo 4. 2 que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles para las que se hubieran recogido. El artículo 6 de dicho texto establece, como norma general, que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo que una ley disponga otra cosa, o que se den alguna de las circunstancias reguladas en el apartado 2 de dicho precepto, tales como la existencia de una relación negocial, laboral o administrativa.

El Real Decreto 884/1989 regula el procedimiento reglamentario del régimen disciplinario de los funcionarios del Cuerpo Nacional de Policía en desarrollo de lo previsto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, especialmente por lo dispuesto en el capítulo II de su título I y en la sección 4 del capítulo IV de su título II.

Dichas normas, al igual que, las que con carácter general regulan el régimen disciplinario de los Funcionarios de la Administración del Estado, en definitiva vienen a establecer la tipificación de las diferentes infracciones y sanciones que se pueden cometer por los funcionarios y el procedimiento administrativo que hay que seguir para poder formalizar la correspondiente sanción.

Por lo tanto, el tratamiento de los datos personales que en este tipo de procedimientos se pueda realizar, estaría habilitado por ley y no precisaría del consentimiento de las personas afectadas.

Finalmente se puso de relieve que la Agencia no podría entrar a analizar la tramitación del procedimiento, por lo que si el afectado no estuviera conforme con el mismo, se deberán utilizar las vías de los recursos correspondientes.

4.5. Datos de salud / Datos biométricos

Han sido varias la consultas planteadas sobre el tratamiento de los datos relativos a la salud, básicamente centradas sobre qué datos pueden tener esta consideración en relación fundamentalmente con las medidas de seguridad a aplicar, dado que de acuerdo con el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal aprobado por Real Decreto 994/1999, de 11 de junio, les sería de aplicación el nivel alto de protección.

4.5.1. ¿Qué se deben de considerar datos de salud?

Para contestar a esta pregunta se ha partido de los informes del Servicio Jurídico de la Agencia en los que se ha estudiado este tema.

Por datos de salud debe partirse del concepto que quepa dar a los mismos, a partir de las normas, nacionales e internacionales, vigentes en España.

La norma esencial en la protección de datos de carácter personal en nuestro país es la LOPD. Sin embargo esta norma, si bien se refiere expresamente a los datos de salud, considerándolos especialmente protegidos y limitando la posibilidad de su recopilación y cesión, no establece un concepto concreto de este tipo de datos.

Ello exige, para la delimitación del concepto establecido en la Ley Orgánica, atender, por imperativo del artículo 10.2 de nuestra Constitución a las normas contenidas en Tratados Internacionales reguladores de la protección de datos de carácter personal que hayan sido ratificados por España, pasando a formar parte de su ordenamiento interno, según dispone el artículo 1.5 del Código Civil.

En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, como el artículo 6 del Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, formalizado en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección, de tal forma que, como indica el citado Convenio, tales datos "no podrán tratarse automáticamente a menos que el derecho interno prevea garantías adecuadas".

El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de "datos de carácter personal relativos a la salud", considerando que su concepto abarca "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo".

En este mismo sentido, la Recomendación nº R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos afirma que "la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas".

4.5.2. Tratamiento de datos biométricos

En el caso del tratamiento de datos biométricos, han sido varias las consultas que se han interesado por si este tipo de

datos pudieran tener una regulación específica.

En estos casos se ha procedido a señalar que, en primer lugar debe partirse del análisis de la incidencia que los datos biométricos tienen en el ámbito de aplicación de la LOPD.

Son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etcetera.

No obstante la exactitud del sistema y el hecho de que acostumbren a utilizarse en medios policiales, es lo cierto que el procesado de datos biométricos y su vinculación con la identidad de los ciudadanos no tiene por que tener mayor transcendencia respecto de la privacidad que los métodos más tradicionales y menos exactos que se emplearon con anterioridad (códigos secretos, la firma, etc.) siempre que sea a efectos identificativos. Por ello, la obtención y el uso de datos biométricos tales como la huella dactilar, el iris del ojo, etc. no tienen por que considerarse, en sí, como un sistema que altere los sistemas tradicionales.

El artículo 4.1 de la LOPD establece, efectivamente, que los datos sometidos a tratamiento no deben ser excesivos en relación con el ámbito y las finalidades legítimas para las que se han obtenido.

La información contenida en los datos biométricos no contiene ningún aspecto concreto de la personalidad y tan sólo, cuando dicha información se vincula a la identidad de una persona, es posible identificarla con toda certeza, de modo que los datos que se recaban no pueden considerarse de mayor trascendencia que los relativos a un número de uso personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos.

Obviamente, en el caso de que se procediera a ceder la información o a utilizarla con finalidades distintas de aquellas para las que se obtuvieron, tal actuación supondría una violación de la LOPD y daría lugar a la necesaria intervención de la Agencia de Protección de Datos.

4.6. Sector Seguros

4.6.1. Cesión de datos al Fichero Histórico de Seguros del Automóvil

Han sido varias las quejas y consultas planteadas por los ciudadanos respecto a este tema, manifestando su disconformidad con que se cedan sus datos personales derivados de la contratación de una póliza de seguros de automóvil al fichero común creado por la Unión de Aseguradoras.

En estos casos se ha enviado información explicando que, en virtud de la disposición adicional sexta de la LOPD se ha modificado el artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados con la siguiente redacción:

"Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la Ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

A la vista de lo establecido en esta disposición, la creación del fichero histórico de siniestros de UNESPA es acorde con la LOPD y, ningún tomador de la póliza de seguros, podría oponerse a la cesión de sus datos a este fichero por parte de su compañía de seguros, en el caso de que esté adherida al Código.

En el Registro General de Protección de Datos figura inscrito a nombre de UNESPA el Código Tipo "fichero histórico de seguros del automóvil" como fue puesto de relieve y publicado en la memoria correspondiente al año 2000.

Como garantía de que los datos personales, una vez introducidos en el fichero histórico, no pueden ser consultados en cualquier momento, el propio Código Tipo prevé que las entidades adheridas no podrán volcar el contenido íntegro del fichero común en sus bases de datos. Para efectuar las consultas será necesario que se haya producido una solicitud de aseguramiento del interesado ante la entidad que consulta el fichero y, dicha entidad, deberá identificarle correctamente debiendo informar al sistema mediante las claves necesarias.

Como respuesta a la consulta efectuada, el sistema facilitará a la entidad la información que se encuentre en el fichero

relativa a pólizas suscritas, sus correlativos períodos de cobertura, así como de los siniestros y de las garantías aceptadas. En la información que da el sistema no aparecerán datos personales del tomador del seguro ni valoraciones personales de ningún tipo.

Por último, se indica que, el tomador del seguro tendrá la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en el apartado 8.2 del referido Código.

No obstante, para que pueda ser efectivo el derecho de oposición se debe acreditar la existencia de motivos fundados y legítimos relativos a una concreta situación personal.

Igualmente se indicó que también se podría utilizar la vía de plantear una tutela de derechos ante la Agencia de Protección de Datos ante la negativa de facilitarle el acceso, rectificación, cancelación u oposición al tratamiento de sus datos de conformidad con lo previsto en el artículo 18 de la LOPD.

4.7. Reglamento de seguridad

4.7.1. Plazos para la implantación de las medidas de seguridad

En esta consulta que ha sido reiteradamente planteada, se solicita información acerca de los plazos de implantación de las medidas de seguridad.

Se ha venido informando que, estos plazos están regulados en la Disposición Transitoria Única del Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, que entró en vigor el 26 de junio de 1999, diciendo así:

" En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento."

En consecuencia y a la vista de la disposición anterior las medidas de nivel básico y medio ya han debido de ser implantadas, pues su plazo ha finalizado. Respecto de las medidas de nivel alto, el plazo de implantación finalizaba, en principio, el dia 26 de junio de 2001, si bien ha sido ampliado hasta el dia 26 de junio de 2002 por Acuerdo de Consejo de Ministros publicado en el BOE de 25 de junio de 2001.

También se señaló que, en el supuesto de que el fichero no estuviera en funcionamiento con anterioridad a la entrada en vigor al referido Reglamento, no serán de aplicación los plazos previstos en la disposición referida y las medidas en cualquiera de sus tres niveles, básico, medio o alto, deberán adoptarse antes de la puesta en funcionamiento del fichero o tratamiento.

4.7.2. Control de acceso a locales

En esta consulta se estaba planteando que medidas de seguridad se deberán implantar de conformidad con el Reglamento de Medidas de Seguridad, para controlar el acceso a los locales donde estén ubicados los servidores de los sistemas informáticos de la empresa.

En contestación a la consulta planteada se indicó que en el Reglamento de Medidas de Seguridad la única previsión que se hace al respecto es la contenida en el artículo 19 previendo que el único personal que podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información, es aquel que esté autorizado en el documento de seguridad.

Una vez hecha esta previsión, sin embargo no se concretan que tipo de medidas se pueden establecer para controlar el acceso, y en este sentido a modo de referencia se le puso de manifiesto que a los efectos de establecer los sistemas de control de accesos a los locales, los responsables tienen que mantener unos controles de acceso efectivos.

4.8. Ficheros públicos

4.8.1. Ficheros Policiales

En relación con los ficheros policiales, se ha interesado conocer sobre todo, aquellas cuestiones relativas a si la policía puede o no acceder a información personal de los ciudadanos.

En este sentido se informó que los ficheros policiales tienen una regulación especial contenida dentro del artículo 22

de la LOPD y en base a ella, la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

A la vista de la regulación mencionada, el artículo 22 habilita a todas las Fuerzas y Cuerpos de Seguridad del Estado para la obtención y tratamiento de los datos, lo que llevará aparejada la procedencia de la cesión instada del responsable del fichero en su caso, siempre y cuando se cumplan las siguientes condiciones:

???Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales.

???Que se trate de una petición concreta y específica, al no ser compatible con lo señalado el ejercicio de solicitudes masivas de datos.

???Que la petición se efectúe con la debida motivación, que acredite su relación con lo supuestos que se han expuesto.

???Que, en cumplimiento del artículo 22.4, los datos sean cancelados cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento.

4.8.2. Padrón Municipal

Sobre la obtención de datos del Padrón Municipal, se ha recogido una consulta planteada por una Asociación de Vecinos sobre si dicha Asociación tendría legitimación para acceder a los datos del Padrón Municipal de Habitantes y en caso positivo se pregunta sobre el tipo de datos a los que se podría acceder y en que condiciones.

En contestación a la consulta se informó que, con carácter general, y según dispone el artículo 11.1 de la LOPD "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". La regla general anterior tiene una serie de excepciones reguladas en el apartado 2 del propio artículo 11, entre las que se encuentra la excepción legal que permite la cesión cuando una ley lo establezca.

En particular, y en lo referente al Padrón Municipal de Habitantes, el artículo16.3 de la Ley Reguladora de las Bases del Régimen Local prevé que sólo procederá la cesión de los datos contenidos en el padrón municipal a otras Administraciones en los supuestos en que dicha cesión se refiera a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio.

Dado que el precepto citado limita la cesión de los datos del padrón a las Administraciones Públicas y que la Asociación consultante carece de dicha naturaleza, la cesión no se encontraría amparada por lo establecido en la Ley de Bases de Régimen Local y, en consecuencia resultará contraria a lo establecido en la Ley Orgánica 15/1999.

Se informa también que, la posibilidad del derecho de acceso a los archivos y registros de las Administraciones Públicas, consagrado por el artículo 105.b) de la Constitución y regulado por los artículos 35 y 37 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, tal y como reiteradamente ha señalado el Tribunal Supremo, no puede entenderse prevalente sobre la garantía del derecho fundamental a la protección de datos de carácter personal, quedando el acceso limitado en los supuestos en que los archivos y registros contuvieran datos de carácter personal a las previsiones reguladoras de la protección de datos. Así se desprende también de la doctrina sentada por nuestro Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre.

4.8.3. Suministro de agua potable

El consultante exponía su disconformidad con que la empresa, que le está prestando el suministro de agua potable y gestionando las aguas residuales, no proceda a cancelarle sus datos personales, dado que según él no existe un contrato previo de suministro que habilite a dicha empresa para prestar el servicio.

Se le indicó al consultante que el suministro de aguas potables y gestión de aguas residuales es un servicio obligatorio que tiene encomendado cada Municipio en base a lo dispuesto en el artículo 25.2.l) de la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local.

Dicho servicio de naturaleza municipal, se puede prestar por gestión directa de cada uno de los Ayuntamientos, o bien adjudicando la prestación del servicio a una empresa, previa la tramitación del correspondiente procedimiento.

A la vista de lo anterior, no es necesario que los vecinos contraten la prestación de este servicio, sino que es el propio Ayuntamiento el que tiene la obligación de dárselo, y en este sentido, por lo que se refiere a la regulación del tratamiento de datos recogido en la LOPD, no será necesario el consentimiento de los afectados para el tratamiento de sus datos de conformidad con lo previsto en el artículo 6, dado que dicho tratamiento deriva de la relación administrativa que como vecinos tienen con el Ayuntamiento prestador del servicio público, y el hecho de que no sea el propio Ayuntamiento, sino la empresa que tiene adjudicada la concesión municipal para la prestación del servicio, en el caso

consultado, la que procede al tratamiento de sus datos, también en forma legal, sería conforme con lo previsto en el artículo 12 de la LOPD, mientras dure la concesión.

4.8.4. Acceso al Registro de Vehículos y Conductores de la Dirección General de Tráfico.

En contestación a la consulta planteada por la que se interesa conocer en que condiciones y cuales son los supuestos autorizados para uso por parte de la Guardia Civil al archivo de conductores y vehículos de la Dirección General de Trafico, se informo en primer lugar de la regulación legal que tienen este tipo de ficheros, y después se le informo de la excepción que a este respecto queda regulada en el artículo 22 de la LOPD.

El Registro de Conductores e Infractores a que se refiere el artículo 5.h), del texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto Legislativo 339/1990, de 2 de marzo, será llevado y gestionado por la Dirección General de Tráfico, de conformidad con lo previsto en el artículo 84 del Reglamento General de Conductores (R.D. 772/1997)

La Dirección General de Tráfico como titular del órgano responsable del Registro o fichero automatizado, tiene la obligación de adoptar las medidas de gestión y organización que sean necesarias para asegurar, en todo caso, la confidencialidad, seguridad e integridad de los datos automatizados de carácter personal existentes en el registro y el uso de los mismos para las finalidades para las que fueron recogidos, así como las conducentes a hacer efectivas las garantías, obligaciones y derechos reconocidos en la LOPD.

Esta obligación implica, con carácter general, que la información contenida en dicho Registro únicamente se podrá facilitar a cada interesado y respecto de sus propios datos que figuren inscritos, y ello en base al ejercicio del derecho de acceso regulado en el artículo 15 de la LOPD.

En cuanto a la anotación en dicho registro de las sanciones impuestas a los titulares de los permisos de conducir, se le señala que esta materia está expresamente regulada en el artículo 19 del Reglamento de Procedimiento Sancionador en materia de tráfico, circulación de vehículos a motor y seguridad vial, aprobado por R.D. 3209/1994 de 25 de febrero.

En dicho precepto se establece que, una vez que adquieran firmeza las sanciones graves y muy graves, serán anotadas por la Jefatura de Tráfico instructora del expediente en el Registro de Conductores e Infractores y cuando proceda, en los Registros a que se refiere el artículo 5, párrafo h), del Texto Articulado de la Ley sobre tráfico, circulación de vehículos a motor y seguridad vial y se cancelarán de oficio o a petición del interesado, a efectos de antecedentes, una vez transcurridos seis meses desde su total cumplimiento o prescripción.

Igualmente se regula que los datos relativos a las sanciones anotadas en los Registros sólo se certificarán a petición del propio interesado, de las autoridades judiciales o de las administrativas con potestad sancionadora en materia de tráfico y transcurrido el plazo de los seis meses, únicamente se podrán utilizar por la Dirección General de Tráfico para fines estadísticos o de gestión reglamentaria.

Por otra parte se puso de manifiesto que el Real Decreto 2822/1998, de 23 de diciembre, aprueba el Reglamento General de Vehículos, cuyo artículo 2 dispone que: "El Registro de Vehículos tendrá carácter puramente administrativo, será público para los interesados y terceros que tengan interés legítimo y directo mediante simples notas informativas o certificaciones (...). Tendrá también función coadyuvante de las distintas Administraciones Públicas, Organos Judiciales y Registros Civiles o mercantiles con los que se relaciona".

Por consiguiente la consulta al fichero Vehículos, a diferencia del Registro de Conductores, es una consulta pública y será informada por la Dirección General de Tráfico a los interesados y terceros que acrediten un interés legítimo y directo en su consulta, como puede ser por ejemplo el averiguar quien es la parte contraria de un siniestro.

Finalmente se señaló que la LOPD tiene una regulación especial contenida dentro de su artículo 22 y en base a ella, la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

A la vista de la regulación mencionada, se indica que el artículo 22 habilita a todas las Fuerzas y Cuerpos de Seguridad del Estado para la obtención y tratamiento de los datos, siempre y cuando se cumplan las condiciones que ya han sido expuestas.

4.8.5. Campaña del Censo 2001

A raíz de la realización del censo de población y viviendas llevado a cabo por el Instituto Nacional de Estadística a partir del mes de octubre de 2001, han sido varias las quejas y consultas recibidas en las que se manifiesta no estar conformes con el tipo de preguntas y la información solicitada a los ciudadanos.

En contestación a estas quejas se ha informado que el Instituto Nacional de Estadística está realizando los censos de población y viviendas, censos que desde el año 1900 se vienen realizando cada 10 años y que están sometidos en su elaboración a la Ley 12/1989, de 9 de mayo, de la función estadística pública.

De la información que se obtiene a través del censo se permitirá a la Administración la planificación de políticas demográficas, sanitarias, educativas, asistenciales o medioambientales, así como la evaluación de sus resultados.

En concreto y por lo que se refiere a los datos solicitados en este Censo 2001, se le indica que los cuestionarios fueron sometidos al informe de esta Agencia y se puso de manifiesto que el contenido de los mismos cumplían con el principio de proporcionalidad, esencial para su adaptación a los previsto en el artículo 4.5 de la Ley 12/1989, dado que existía una adecuada correlación entre la información solicitada y el resultado que de la misma se pretende obtener.

También se le señala que cualquier información estadística que se haga publica por el INE como consecuencia del censo de población y vivienda, nunca podrá hacer referencia a datos personales de ningún ciudadano, dado que ello contravendría el secreto estadístico regulado en la propia ley 12/1989 y podría ser objeto de denuncia ante esta Agencia que tiene la función de velar por el cumplimiento, en el ejercicio de la función estadística pública, de los principios de secreto, transparencia, especialidad y proporcionalidad.

Finalmente se indica que junto con los censos de población y vivienda se están recogiendo los datos del Padrón Municipal y dicha recogida resulta adecuada, actuando el Instituto Nacional de Estadística en su función de control de los datos contenidos en el Padrón Municipal, en los términos derivados de los artículos 17 de la Ley reguladora de las Bases del Régimen Local y 78 y 79 del Reglamento de Población y Demarcación Territorial de las Entidades Locales aprobado por Real Decreto 212/1996, de 20 de diciembre.

4.9. Excepciones a los derechos de acceso

Dentro de este apartado se va a recoger una excepción al ejercicio del derecho de acceso que deben de conocer los ciudadanos, dado que en determinadas ocasiones se pretender ejercitar tutelas de derecho ante la Agencia por la falta de contestación al acceso solicitado, y ello no es posible derivado precisamente de que este derecho, así como el de cancelación, rectificación y oposición, tienen un carácter personalísimo que impiden que nadie que no sea el propio afectado pueda ejercitarlos.

Como norma general, el Real Decreto 1332/1994 en su artículo 11 establece el carácter personal de estos derechos, señalando que no obstante podrá actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

Fuera de los casos de minoría de edad y de incapacidad, también se pueden presentar otras circunstancias especiales que aunque no vienen contempladas específicamente en la Ley, sin embargo pueden dar lugar a que se denieguen los accesos por los responsables. Así se puede dar en el supuesto de pretender ejercitar estos derechos a través de representante y no encontrarse en situación de minoría de edad o incapacidad.

4.9.1. Representación en el ejercicio del derecho de acceso

En esta consulta se interesaba conocer si la actuación del Registro de Aceptaciones Impagadas es correcta, al haberse negado a cancelar los datos personales dado que el ejercicio del derecho de cancelación se había realizado a través de un despacho de abogados.

Como punto de partida deberá tenerse en cuenta para resolver esta cuestión lo dispuesto en el artículo 11, párrafo primero, en conexión con el artículo 14.2, ambos del Real Decreto 1332/1994. A tenor del primero de estos preceptos los derechos de acceso a los ficheros, 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 LOPD.

Por su parte, el artículo 14.2 establece que "tratándose de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado". En este mismo sentido se pronuncian las normas primera (apartado primero) y segunda (apartado quinto) de la Instrucción 1/1998 de la Agencia de Protección de Datos.

Estos preceptos deberán ser interpretados tomando en consideración el hecho de que la LOPD, según su artículo primero tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, y siguiendo el llamado "principio de interpretación conforme a la Constitución", reiteradamente consagrado por nuestro Tribunal Constitucional, según el cual las normas que conforman nuestro Ordenamiento Jurídico deberán ser interpretadas en el sentido que resulte más congruente con lo que la Norma Suprema establece.

Tomando en consideración todo ello, se entiende que la referencia que el artículo 11 del Real Decreto 1332/1994, relativa al ejercicio de los derechos de acceso, rectificación y cancelación por el afectado, deberá ser interpretada de modo que quede perfectamente conciliado su derecho a que ese ejercicio se produzca de la forma que le resulte menos gravosa (lo que es conforme con las garantías atribuidas por nuestro texto constitucional) con la seguridad de que sólo el interesado podrá ostentar la voluntad adecuada para decidir dicho ejercicio, dado el carácter personalísimo del derecho.

Pues bien, de lo establecido en este precepto, resulta evidente que sólo el interesado podrá efectuar la manifestación de su voluntad consistente en la emisión de una declaración por la que pretenda el ejercicio de los derechos de acceso, rectificación o cancelación, a menos que se trate de una persona que carezca de la suficiente capacidad de obrar, en cuyo supuesto su voluntad podrá resultar suplida por la de su representante legítimo (tal y como prevé el párrafo

segundo). Ahora bien, lo establecido en el citado artículo 11 no obsta a que la declaración de voluntad que inequívoca y específicamente haya de efectuar el interesado pueda ponerse en conocimiento de su último destinatario (el responsable del fichero) a través de la persona a la que aquél haya legítimamente otorgado su representación.

En consecuencia, el artículo 11 del Real Decreto 1332/1994 pretende que nadie, salvo el propio interesado, pueda decidir si quiere ejercitar los derechos que la LOPD le atribuye, ante quién desea ejercitar esos derechos, a qué ficheros se refiere tal ejercicio y en qué condiciones habrá de producirse el mismo pero, una vez efectuada por el interesado una declaración clara, inequívoca y suficientemente explícita en ese sentido, la transmisión al responsable del fichero de esa declaración de voluntad, en los estrictos términos en que aquélla se haya manifestado, podrá encomendarse a un representante voluntario o mandatario, que actuará (dentro de esos límites) ante el responsable del fichero.

Por tanto, se estima que de lo dispuesto en el artículo 11 del Real Decreto 1332/1994 no se desprende una prohibición del ejercicio de los derechos de acceso, rectificación y cancelación por un representante voluntario o mandatario del propio afectado, por cuanto ese ejercicio se producirá siempre en nombre y por cuenta del propio afectado, considerándose el ejercicio del derecho por el mandatario como efectuado por el propio interesado que le confiere la representación (tal y como se desprende *a sensu contrario* de lo dispuesto en el artículo 1717 del Código Civil).

Por otra parte, se entiende que no son admisibles los apoderamientos genéricos, sino aquéllos que se refieran concretamente al ejercicio de alguno de los derechos consagrados por la LOPD ante los responsables de los ficheros, indicando los términos en que el apoderamiento se realiza, sin que el mandatario pueda, en modo alguno, exceder de lo dispuesto en esos términos y sin que quepa atribuir al mismo una potestad genérica de actuación. Esta atribución genérica desvirtuaría la exigencia contenida en el artículo 11 del Real Decreto 1332/1994, por cuanto no supondría una concreta manifestación de la voluntad del interesado de ejercitar los derechos, toda vez que éstos serían ejercidos únicamente si el apoderado lo considerase oportuno y en los términos en que el mismo estimase adecuados.

Por último, en cuanto a los requisitos formales que deberá ostentar el apoderamiento que se confiera, no será posible un mandato verbal puesto que sólo mediante un apoderamiento escrito podrá conocer el responsable del fichero la concreta voluntad de ejercicio del derecho por el afectado. Por otra parte, si el apoderamiento fuera efectuado mediante documento privado sería preciso, a fin de que el mismo pudiera dar fe ante el responsable del fichero que dicho apoderamiento deriva directa e inequívocamente del interesado, titular del derecho protegido, que la firma de éste último apareciera autenticada mediante medio que permitiese a aquél tener perfecto conocimiento de que la declaración de voluntad procede inequívocamente del propio afectado, aportándose por el representante el original de dicho apoderamiento. Igualmente, será posible el ejercicio del derecho por apoderado cuyo poder aparezca otorgado en escritura pública, siempre y cuando dicho apoderamiento cumpla los requisitos de contenido a los que nos hemos referido con anterioridad.

En todo caso, lo indicado hasta ahora debe entenderse aplicable a los supuestos de ejercicio de los derechos ante el responsable del fichero. En caso de que el afectado pretenda solicitar la tutela de sus derechos ante la Agencia de Protección de Datos, conforme a lo establecido en el artículo 17 de la LOPD, la representación se regirá por lo dispuesto en el artículo 32.3 de la Ley 30/1992, según el cual la representación deberá acreditarse "por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado".

MEMORIA DE 2001 - CÓDIGOS TIPO

El art. 32 de la LOPD establece la posibilidad de adoptar acuerdos sectoriales, mediante decisiones de empresa o convenios administrativos, que pueden ser depositados en la Agencia para su inscripción en el Registro.

Las políticas públicas relativas a la protección de la privacidad personal en la sociedad global de la información siguen dos conductas muy diferenciadas, mientras que en unos países están marcadas por unos cánones muy restrictivos, en otros se basan en la liberalización con el objeto de fomentar la actividad empresarial.

En el segundo caso, los códigos tipo tienen un papel fundamental para encontrar el equilibrio entre estas formas de actuación instrumentando la autorregulación a través de acuerdos y códigos privados, estándares de privacidad y sellos de garantía.

En el caso de la Unión Europea, según las pautas recogidas en la Directiva, así como de las discusiones mantenidas por los distintos grupos de trabajo, el objetivo que se pretende conseguir mediante la elaboración de códigos tipo es el de concienciar y educar en materia de protección de datos a los distintos agentes que intervienen en los tratamientos de datos personales: los responsables o personas que deciden acerca del tratamiento, los usuarios o personas que lo realizan y los afectados o titulares de los datos objeto del mismo.

Durante el año 2001 se han presentado solicitudes de inscripción de códigos tipo a través de las cuales se deducía una intención de los solicitantes de obtener una homologación o certificación de la Agencia de Protección de Datos.

A este respecto, debe señalarse que la LOPD no concede a la Agencia las competencias de homologación o certificación de forma que la presentación de un Código Tipo no resulta apropiada para obtener esta finalidad.

1. CÓDIGOS TRAMITADOS EN 2001

Durante el año 2001 se han depositado en el RGPD cinco solicitudes de inscripción de Códigos Tipo. Estos han sido:

Código Ético de Protección de Datos Personales informatizados en empresas y despachos profesionales presentado por la Asociación Nacional de Fabricantes (ANF),

Código Tipo de ACES presentado por la Agrupación Catalana de Establecimientos Sanitarios (ACES),

Código Tipo para el tratamiento de la información referente a personas físicas identificadas o identificables cuando sus datos hayan de ser tratados por personal sanitario o por cuenta del mismo presentado por la Unión Catalana de Hospitales,

Código de Conducta APTICE para el comercio y el gobierno electrónicos, presentado por la Asociación para la Promoción de las Tecnologías de la Información y el Comercio Electrónico.

Proyecto de código tipo de los profesionales de Odontología y de la Estomatología de España.

El *Código Ético de Protección de Datos Personales informatizados en empresas y despachos profesionales* de ANF y el *Código Tipo de ACES* han quedado inscritos en el Registro como se indica a continuación.

El *Código Tipo de la Unió Catalana d'Hospitals* y el *Proyecto de código tipo de los profesionales de Odontología y de la Estomatología de España* no han sido inscritos, el primero de ellos por haber sido archivado a solicitud de la Unió Catalana d'Hospitals y el segundo por no haberse iniciado su tramitación dado que la solicitud no se ajustaba a los requisitos establecidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Por último, el *Código de Conducta APTICE para el comercio y el gobierno electrónicos* tuvo su entrada en el registro de la Agencia el día 27 de diciembre, por lo que no fue posible su inscripción en 2001, encontrándose en tramitación al cierre de esta memoria.

1.1. Código ético de protección de datos personales informatizados en empresas y despachos profesionales

Este código se presentó en la Agencia en abril de 2001. El primer borrador no se adecuaba a lo establecido en el artículo 32 de la LOPD, puesto que se le había dado un enfoque comercial basado en la exigencia de utilización de determinados productos tecnológicos.

A partir de dicha presentación, se estableció un flujo de notificaciones entre la Agencia y ANF en el que por parte de la Agencia se van comunicando las deficiencias de los diferentes borradores del Código, a las que ANF corresponde con nuevas redacciones en las que se van subsanando progresivamente los extremos señalados, y se complementa la documentación aportada.

Finalmente, con fecha 21 de diciembre de 2001 se presentó el texto definitivo de dicho código, solicitando la inscripción de este código tipo en el Registro General de Protección de Datos.

La Resolución de inscripción del Director tuvo en consideración los aspectos que se citan a continuación.

La Asociación Nacional de Fabricantes se constituye en fecha 30 de octubre de 1995, como asociación sin ánimo de lucro, al amparo de lo previsto en la Ley 191/1964, de 24 de diciembre, de Asociaciones.

Pueden ser miembros de la Asociación todas aquellas personas físicas o jurídicas que desarrollen una actividad empresarial, en concreto, fabricantes de cualquier ramo.

En Asamblea General Extraordinaria celebrada en fecha 20 de junio de 2000, se reconoce por los miembros de ANF la necesidad de regular el tratamiento de los datos de carácter personal mediante normas de compromiso voluntario.

Con la elaboración de este Código, ANF ha pretendido arbitrar un sistema que facilite a los miembros de la Asociación que se adhieran al mismo, el cumplimiento de sus obligaciones en materia de protección de datos de carácter personal, y por otra parte, garantizar plenamente la protección de los datos a los titulares de los mismos, así como el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Con este Código se comprometen a tomar una posición activa sobre los datos personales que tienen la obligación de custodiar, lo que supondrá un aumento de confianza de todos los clientes al facilitar sus datos, así como la posibilidad de utilización del "Sello TID de protección de datos", refiriéndose las siglas TID a un tratamiento informatizado o digital de los datos.

El código consta de un preámbulo en el que se identifica a ANF como responsable del código, se indica el objeto y el ámbito de aplicación del mismo. En el primer capítulo se establecen los principios generales respecto a los niveles de seguridad de los ficheros y de la red. El segundo capítulo recoge los derechos de los titulares de los datos, delimitando las fuentes de recogida de datos, el deber de información y la finalidad de los ficheros, y estableciendo los procedimientos para el ejercicio de los derechos de oposición, acceso, rectificación y cancelación. El capítulo tercero se dedica a las técnicas de Internet. En el cuarto capítulo se establecen las modalidades de utilización del Sello de Garantía y en el quinto el procedimiento de control del cumplimiento de las normas del código y resolución de los litigios.

Sólo pueden adherirse al Código Tipo las entidades que pertenecen a ANF, presentando su solicitud por escrito ante esta entidad, aceptando las obligaciones impuestas en el Código, y garantizando, sin perjuicio de que se exija el cumplimiento de los preceptos establecidos por la LOPD y las normas que la desarrollan, que se aplican las siguientes medidas:

* Los ficheros de clientes, objeto del código, en principio, están obligados al cumplimiento de las medidas de seguridad calificadas de nivel básico por el Reglamento de Medidas de Seguridad. Sin embargo, como valor añadido en protección de datos, los adheridos a este código se comprometen al cumplimiento de las medidas de seguridad de nivel medio. Todo ello, siempre que por otras circunstancias no estuvieran obligados al cumplimiento de las medidas de seguridad de nivel alto.

* Previamente a la adhesión al Código se confirma que se ha cumplido con la obligación de inscribir los ficheros con datos de carácter personal en el RGPD .

* La captación de datos personales mediante conexiones telemáticas únicamente se realizará utilizando un sistema de conexión segura, utilizando el protocolo de seguridad SSL de 128 bites, siendo ésta una medida tecnológica que dificulta la captación por terceros de la información transmitida.

* No se utilizará en sus páginas web ninguna técnica que pudiera facilitar la sustracción de información de los equipos que las visitan. Las entidades adheridas al código se comprometen a no explotar comercialmente sus ficheros y a no utilizar buscadores que puedan dar respuesta por aproximación formando dinámicamente listados de datos personales.

* Las empresas y profesionales adheridos al código informarán en su página web de la denominación completa de su razón social y dirección.

En el Código también se recogen otras previsiones que suponen ventajas añadidas para los titulares de los datos:

* Se detallan los derechos de los titulares sobre sus datos de carácter personal, así como los deberes de los adheridos al Código para lograr el respeto de los derechos de los afectados.

* Se enumeran las fuentes de recogida de datos.

* Se regula el procedimiento para el ejercicio de los derechos de acceso, garantizando que la contestación se efectuará por escrito en un plazo no superior a 10 días, cuando el Real Decreto 1332/1994 amplía este plazo hasta un mes.

* También se regulan los derechos de oposición, rectificación y cancelación de los datos de carácter personal, adjuntándose al Código los formularios para facilitar el ejercicio de estos derechos, según los modelos publicados por la Agencia de Protección de Datos.

* Se ofrece un servicio gratuito de asesoramiento sobre cualquier cuestión relacionada con la protección de los datos de carácter personal.

* Se crea un Comité de Protección de Datos para velar por el cumplimiento de las normas contenidas en el Código según las previsiones de autorregulación que se incluyen en el mismo, de acuerdo con lo establecido en el art. 9.4 del Real Decreto 1332/1994. Este comité presentará denuncia ante la Agencia de Protección de Datos en el caso de existencia de violaciones a los principios de la LOPD.

* El Código también ofrece la posibilidad de someterse al Tribunal de Arbitraje del Consejo Empresarial de la Distribución del que es miembro ANF. Sin perjuicio de la potestad sancionadora que puede ejercer la Agencia.

El Director de la Agencia autorizó la inscripción de este Código al considerar que el texto del mismo cumplía los requisitos legales exigidos para su inscripción en el Registro.

No obstante, la resolución contiene una advertencia expresa a ANF de que el "Sello de garantía TID de protección de datos" únicamente podrá implicar el cumplimiento de las previsiones recogidas en el Código, sin que para ello resulte necesario la utilización de una tecnología de seguridad específica.

1.2. Código Tipo de ACES

El segundo código inscrito durante este año ha sido el *Código Tipo de ACES*, presentado por la Agrupació Catalana d'Establiments Sanitaris (ACES), en el mes de junio de 2001, a través de su Director General.

ACES es una asociación privada sin ánimo de lucro, con personalidad jurídica propia, e integrada por centros y establecimientos sanitarios privados del ámbito territorial de Cataluña. Sus Estatutos se encuentran publicados en el Boletín Oficial de la Provincia de Barcelona nº 118, de 18 de mayo de 1977.

La finalidad de la ACES es el asesoramiento, defensa y representación de sus miembros, procurando la optimización de métodos de trabajo y objetivos en general atendiendo fundamentalmente a la promoción de sus intereses sociales, laborales, profesionales y culturales.

Conforme al art. 2 de los Estatutos, pueden formar parte de ACES como socios de número las personas físicas o jurídicas que siendo de titularidad privada desarrollen su actividad principal dentro del sector sanitario.

El *Código Tipo de ACES* tiene su origen en la multitud de consultas planteadas a ACES por parte de sus asociados en relación con el cumplimiento de la normativa legal en materia de protección de datos, con el objeto de dar respuesta a esta problemática, facilitar el cumplimiento de esta normativa y garantizar los derechos de los afectados.

Previamente a la presentación del Código en la Agencia, éste había sido remitido a la Organización de Consumidores y Usuarios de Cataluña (OCUC), contando con el informe favorable de la misma.

Las principales ventajas que presenta el Código son las siguientes:

* Resolver de manera uniforme, a todos los asociados, las cuestiones y dudas surgidas en el proceso de adecuación a la LOPD y sus normas de desarrollo en un sector particularmente sensible al tratarse datos especialmente protegidos relativos a la salud de las personas.

* Facilitar a los miembros el reparto de los costes que supongan la adaptación a la Ley.

* Conseguir implantar un régimen homogéneo de protección de datos de carácter personal en el seno de la ACES, lo que supone ventajas tanto para la propia organización como para los usuarios.

* En relación con la organización, permite añadir a la imagen de ACES, como característica de calidad homogénea del colectivo, el esfuerzo corporativo y la sensibilización del grupo en orden a garantizar el respeto a los derechos y libertades de los ciudadanos en el tratamiento de los datos personales de sus usuarios o pacientes, de conformidad con la legislación aplicable.

* Entre las medidas que incluye el código se encuentran las encaminadas a asegurar la debida instrucción por parte del personal autorizado para acceder a los datos de carácter personal de las disposiciones del propio código tipo y del régimen de derechos y obligaciones, procedimientos y cautelas que comporta de conformidad con la ley.

En relación con los usuarios, la uniformidad del régimen de protección de datos de carácter personal en el seno de ACES supone una ventaja, al proporcionarles una mayor seguridad garantizada mediante el establecimiento de procedimientos y regímenes únicos y facilitar el ejercicio de derechos y la defensa de sus intereses a los afectados de forma normalizada.

Todo ello, sin perjuicio de la obligación legal del cumplimiento de la LOPD y sus normas de desarrollo.

Las disposiciones del Código son de aplicación a todos los miembros de la Agrupación. Los centros y establecimientos sanitarios que en un futuro entren a formar parte de la ACES deberán efectuar por escrito una declaración expresa de aceptación y sometimiento al mismo.

ACES desarrollará un logotipo identificador del Código Tipo, que se incorporará en documentos, circulares y boletines de la Agrupación.

Todos los centros y establecimientos sanitarios miembros numerarios de ACES reproducirán este logotipo en los documentos que tengan por destinatarios a los pacientes o usuarios y colocarán un cartel a la vista del público en el departamento de información o recepción de pacientes, así como en los vestíbulos y salas de espera, informando de la existencia del Código Tipo, y de su inscripción en el Registro.

Se facilitará un ejemplar de consulta a cualquier usuario que así lo requiera. A este efecto en la oficina de información o de recepción de los centros sujetos al Código dispondrán al menos de dos ejemplares editados del mismo, sin perjuicio de la posibilidad de habilitar un terminal informático para su consulta electrónica.

En relación con el tratamiento y uso de los datos personales se observarán los principios de protección de datos determinados por la LOPD, así como las obligaciones que ésta exige a los responsables de los ficheros.

El deber de información en la recogida de los datos al que hace referencia el art. 5 de la LOPD, se facilitará mediante un Documento de Información en el que figuren los datos recabados y a continuación:

* Indicación del fichero o tratamiento de datos al que serán destinados.

* Expresión de la finalidad de la recogida de los datos.

* Indicación de los destinatarios de la información.

* Información sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, con indicación de la existencia del Código Tipo a disposición de los interesados y de los formularios que contiene para el ejercicio de esos derechos, así como de la legislación aplicable en materia de protección de datos.

* Comunicación de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Del documento de información se entregarán dos copias al interesado, requiriéndole para que firme una que conservará el responsable del fichero, o los usuarios autorizados que recaben personalmente los datos, en el archivo correspondiente al interesado como prueba de la información prestada.

En cuanto a la obligación de recabar el consentimiento del afectado para el tratamiento de los datos de carácter personal, se informará expresamente con la siguiente cláusula:

"El afectado, titular de los datos personales arriba consignados, al suscribir este Documento de Información autoriza expresamente al responsable del fichero para el tratamiento de esos datos personales para las finalidades expresadas. "

También se va a informar al afectado, cuando el responsable tenga la necesidad de comunicar los datos de carácter personal objeto de tratamiento a un tercero. Para ello, se remitirá, por medio que deje constancia del envío y de la fecha de recepción, un comunicado al interesado en el que se expondrán los siguientes extremos:

* Datos identificativos del responsable del fichero cedente: denominación, actividad, dirección postal, teléfono, y en su caso, fax y dirección de correo electrónico.

* Datos de carácter personal del interesado que obran en poder del responsable del fichero y cuya comunicación a un tercero se pretende autorizar.

* Circunstancias en que el responsable del fichero obtuvo los datos que se pretende comunicar, con mención de la información o el consentimiento prestados con ocasión de la recogida de los mismos.

* Finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar.

* La sujeción del cesionario, por el sólo hecho de la comunicación de los datos personales, a las disposiciones de la LOPD.

* La advertencia, gráficamente destacada, de que si no manifiesta lo contrario en el término de 15 días naturales contados a partir del día siguiente al de la recepción del comunicado, se entenderá que presta su consentimiento a la comunicación de sus datos personales expuesta. No obstante, el afectado podrá revocar el consentimiento prestado en cualquier momento. En este caso, la revocación no podrá tener efectos retroactivos.

También se contemplan en el código tipo las obligaciones del responsable del fichero y del personal que va a efectuar el tratamiento de los datos, que quedan reflejados en un documento denominado *Compromiso Escrito* , en el que se expone el deber de secreto y de custodia que les obliga y las sanciones administrativas y penales, laborales o profesionales, a que puede dar lugar su incumplimiento. Asimismo, mediante este documento, se asume personalmente el compromiso de cumplimiento de dichas obligaciones y la eventual responsabilidad patrimonial en la que incurriría en caso de que el centro sanitario al que pertenezca sea sancionado económicamente o deba responder por los daños y perjuicios causados por infracción de dicho deber por conducta imputable personalmente al mismo. En este caso al centro o establecimiento sanitario le asistirán las acciones legales pertinentes para repercutir lo pagado por este concepto al personal directamente responsable de la conducta que haya supuesto la infracción de la obligación de

guardar secreto.

Asimismo se adoptarán los acuerdos y negociaciones, en su caso pertinentes, para incluir esta obligación de guardar secreto y custodia de los datos personales entre las obligaciones profesionales o laborales del personal autorizado para su uso y acceso, pudiendo dar lugar su incumplimiento a las sanciones laborales y profesionales aplicables, incluso el despido, en función de la gravedad de la conducta infractora y de las circunstancias que concurran, lo que se determinará y establecerá mediante los procedimientos y ante las instancias competentes.

El responsable del fichero cuidará de que el personal autorizado para acceder a los datos personales conozca y pueda prestar información a los interesados sobre sus derechos de acceso, rectificación y cancelación.

En este sentido, estarán a disposición del público los modelos de solicitudes para el ejercicio de estos derechos que se adjuntan al código tipo.

Por lo que respecta a las garantías de los derechos de los afectados, se crea un órgano mixto formado por un representante de la Agrupación y uno de la Organización de Consumidores y Usuarios de Cataluña (OCUC) encargado de la determinación mediante el procedimiento arbitral establecido al efecto, de determinar la cuantía de la indemnización de los daños y perjuicios sufridos como consecuencia de la infracción de sus derechos en esta materia. No obstante, el afectado puede optar por reclamar la defensa de sus derechos ante los Tribunales de Justicia.

Todo ello con independencia de la función de tutela y auxilio a los interesados y de la competencia para perseguir y sancionar las infracciones al régimen legal aplicable en la materia, que corresponden en todo caso a la Agencia de Protección de Datos.

Los afectados que sufran cualquier daño, lesión o perjuicio, tanto material como moral, en sus derechos e intereses legítimos, como consecuencia de la infracción del régimen establecido en la legislación aplicable y en este Código Tipo en relación a los datos de carácter personal que haya proporcionado o de los que disponga cualquier miembro asociado, podrán ejercitar las acciones legales correspondientes ante la jurisdicción ordinaria.

Por todo ello, cumpliendo el Código los requisitos legales exigidos para su inscripción en el Registro General de Protección de Datos, se procedió a dicha inscripción en el mes de diciembre de 2001.

Los textos completos de los códigos inscritos durante el año 2001 se encuentran en los Anexos de esta memoria.

MEMORIA DE 2001 - LA PROTECCIÓN DE DATOS EN ESPAÑA. ANÁLISIS DE LOS PRINCIPALES DESARROLLOS

1. INFORMES SOBRE PROYECTOS DE DISPOSICIONES GENERALES

Entre las funciones que legalmente se encuentran asignadas a la Agencia de Protección de Datos se encuentra la de informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley Orgánica 15/1999, de 13 de enero, de Protección de Datos de Carácter Personal.

Durante el año 2001 han sido 55 los proyectos de disposiciones que, para el ejercicio de esta competencia, han sido remitidos a la Agencia de Protección de Datos, de entre las que, por su especial trascendencia, pueden reseñarse las siguientes:

-Anteproyecto de Ley Financiera

-Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

-Anteproyecto de Ley sobre Firma Electrónica

-Anteproyecto de Ley de Protección de Datos de la Comunidad Autónoma de Madrid

-Proyecto de Ley de Protección de Datos de la Comunidad Autónoma de Cataluña.

–Borrador de Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones

–Anteproyecto de Ley de Estadística de la Comunidad Autónoma de Murcia

-Anteproyecto de Ley de Estadística de la Comunidad Autónoma de Castilla-La Mancha

–Anteproyecto de Ley Orgánica de Reforma Concursal

-Proposición de Ley sobre incremento de las garantías de los trabajadores y funcionarios en materia de derecho a la intimidad, igualdad y no discriminación por razones de salud, presentada a la Mesa del Congreso de los Diputados por el Grupo Parlamentario Socialista

-Proyecto de Orden del Ministerial por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado y se delimitan los datos sobre los abonados a entregar por los operadores a la Comisión del mercado de las Telecomunicaciones para la elaboración de guías telefónicas

-Proyecto de Real Decreto por el que se regula la conservación de la documentación histórica, el control de la eliminación de documentos de la Administración General del Estado y sus Organismos Públicos y su conservación en soporte distinto al original,

-Proyecto de Decreto para la Aplicación de la Ley 5/2001, de 17 de mayo de la Comunidad Autónoma de Castilla-La Mancha, de prevención de malos tratos y de protección a las mujeres maltratadas.

Igualmente, en ejercicio de otras competencias consultivas, como la atribuida por el artículo 6.a) del Estatuto de la Agencia de Protección de Datos aprobado por Real Decreto 428/1993, de 26 de marzo en materia censal y estadística, puede señalarse que se han informado en este periodo los cuestionarios censales remitidos por el Instituto Nacional de Estadística para la elaboración de los censos de población y vivienda iniciados en el año 2001.

Debe significarse como, entre los proyectos de disposiciones generales informadas en el periodo comentado, ha sido especialmente significativo el número disposiciones dirigidas a la creación de ficheros o a la modificación de disposiciones ya existentes que los regulaban, muy particularmente en el ámbito de la Administración General del Estado. Analizando este dato, puede considerarse que ello ha obedecido por un lado a una actividad de los organismos responsables de los ficheros en orden a adaptar disposiciones ya en vigor de creación de ficheros públicos tanto a la Ley Orgánica 15/1999, como a las modificaciones en ella introducidas por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre (que la declaró parcialmente inconstitucional precisamente en preceptos relativos a ficheros públicos, como fue ampliamente analizado en la Memoria del año 2000 de esta Agencia de Protección de Datos).

También en ello ha influido el cada vez más cercano fin del periodo transitorio establecido en la Disposición Adicional Primera de la Ley Orgánica 15/1999 para adecuar los ficheros automatizados preexistentes a la entrada en vigor de la Ley, que expresamente indicaba que en el plazo de tres años "las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente".

Sin duda, otro factor coadyuvante han sido los requerimientos efectuados por el Director de la APD a los Departamentos ministeriales y otros organismos públicos en el año 2000 (para que se hiciesen constar los cambios derivados de reestructuraciones orgánicas) y en el año 2001 (por ejemplo, en relación con la Sentencia del Tribunal Constitucional

292/2000), a todos los cuales se ha hecho ya referencia en el apartado de esta Memoria correspondiente al Registro General de Proteccion de Datos.

2. DESARROLLO NORMATIVO

De obligada mención en el presente apartado durante el año 2001 es la Resolución de 27 de julio de 2001 (BOE de 17 de agosto), de la Agencia de Protección de Datos, de creación y modificación de ficheros de datos de carácter personal de la Agencia, que viene a derogar las anteriores Resoluciones de la misma de 18 de julio de 1994 y de 7 de febrero de 1995, de creación y modificación de los ficheros de datos de carácter personal de la Agencia.

A esta disposición se ha hecho ya extensa referencia en el Capítulo dedicado al Registro General de Protección de Datos (al tratarse de una norma que tiene especial incidencia en su ámbito de actuación) y se reproduce íntegramente en el Anexo de esta memoria.

3. CONSULTAS DE RESPONSABLES DE FICHEROS

El Gabinete Jurídico, incardinado en la Unidad de Apoyo al Director de la Agencia, junto a la función consultiva y de asesoramiento en Derecho a los distintos órganos de la propia Agencia que le es propia, ejerce también, a instancia del Director, una función de asesoramiento externo, emitiendo dictámenes jurídicos sobre las cuestiones de mayor complejidad sometidas al parecer de la Agencia de Protección de Datos por los responsables de ficheros, tanto particulares como Administraciones Públicas.

Durante el año 2001 se ha mantenido el importante volumen de actividad desplegado en el ejercicio de esta función, que desarrolla la Agencia aun cuando no existe una atribución legal o reglamentaria de la misma, pero que se considera de gran interés en orden a proporcionar asistencia y asesoramiento a personas y entidades en el cumplimiento de las obligaciones que les impone la Ley Orgánica 15/1999.

En el periodo de referencia, han sido emitidos un total de 545 informes. Aunque el número de los mismos ha descendido ligeramente respecto de los que se emitieron en el año 2000 (606), debe destacarse como se ha incrementado notablemente, en muchos casos, la complejidad de las cuestiones planteadas, descendiendo correlativamente el volumen de consultas que han sometido cuestiones mas simples o reiteradas otros años.

A modo de ejemplo, en el 2001, se ha contabilizado un importante volumen de consultas relacionadas con la publicación y la cesión de datos de carácter personal en Internet, lo que pone de manifiesto la importancia cada vez mayor de este medio, y ello tanto desde perspectiva del sector público como del privado.

Igualmente, ha sido importante el volumen de cuestiones que han indagado el criterio de la Agencia de Protección de Datos en relación con las transferencias internacionales, dentro de una práctica creciente de transmisiones de datos por parte de empresas españolas a sus filiales o matrices en el extranjero, de algunas de sus bases de datos, tanto de clientes como de trabajadores en muchos casos, cuando no, como en algún supuesto, de la totalidad de las mismas.

3.1. Datos estadísticos de interés relacionados con las consultas

Atendiendo en primer lugar a la naturaleza pública o privada de los consultantes, pueden distribuirse los informe emitidos como sigue:

Administraciones Públicas.....251

Administración General del Estado.....70
Comunidades Autónomas.....16
Entidades Locales.....90
Otros organismos públicos.....75

Consultas Privadas.....294

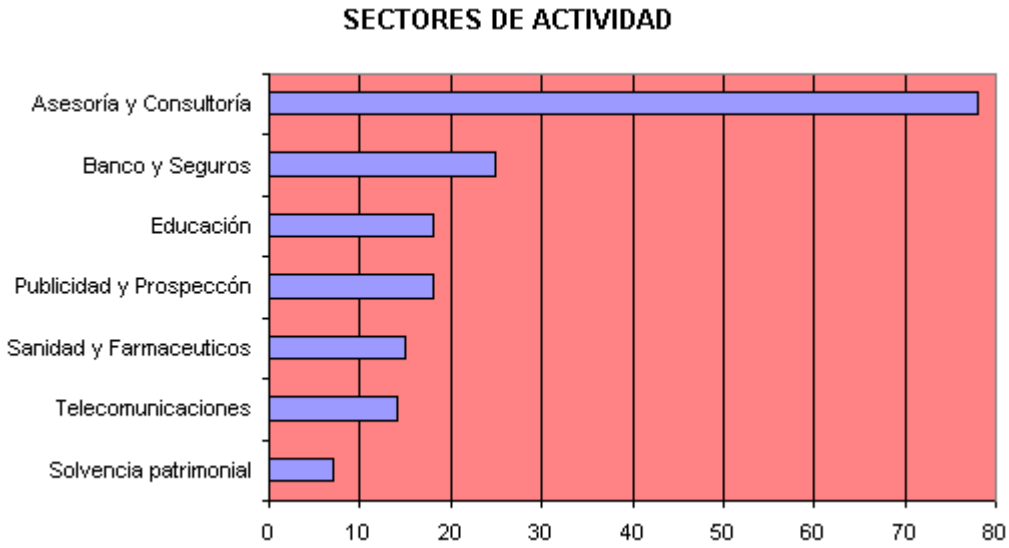
Empresas.....235
Particulares.....13
Asociaciones/Fundaciones.....28
Sindicatos.....8
Otros.....10

Total informes..... 545

Como puede observarse, del volumen de informes evacuados a instancia de responsables de ficheros durante el año 2001, 294 han correspondido a consultas privadas, mientras que 251 han sido las planteadas por las Administraciones Públicas, pudiendo reseñarse que en este año ha seguido siendo mayor (al igual que ocurrió el pasado año, y como es previsible y lógico) el número de consultas planteadas por particulares (personas físicas o jurídicas), aunque también debe ponerse de manifiesto que ha aumentado proporcionalmente el número de las remitidas por las Administraciones Públicas, invirtiéndose así la tendencia decreciente verificada el año 2000.

Considerando estas cifras, puede apreciarse como, respecto a las provenientes del sector público, ha disminuido respecto al año anterior el número de las consultas planteadas por Ayuntamientos (aunque como es lógico, siguen siendo las más numerosas, dado el número de estas administraciones territoriales y, en muchos casos, la insuficiencia de medios de asesoría jurídica propios), mientras que en cuanto a las del sector privado, al igual que ocurrió en el año 2000, predominan notablemente las consultas planteadas por empresarios, habiendo sido sumamente significativo en el año 2.001, y considerando ya la distribución sectorial de las consultas, el volumen de las planteadas por entidades que realizan actividades de asesoría y consultoría, tanto relativas a la gestión de sus propios ficheros como a la función asesora de sus clientes responsables de ficheros. Se repite así una circunstancia ya apreciada en la Memoria del pasado año.

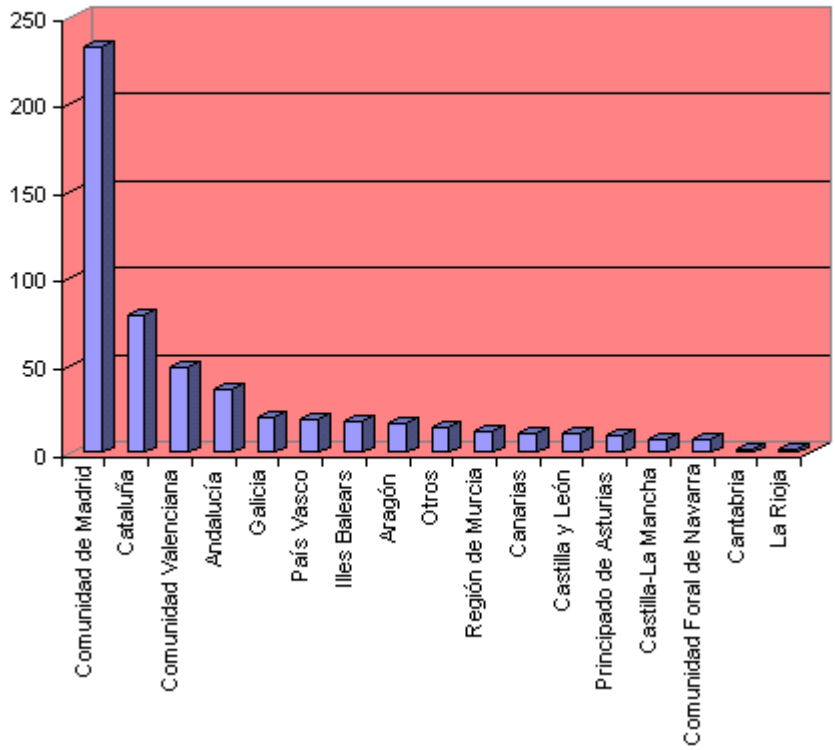
Atendiendo a las consultas formuladas por el sector privado, puede establecerse la siguiente distribución por sectores de actividad



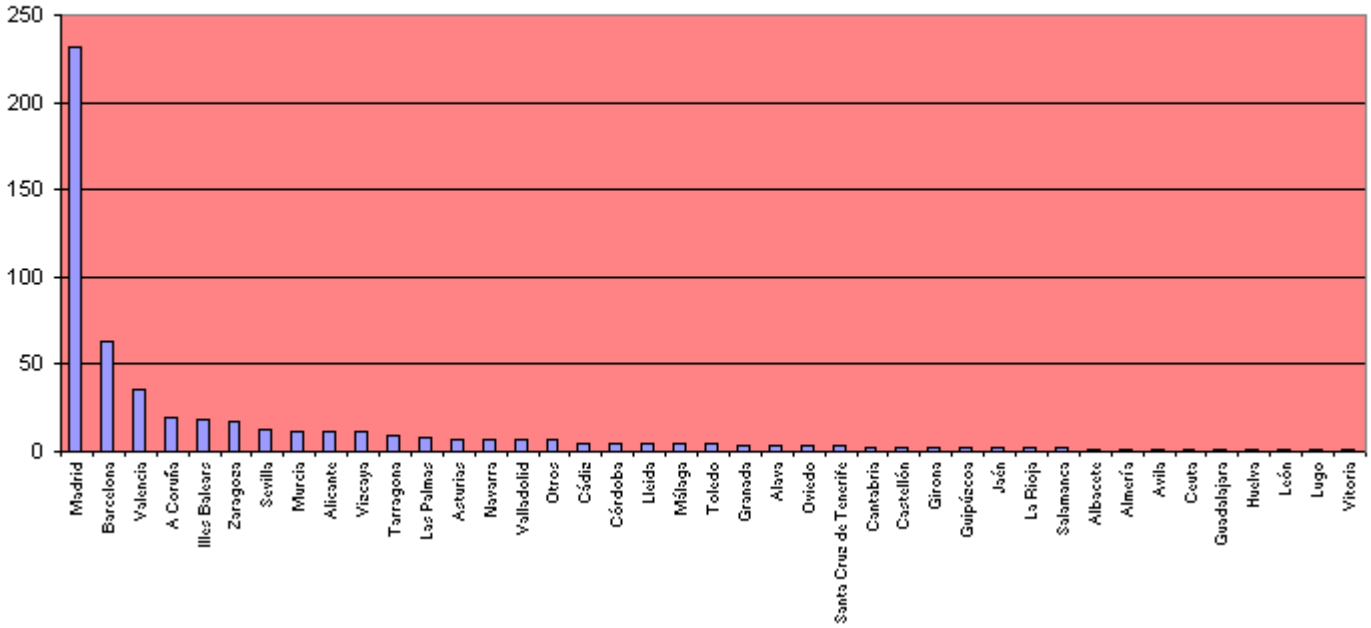
Como puede observarse, dicha distribución no presenta modificaciones sustanciales respecto al año anterior, siendo las consultas planteadas desde el sector de la consultoría y el asesoramiento las que predominan notablemente frente a los demás.

También ha existido una continuidad respecto al pasado año en cuanto a la distribución geográfica de las consultas planteadas, cuya distribución se ofrece a continuación, tanto por Comunidades Autónomas como por provincias.

DISTRIBUCION POR COMUNIDADES AUTÓNOMAS



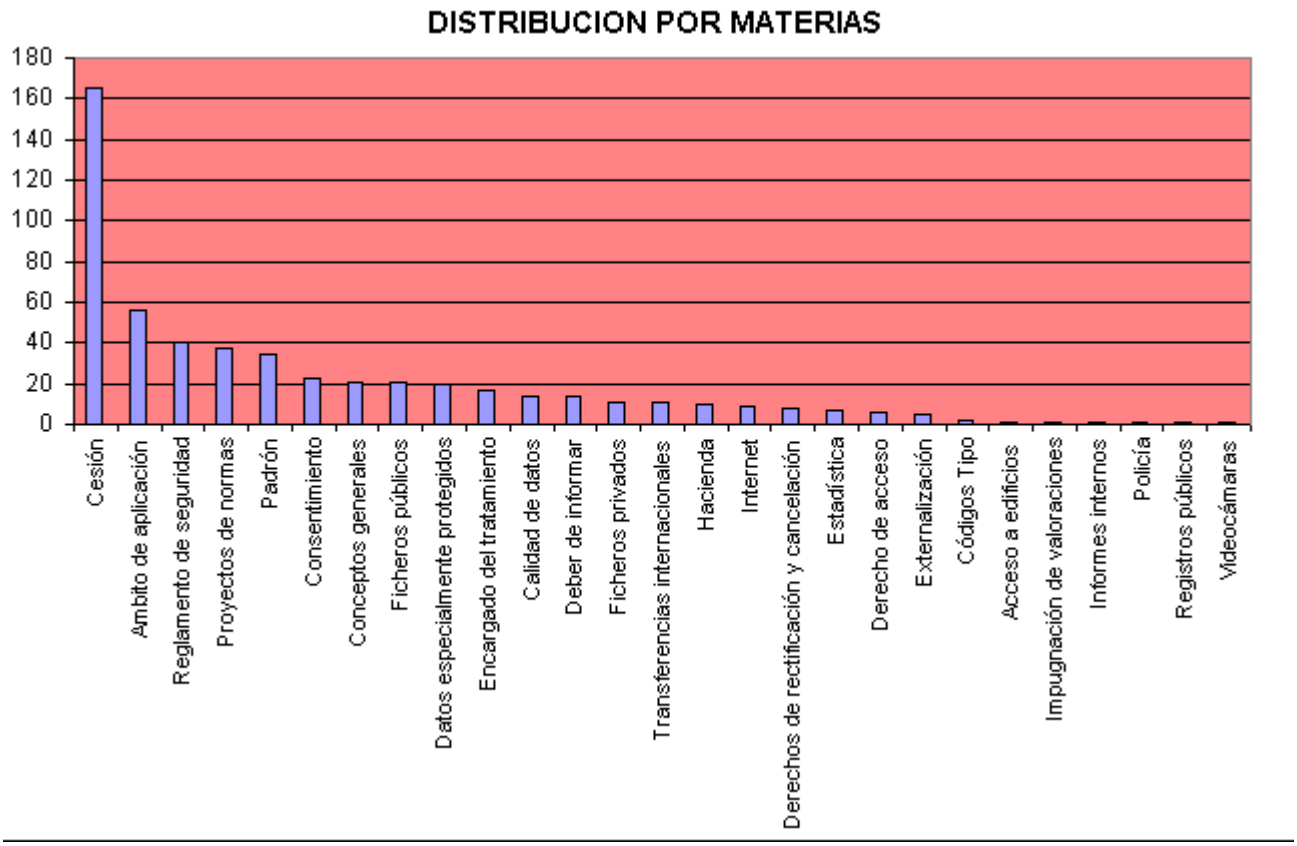
DISTRIBUCION POR PROVINCIAS



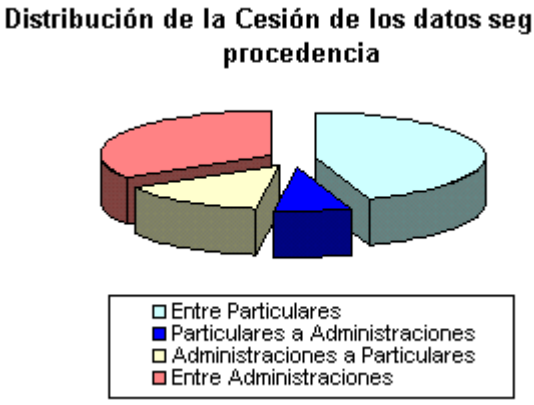
Finalmente, se ofrece la distribución de consultas atendiendo a la materia, donde puede observarse como predominan aquellas relativas a las cesiones de datos, en las que se ha incrementado las referidas a cesiones entre Administraciones Públicas, consecuencia de la modificación operada en la LOPD en este concreto aspecto por la Sentencia del Tribunal Constitucional 292/2000.

Se ha mantenido el número de consultas relativas a la implantación del Reglamento de medidas de seguridad de los ficheros automatizados, aprobado por Real Decreto 994/1999, de 11 de junio, especialmente las relativas a medidas de nivel alto, cuyo periodo de implantación si bien concluía precisamente en el año 2001, fue prorrogado hasta el 26 de junio de 2002, suscitándose una gran diversidad de cuestiones, generalmente de carácter interpretativo.

También se han incrementado las consultas relativas a transferencias internacionales, planteadas principalmente por empresas españolas pero también en algún caso desde empresas extranjeras, del ámbito de la Unión Europea.



Dado que como se ha indicado las consultas relativas a cesiones de datos siguen siendo las mas abundantes, se acompaña un cuadro clasificatorio de las mismas atendiendo al cedente y cesionario.



3.2. Estudio de las cuestiones más relevantes planteadas por los responsables de ficheros o tratamientos.

Como vienen siendo ya habitual en cada Memoria anual de la Agencia, se considera de interés comentar aquellas cuestiones que, al hilo de las consultas planteadas, y atendiendo a su trascendencia o generalidad, se consideran mas significativas.

3.2.1. Cesión de datos de la Guía Telefónica

Se formuló a la Agencia de Protección de Datos una consulta relativa a la legalidad, conforme a la normativa de protección de datos, de la previsión normativa de que por el operador dominante del servicio de telefonía, se cediesen los datos de sus clientes que constan en la guía telefónica tanto a la Comisión del Mercado de las Telecomunicaciones como a terceros para que por éstos se presten servicios de guía telefónica y/o de información telefónica de abonados.

Considerada la cuestión desde la perspectiva de la normativa reguladora de la protección de datos de carácter personal, no cabe duda que los datos referidos, relacionados con los propios abonados al servicio prestado por la compañía telefónica, son datos de carácter personal, al encajar en el concepto establecido en el artículo 3 a) de la Ley Orgánica 15/1999, dado que serán datos de carácter personal, a los efectos de la misma, "cualquier información concerniente a personas físicas identificadas o identificables". Del mismo modo, la transmisión de los datos a la Comisión o a los restantes operadores del mercado constituirá una cesión o comunicación de datos de carácter personal, definida por el artículo 3 i) de la propia Ley como "toda revelación de datos realizada a una persona distinta del interesado".

Respecto de la cesión o comunicación de datos, y siguiendo en este punto la referencia que la consultante efectúa de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, rige (salvo en la cesión entre administraciones públicas para el desempeño de competencias similares) el principio de reserva de Ley, de tal modo que será necesario que, a falta de consentimiento, expreso o tácito cuando la Ley lo permita, del afectado, será necesaria la existencia de una habilitación legal que dé cobertura a la comunicación, pudiendo dicha habilitación incluso traer su causa de lo establecido en la propia Ley Orgánica 15/1999, tal y como sucede en los supuestos incluidos en los apartados b) a f) del artículo 11.2 de la misma.

Analizando si en el caso indicado la cesión de los datos de abonados a la guía telefónica tenía amparo en una norma con rango de Ley o ello vulneraba, al venir establecida la misma en una norma con simple rango reglamentario, el artículo 21, siendo de aplicación en consecuencia el artículo 11.1 de la LOPD, que exige la concurrencia, a falta de previsión legal, del consentimiento del afectado.

Ello exige analizar si la obligación impuesta por el artículo 14 del Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones, aprobado por Real Decreto 1736/1998, de 31 de julio, trae su causa de una norma con rango de Ley o si tal norma no existe, en cuyo caso sería exigible el mencionado consentimiento.

El citado artículo establece, en su párrafo segundo que "la Comisión del Mercado de las Telecomunicaciones deberá suministrar gratuitamente a las entidades que deseen elaborar guías telefónicas los datos que, de conformidad con lo establecido en la Orden reguladora de las licencias individuales y en la Orden a la que se refiere el artículo 67.1, le faciliten los operadores que presten el servicio de telefonía disponible al público".

Dicho precepto es lógico reflejo de lo establecido en los párrafos primero y quinto del citado artículo 14. El primero de ellos consagra que "los abonados al servicio telefónico fijo disponible al público tendrán derecho a disponer de una guía telefónica de carácter gratuito, unificada para cada ámbito territorial, que será, como mínimo, provincial. Asimismo, tendrán derecho a figurar en la guía y, en su caso, a solicitar la corrección o supresión de los datos relativos a ellos. Estas guías deberán estar a disposición de todos los usuarios y ser actualizadas periódicamente. Mediante Orden del

Ministerio de Fomento se fijarán los criterios para su elaboración, actualización y los datos que deberán figurar en ellas" (puede indicarse al cierre de esta memoria, que esta previsión reglamentaria ha sido desarrollada por la Orden del Ministerio de Ciencia y Tecnología de 21 de diciembre de 2001 -BOE del 28 de diciembre-, por la que se regulan determinados aspectos del Servicio Universal de Telecomunicaciones, así como por la más reciente Orden de 26 de marzo de 2002).

Por su parte, el párrafo quinto establece el deber de los operadores designados para la prestación de servicio universal de poner "a disposición de todos los abonados del servicio telefónico fijo disponible al público, incluidos los usuarios de teléfonos públicos de pago y respecto de los números telefónicos de dicho servicio, al menos, un servicio de consulta telefónica actualizado", que "se prestará a un precio asequible y tendrá carácter gratuito para el usuario cuando se efectúe desde un teléfono público de pago".

En consecuencia, el artículo 14 no establece una obligación de los operadores de facilitar los datos correspondientes a los abonados a la Comisión del Mercado de las Telecomunicaciones sino que, presumiendo la existencia de dicha obligación (con referencia expresa a las órdenes en que la misma se incluya), impone a la Comisión el deber de facilitar dichos datos a "las entidades que deseen elaborar guías telefónicas", con el fin de dar pleno cumplimiento a los derechos (y correlativos deberes para las operadoras) contenidos en los párrafos primero y quinto del artículo.

Dado que la obligación de suministrar los datos a la Comisión del Mercado de las Telecomunicaciones no se encuentra incluida en el texto del Reglamento, y dado el principio de reserva de Ley, al que ya se hizo referencia, deberá ahora indagarse cuál es la norma que, en su caso, daría cobertura a esta obligación.

Pues bien, la norma esencial reguladora del sector es la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, cuyo artículo 37.1 b) consagra, como indica la consulta, el derecho a "que los abonados al servicio telefónico dispongan, gratuitamente, de una guía telefónica, actualizada e impresa y unificada para cada ámbito territorial", añadiendo que "todos los abonados tendrán derecho a figurar en las guías y a un servicio de información nacional sobre su contenido, sin perjuicio, en todo caso, del respeto a las normas que regulen la protección de los datos personales y el derecho a la intimidad".

La materialización de este derecho y la forma de dar cumplimiento a lo previsto en el artículo 37.1 b), se contiene en el artículo 54.3 de la propia Ley General de Telecomunicaciones, que vinculando el derecho con el principio esencial de liberalización del sector que la misma persigue, dispone claramente que "la elaboración y comercialización de las guías de abonados a los servicios de telecomunicaciones se realizará en régimen de libre competencia".

A fin de garantizar la libre competencia en el sector, y asegurar asimismo el derecho de los afectados a disponer de los directorios necesarios para el uso adecuado del servicio (y sin perjuicio del ejercicio por aquellos de los derechos que la Ley les garantiza en su Título III), la Ley General de Telecomunicaciones establece en el párrafo primero de su artículo 11.2 una serie de reglas que garanticen, en la medida de lo posible, la igualdad de condiciones en la actividad de los operadores. Así, en lo que afecta a la cuestión examinada, el citado precepto indica que "igualmente, en el régimen aplicable a las autorizaciones generales, se podrá incluir la determinación de las condiciones impuestas a sus titulares, relativas al suministro de la información que sea precisa para (...) facilitar los datos para la confección de la guía unificada para cada ámbito territorial y atender los requerimientos que vengan impuestos por la normativa aplicable".

En consecuencia, el legislador viene a concretar expresamente, en una norma con rango de Ley, la posibilidad de que, en un desarrollo reglamentario posterior, se exija a los operadores la aportación de los datos necesarios para dar pleno cumplimiento a los derechos/deberes que él mismo consagra en la propia Ley.

De lo antedicho se desprende que no nos encontramos en este caso ante una cesión que simplemente trae cobertura de lo dispuesto en una norma reglamentaria, lo que chocaría con lo establecido en el artículo 11.1 de la Ley Orgánica 15/1999 y con la interpretación efectuada por nuestro Tribunal Constitucional, sino que existe una norma con rango de Ley habilitante de la cesión, sin perjuicio de que la misma quede o no posteriormente concretada en una norma reglamentaria dictada en su desarrollo.

Esta concreción reglamentaria se efectúa a través de lo establecido en el artículo 14 del Real Decreto 1736/1998 y en el artículo 27 de la Orden de 22 de septiembre de 1998, que concreta la obligación prevista por el artículo 11.2 de la Ley General de Telecomunicaciones, al establecer, entre las condiciones generales exigibles para los titulares de licencias de tipo B (habilitante "para la prestación del servicio telefónico disponible al público, mediante el establecimiento o la explotación, por su titular, de una red pública de telecomunicaciones", según el artículo 25) la de "facilitar a la Comisión del Mercado de las Telecomunicaciones, de forma impresa y en soporte informático, los datos correspondientes a sus abonados para la confección de una guía unificada para cada ámbito territorial, en los términos de lo previsto en los artículos 37.1.b) de la Ley General de Telecomunicaciones y 14 del Reglamento de Obligaciones de Servicio Público y respetando, en todo caso, los derechos de los usuarios, especialmente, los contemplados en el artículo 54 de la misma Ley".

En consecuencia, se consideró por la APD que la transmisión de los datos referentes a los abonados resultaría conforme a lo establecido en el artículo 11 de la Ley Orgánica 15/1999, al traer dicha cesión causa de lo establecido en el artículo 11.2 de la Ley General de Telecomunicaciones, concluyéndose al respecto:

-que la cesión por el operador dominante de los datos correspondientes a los abonados para la elaboración de directorios telefónicos se encuentra amparada por el artículo 11.2 a) de la Ley Orgánica 15/1999, al existir una norma con rango de Ley (el artículo 11.2 de la Ley general de Telecomunicaciones) de la que se deriva directamente dicha obli-

gación.

-que la entidad que decida elaborar un directorio telefónico estará obligada a cumplir el deber de información al que se refiere el artículo 5.4 de la Ley Orgánica 15/1999, así como a notificar el fichero resultante, a efectos de su inscripción en el Registro General de Protección de Datos.

3.2.2. Bloqueo de datos de carácter personal

Se planteo el alcance de la excepción o suspensión de la obligación de cancelación de datos que implica el bloqueo de los mismos, así como la conciliación del artículo 16.3 de la LOPD con la normativa reglamentaria de desarrollo dictada al amparo de la LORTAD y que regulaba la cancelación, concluyéndose la subsistencia de éstas en una interpretación coordinada con aquella disposición, y entrándose a analizar el supuesto del bloqueo de datos..

Así, el artículo 16.1 del Real Decreto 1332/1994, de 20 de junio, hace también referencia al bloqueo de datos, disponiendo que "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", con la excepción prevista en su párrafo segundo, según la cual "Se exceptúa, no obstante, el supuesto en el 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 aquéllos figuren".

Por otro lado, el apartado 8 de la Norma Tercera de la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, dispone que "la cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas", añadiendo el apartado 9 de la misma Norma que "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".

Las citadas previsiones fueron dictadas al amparo de lo establecido en la Ley Orgánica 5/1992, que no contenía previsión alguna en relación con el bloqueo de los datos de carácter personal, limitándose a reflejar esta obligación de cancelar, sin delimitar en qué consistía efectivamente la obligación de cancelación. Así, el artículo 15.2 de la derogada Ley se limitaba a señalar que "los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso", añadiendo el artículo 15.4 que "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" y el artículo 15. 5 que "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".

Sin embargo, la nueva Ley Orgánica 15/1999 sí viene a hacer una referencia expresa al bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que siguiendo lo ya apuntado por la LORTAD, indica que "los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".

Del análisis conjunto de las dos normas últimamente citadas se desprende claramente que existirán determinados supuestos en que la cancelación o bien no podrá tener lugar, dada la obligación de conservación impuesta por la Ley, o bien deberá suponer una fase previa de bloqueo de los datos que, produciendo unos efectos similares al borrado físico de los mismos, salvo en determinadas circunstancias, no implicará automáticamente ese borrado.

Así, el artículo 16.3 viene a reconocer, en consonancia con lo ya previsto en el artículo 15.5 de la LORTAD y 16.5 de la nueva Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

Por el contrario, el responsable del fichero estará obligado, bien por el contenido de aquélla relación jurídica, bien por lo establecido en una norma imperativa, al mantenimiento del dato, si bien sometido a determinadas condiciones que aseguren y garanticen el derecho del afectado a la protección de sus datos de carácter personal, no pudiendo disponer de tales datos en la misma medida en que podría hacerlo en caso de que no procediera (de oficio –por haber dejado de ser necesarios para el cumplimiento de la finalidad del fichero- o a solicitud del afectado) la cancelación de los mismos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto "en las disposiciones aplicables" o a la "atención de las posibles responsabilidades nacidas del trata-

miento", tal y como prevé la meritada Ley.

En este sentido, debe recordarse en relación con el mantenimiento del dato bloqueado, en cuanto supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que "cumplido el citado plazo deberá procederse a la supresión), que ha de tenerse en cuenta que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia fiscal (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En consecuencia, cabe entender que la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento. Por este motivo, y con las peculiaridades que se han venido indicando, ha de considerarse que lo establecido en el Real Decreto 1332/1994 y en el apartado 8 de la Norma Tercera de la Instrucción 1/1998, debe interpretarse de forma armonizada con la citada disposición, no existiendo una obligación terminante de borrado físico en todos los casos.

3.2.3. Ámbito subjetivo de aplicación de la LOPD

Esta cuestión se suscitó en el año 2001 con ocasión del análisis de si conforme a las previsiones de la LOPD, era factible la publicación o, en su caso, comercialización de los datos que constan en el censo público de empresas al que se refiere el artículo 2.1 h) de la Ley 3/1993, de 22 de marzo, básica de Cámaras Oficiales de Comercio, Industria y Navegación (Censo Público Cameral de Empresas).

Ello exigió analizar el ámbito de aplicación de la propia Ley Orgánica 15/1999, y la cuestión de su aplicación en los supuestos en que los datos se refieran a personas físicas que lleven a cabo una actividad mercantil o empresarial.

Hasta la entrada en vigor de la Ley Orgánica 15/1999, se entendía que dichos datos debían considerarse asimilados a los correspondientes a personas jurídicas, toda vez que el objeto de protección de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (LORTAD) consistía en la protección de la intimidad personal y familiar de las personas físicas, siendo así que no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, no podía ser aplicable a esas personas la protección consagrada por la LORTAD, ni siquiera cuando su actividad se identifique plenamente con la de una persona física determinada, habida cuenta que el ámbito personal que se protegía debía ser considerado como distinto del empresarial.

Sin embargo, como ya se indicó, la nueva Ley Orgánica 15/1999 extiende su manto protector más allá de la mera protección del derecho a la intimidad personal y familiar para consagrar el denominado derecho a la "autodeterminación informativa" o a la "libertad informática", reconocido expresamente por la jurisprudencia de nuestro Tribunal Constitucional, a partir de su Sentencia 254/1993, y considerado, como se dijo, un derecho fundamental específico y distinto de la intimidad en la Sentencia del Tribunal Constitucional 292/2000. Por este motivo es objeto de la Ley no sólo la protección de los ciudadanos frente al uso inadecuado de técnicas informáticas, sino, en un sentido mucho más extenso, la protección de cualesquiera derechos fundamentales y libertades públicas de las personas físicas frente al tratamiento automatizado de sus datos de carácter personal.

Ello supone que, si bien los empresarios individuales pueden carecer de un derecho a la intimidad personal y familiar, ello no implica que el tratamiento de los datos referidos a los mismos pueda dar lugar a una vulneración de otros derechos que les atribuye la Constitución (por ejemplo, el tratamiento de los datos relacionados con la pertenencia de un empresario a una determinada asociación puede vulnerar el derecho de asociación, consagrado por el artículo 22 de la Constitución), así como que las mismas carezcan de un derecho específico a la protección de datos, dado que en modo alguno, con independencia de su esfera de actuación, dichas personas podrían ser consideradas personas jurídicas.

Por ello, no es posible, dentro de este nuevo marco normativo, ofrecer una solución unívoca de la cuestión planteada, debiendo estarse estrictamente a los datos que sean objeto de tratamiento en cada caso concreto para apreciar si el fichero se encuentra o no sujeto a las normas reguladoras de la protección de datos de carácter personal, debiendo tenerse en consideración la reiterada jurisprudencia de nuestro Tribunal Constitucional que exige atender en cada caso concreto a una adecuada protección de los derechos fundamentales consagrados en la Constitución.

En relación con la concreta cuestión que se analizó (el Censo público cameral) planteada, la Agencia de Protección de Datos ya se había pronunciado sobre la misma en su Resolución de 27 de febrero de 2001, recaída en el expediente iniciado como consecuencia de la denuncia efectuada a una determinada Cámara de Comercio como consecuencia de la transmisión a terceros de los datos contenidos en el censo público regulado por la Ley 3/1993. La citada Resolución acuerda el archivo del expediente, indicando en su Fundamento Jurídico II que:

"... la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, y por extensión lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de las cuales sea posible diferenciar su actividad mercantil de su propia actividad privada, estando en el primer caso excluidos también del ámbito de aplicación de la Ley Orgánica 15/1999.

En definitiva pues, tanto las personas jurídicas como los profesionales y los comerciantes individuales (éstos dos últimos sólo en los estrictos términos señalados en el párrafo que antecede, esto es, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios) quedan fuera del manto protector de la Ley Orgánica 15/1999.

A contrario sensu, tanto los profesionales como los comerciantes individuales quedarían bajo el ámbito de aplicación de la Ley Orgánica 15/1999 y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando, en consecuencia, la condición de comerciante (es el caso de los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3/1993 por su artículo 6) y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada. En estos dos casos deberán aplicarse siempre las garantías de la Ley Orgánica 15/1999 dada la naturaleza fundamental del derecho a proteger. Ello exigirá siempre ir analizando caso por caso para hallar en cada supuesto concreto el límite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados personas físicas, o, por el contrario, aquél no resulte amenazado por incidir tan solo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales".

Aplicando lo anteriormente expuesto al Censo Público que mantiene el Consejo Superior de Cámaras resultará que, si bien en principio podría resultar excluido del ámbito de aplicación de la Ley Orgánica 15/1999, dado que la inclusión de los datos en el censo público se produce como consecuencia del ejercicio del comercio, esta exclusión no puede afirmarse con carácter absoluto, pues la Ley Orgánica tendrá eficacia respecto de los datos de personas físicas no organizadas bajo la forma de empresa o de las que no fuera posible diferenciar su actividad mercantil de la propia actividad privada.

Incluso en el supuesto de que el fichero sí quedara sometido al ámbito de aplicación de la Ley Orgánica 15/1999, el artículo 11.2 b) de la misma prevé la posible cesión de los datos de carácter personal en los supuestos en que los mismos aparezcan recogidos en fuentes accesibles al público.

El artículo 3 j) de la Ley Orgánica incluye, dentro de la enumeración taxativa de dichas fuentes "las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo".

El censo público de empresas al que se refiere el artículo2.1 b) de la Ley 3/1993 es, precisamente, un listado de todas aquellas personas que desempeñan una determinada actividad (el ejercicio del comercio), bien en el ámbito de una Cámara de Comercio, bien en el ámbito nacional (en el caso del elaborado por el Consejo Superior, en virtud de la competencia que le atribuye el artículo 18.2 de la Ley 3/1993).

Tomando este hecho en consideración, y teniendo en cuenta que el artículo 3 j) no limita las listas a las que se viene haciendo referencia a quienes ejerzan una determinada profesión colegiada, sino que emplea el término "profesionales" en un sentido amplio, cabe considerar que el censo público, cuya publicidad se desprende del testo de la propia Ley Básica, es encuadrable dentro del concepto de fuentes accesibles al público perfilado por la Ley Orgánica 15/1999, razón por la cual la transmisión de los datos del citado censo, siempre que se limiten a los expresamente indicados en el artículo 3 j) de la Ley Orgánica 15/1999, se encontraría amparada por el artículo 11.2 b) de la meritada Ley.

3.2.4. Censo de Población de las Administraciones Públicas y cesiones de datos del padrón.

La Disposición Adicional Segunda de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, regula los registros de población de las Administraciones Públicas constituidos a partir de datos proporcionados por el Instituto Nacional de Estadística.

La Agencia de Protección de Datos dictaminó en el año 2001 en relación con esta transmisión por parte del Instituto Nacional de Estadística de copia de los datos contenidos en el Padrón Municipal de Habitantes a determinados organismos, de conformidad con lo previsto en la Disposición Final Segunda de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, cuyo tenor literal indica:

"1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada admi-

nistración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones Públicas".

De lo establecido en esta Disposición se desprende que la cesión solicitada será posible, siempre y cuando se cumplan los siguientes requisitos:

1.-Que la cesión sea solicitada por órganos integrados en la Administración General de Estado o las Administraciones de las Comunidades Autónomas.

2.-Que dicha cesión se limite a los datos de nombre, apellidos, domicilio, sexo y fecha de nacimiento que habrán de constar en los padrones de habitantes y en el censo electoral.

3.-Que los datos se limitarán, desde el punto de vista territorial, al ámbito en que el solicitante ejerza su competencia.

4.-Que los datos deberán ser utilizados por el cesionario con la única finalidad de la creación de ficheros o registros de población, que permitirán la comunicación de los órganos de cada Administración Pública con los interesados residentes en sus respectivos territorios, respecto de las relaciones jurídico administrativas derivadas de sus competencias.

Cuando sea procedente y se verifique la cesión de datos por el INE para la creación de tal registro de población, será preciso que la Administración Pública responsable del mismo proceda a la aprobación de la correspondiente norma de creación del fichero y notificar el mismo al Registro General de Protección de Datos.

Frente a la considerada, se producen otras peticiones de datos al INE por parte de órganos administrativos, que constituyen solicitudes parciales de datos que, si bien se fundan en el ejercicio de funciones administrativas, no tienen como finalidad la creación de un específico registro general, en los términos previstos por la citada Disposición.

En este sentido, de lo establecido en el apartado 2 de la Disposición Adicional, en conexión con el apartado 1 parece desprenderse que la cesión a la que aquélla se refiere debería efectuarse en virtud de una única solicitud, efectuada por el órgano competente en cada Administración Pública, fundada en la creación de un único registro que sería accesible por los distintos órganos integrados en cada Administración, dentro del ámbito territorial de su actividad.

Por ello, para resolver estos otros supuestos de cesión de datos para posibilitar el ejercicio de funciones administrativas particularizadas, debe analizarse la procedencia de los mismos considerando las Disposiciones reguladoras del Padrón Municipal de Habitantes, contenidas en la Ley Reguladora de las Bases del Régimen Local.

Cuando estas cesiones particularizadas se solicitan del INE y no de entidades locales, resultará esencial atender a lo dispuesto en el último párrafo del artículo 17.3 de la citada Ley, según el cual "el Instituto Nacional de Estadística podrá remitir a las Comunidades Autónomas y a otras Administraciones Públicas los datos de los distintos Padrones en las mismas condiciones señaladas en el artículo 16.3 de esta Ley".

Por su parte, el mencionado artículo 16.3 prescribe que "Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública. Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".

Tomando en consideración lo establecido en el citado precepto, será procedente dicha cesión particularizada cuando la misma se solicite por órganos administrativos para el ejercicio de competencias legales y se cumplan los requisitos analizados

3.2.5. Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero

Varias han sido en este año las ocasiones en que se han dirigido consultas a la Agencia por parte de empresas españolas que, formando parte de un grupo empresarial multinacional y con ocasión de procesos de reorganización en los mismos a nivel internacional, pretenden efectuar transferencias internacionales de datos, que en ocasiones obedecen a la centralización de procesos de gestión y en otras a simples supuestos de utilización compartida de recursos por filiales de distintos países, al hilo de las posibilidades brindadas por las nuevas tecnologías.

Entre la variada casuística que se ha analizado, cabe distinguir básicamente dos supuestos, aquellos en que se está en presencia de transferencias internacionales que implican auténticas cesiones de datos, de aquellos otros en que la transferencia se efectúa para el tratamiento de los datos por cuenta de terceros, aunque en ambos supuestos, conforme a la LOPD se trataría de transferencias internacionales.

Dichas transferencias internacionales se regulan en los artículos 33 y 34 de la LOPD, y se definen por la Norma Primera de la instrucción 1/2000 de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los Movimientos Internacionales de Datos como "Toda transmisión de los mismos fuera del territorio español. En

particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable de fichero".

Debe señalarse que dicha Instrucción ha fijado los criterios orientativos seguidos por la Agencia de Protección de Datos en la materia, aclarando a los interesados el procedimiento a seguir para dar cumplimiento a las previsiones contenidas en la normativa reguladora de la materia.

Entrando ya a analizar la naturaleza de los supuestos planteados, se ha considerado que la transferencia internacional implicaba cesión de datos en un supuesto en que se remitían los datos del personal de una empresa española a su empresa matriz, situada en otro estado europeo, que iba a centralizar la gestión de recursos humanos de todas las filiales europeas del grupo, al considerarse que dicha comunicación de datos tenía por objeto la integración de los mismos en un nuevo fichero o su sujeción a un nuevo tratamiento, existiendo un poder de decisión autónomo del cesionario sobre dichos datos que configuraba al mismo como auténtico responsable del mismo.

Conforme al régimen jurídico de las transferencias internacionales de datos efectuadas desde España, con carácter general las mismas están sometidas a la previa autorización del Director de la Agencia de Protección de Datos cuando la misma se vaya a efectuar a países que no proporcionan un nivel de protección equivalente al de la Ley Orgánica 15/1999.

El artículo 34 de la Ley Orgánica excluye de tal requisito determinados supuestos, entre los que figuran el que la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

La no aplicación del régimen de autorización previa del artículo 33 de la Ley Orgánica en modo alguno exime del cumplimiento de los requisitos y obligaciones legales propias de las cesiones o comunicaciones de datos, comenzando con que la misma se efectúe a un tercero para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario, y siguiendo con la necesidad de que la misma cuente con el previo consentimiento del interesado, otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11. 3), salvo que se trate de alguno de los supuestos en que legalmente esta excepcionado dicho consentimiento (artículo 11. 2).

A lo anterior no afecta que la cesión se efectúe entre sociedades integradas en un mismo grupo empresarial, al estarse en presencia de una entidad jurídicamente diferente de aquella a la que los interesados cedieron los datos (aspecto que concurría en el supuesto examinado, donde existían diversas sociedades con distintas personalidades jurídicas), siendo indiscutible que concurre el presupuesto establecido en el artículo 3 i) de la LOPD.

Por otro lado, una vez efectuada la cesión, será preciso que se comunique la misma a la Agencia de Protección de Datos, conforme a lo previsto en el artículo 6 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica, en el que se establece en cuanto a la notificación de ficheros de titularidad privada a la Agencia de Protección de Datos, que la misma deberá especificar "Las transferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos".

El artículo 8 por su parte de la misma norma especifica que "cualquier modificación posterior en el contenido de los extremos a que se refiere el artículo 6 del presente Real Decreto se comunicará, a efectos de inscripción, en su caso, a la Agencia de Protección de Datos, dentro del mes siguiente a la fecha en que aquella se hubiera producido". Por tanto, en el supuesto de una transferencia internacional no comunicada en la notificación inicial del fichero al Registro General de la APD, será de aplicación el precepto y plazo indicado para efectuarla.

Distinto del anterior, fue el supuesto de una empresa que forma parte de un grupo multinacional con presencia en 120 países, el cual, en el ámbito europeo, estaba implantando una centralización del sistema informático en una ciudad europea, donde iban a ubicarse físicamente los servidores y ficheros de todas las filiales europeas. La empresa española grabaría en dicho fichero radicado en ese país europeo los datos de todos sus clientes, accediendo a la información allí almacenada y con la que trabajaría por medio de una conexión telemática a través de líneas privadas y no compartidas.

Se consideró en ese supuesto que el responsable del fichero o tratamiento, en el sentido del artículo 3 d) que lo define como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento", sería la empresa española, mientras que la empresa radicada en un estado comunitario se configura como encargado de tratamiento, en el sentido del apartado g) del mismo artículo que lo define como "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero", dado que el acceso a los datos que se describe, con la única función de almacenamiento o custodia, no es sino la prestación de un servicio al responsable del tratamiento.

La figura del encargado del tratamiento se encuentra regulada en el artículo 12 de la LOPD, que establece: "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento".

En cuanto a los requisitos que exige la LOPD en dicho artículo 12 para la prestación de tales servicios por un encargado de tratamiento, deben considerarse los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento", habiendo desaparecido la posibilidad de conservar los datos durante un periodo máximo de cinco años, que preveía el artículo 27.2 de la LORTAD.

En lo referente a una eventual subcontratación por el encargado del tratamiento con un tercero que implicase una transmisión a éste de los datos en cuestión, de lo establecido en el artículo 12.2 se desprende que no tiene encaje dicha posibilidad en la regulación del supuesto del encargado del tratamiento, según la cual, los datos habrán de ser entregados por éste única y exclusivamente al responsable del fichero sin que le quepa la posibilidad de hacerlo a un tercero

Ello impide, y ello constituye un criterio claro de la APD, la posibilidad de proceder a una subcontratación de este tipo de servicios por parte del encargado del tratamiento, debiendo siempre el responsable ser parte en la relación jurídica, ya que cualquier transmisión de los datos a una terminal que no corresponda al responsable del fichero habrá de ser considerada cesión. Este criterio se ha plasmado en la ya citada Instrucción 1/2000 de la APD, en cuya Norma sexta, apartado segundo, se indica:

"La receptora no podrá comunica los datos ni siquiera para su conservación, a otras personas.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas, situadas fuera del territorio español, se prestasen servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero".

Finalmente, conforme al apartado tercero de la Norma sexta de la Instrucción 1/2000, en caso de que la transferencia efectuada a un encargado del tratamiento se dirija a un destinatario situado en un Estado no miembro de la Unión Europea respecto del que no se haya declarado la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, en el contrato deberán constar cautelas semejantes a las indicadas en la Norma Quinta en lo referente al régimen sancionador y de indemnización a los interesados, así como en lo relativo a las potestades de la Agencia de Protección de Datos, para el caso en que la destinataria emplee los datos para otra finalidad distinta de la que motivó la transferencia, los comunique o los utilice incumpliendo las estipulaciones del contrato".

3.2.6. Videovigilancia en el lugar de trabajo.

Se planteó si resulta conforme a lo establecido en la LOPD la instalación de cámaras para el control de la actividad de los trabajadores de la entidad consultante.

La primera cuestión a resolver fue discernir si las imágenes y sonidos que se obtendrían por tales sistemas de registro se encontraban sometidas a lo dispuesto en la mencionada Ley Orgánica. Para ello fue necesario efectuar dos acotaciones previas:

a) En primer lugar, se plantea el problema de si dichas imágenes y sonidos pueden ser consideradas como datos de carácter personal, de conformidad a lo establecido en la Ley Orgánica de 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal. A tal efecto, y con carácter general, debe indicarse que los artículos 1 y 2 de la citada Ley, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento automatizado de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la Ley Orgánica como "cualquier información concerniente a personas físicas identificadas o identificables".

b) En segundo término, y aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el artículo 3 b) de la Ley.

Pues bien, en relación con el primero de los criterios a los que se ha hecho referencia, debe indicarse que las imágenes a las que se refiere la consulta sólo podrán ser consideradas datos de carácter personal en caso de que las mismas permitan la identificación de las personas que aparecen en dichas imágenes, no encontrándose amparadas en la Ley Orgánica en caso contrario.

Así, en supuestos en que las imágenes se tomaran del lugar de trabajo sí se produciría dicha identificación, dado que

siempre aparecerían en las mismas los trabajadores de la empresa en su lugar de actividad (lo que les hace perfectamente identificables).

Por otra parte, en cuanto a la segunda de las acotaciones, y en referencia a las imágenes obtenidas y, además en el caso examinado registradas, siempre cabría tal identificación derivada de la mera constancia de las cintas grabadas, toda vez que el trabajador se encontraría en su lugar de actividad, siendo perfectamente posible encontrar las imágenes del mismo con el simple conocimiento de su horario. En cuanto al concreto caso examinado, se ignoraba cuales iban a ser los medios de conservación de las mismas, debiendo indicarse que si los mismos podían considerarse estructurados en el modo al que se ha hecho referencia, el fichero se encontrará sometido a lo dispuesto en la Ley Orgánica 15/1999.

Dicho lo anterior, en caso de que exista un sometimiento de los ficheros a la Ley Orgánica, será necesario para proceder al tratamiento de los datos el consentimiento de los afectados, tal y como dispone el artículo 6.1 de la Ley, debiendo informarse a los mismos de los extremos contenidos en el artículo 5.1 de la misma.

Debe finalmente advertirse que el caso examinado, de grabación en vídeo de imágenes, no agota los supuestos en que la obtención o el registro de imágenes pueden quedar sometidos a la LOPD.

3.2.7. Distinción entre ficheros de titularidad pública y de titularidad privada.

Se consultó por una Entidad Pública Empresarial dependiente de una Comunidad Autónoma sobre el carácter público o privado de los ficheros de datos de que era responsable, lo que dio pié a considerar con carácter general la naturaleza pública o privada de los ficheros a la vista de lo establecido en la LOPD.

Como punto de partida, debe indicarse que la Ley no delimita de forma expresa los criterios delimitadores de la titularidad pública o privada de los distintos ficheros, si bien en el articulado del Capítulo I del Título IV viene a identificar los ficheros de titularidad pública como aquéllos cuya responsabilidad corresponde a las Administraciones Públicas (artículos 20 y 21), estableciendo ciertas especialidades en su régimen jurídico en las restantes disposiciones de este capítulo y en el artículo 46, en lo que se refiere al régimen sancionador. A partir de estos preceptos, deberá determinarse cuál es la interpretación que deba darse al término "titularidad pública", contenido en las citadas disposiciones, planteándose dos posibles criterios: por un lado el meramente subjetivo, que atiende a la naturaleza pública o privada del responsable del fichero; por otro, el criterio planteado por la consulta que atiende a la función desempeñada por dicho responsable.

Pues bien, como punto de partida, entendemos que, tal y como se desprende de las disposiciones de la LOPD, el criterio que ha de prevalecer en este punto es el relativo a la naturaleza pública o privada del responsable, ya que la Ley no se diferencia ambas categorías de ficheros con base en criterios relacionados con la actividad llevada a cabo por el responsable, sino con el criterio de la "titularidad" del fichero. Así se desprende, no sólo de las rúbricas de los Capítulos I y II del Título IV de la Ley, sino de lo dispuesto en el artículo 46, que establece una especialidad en materia sancionadora para los supuestos de ficheros de titularidad pública, refiriéndose a los mismos como "ficheros de los que sean responsables las Administraciones Públicas", añadiendo, en su apartado segundo la posible imposición de las sanciones "establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas".

En el caso examinado, como se ha indicado, el responsable del fichero era una Empresa Pública, configurada por la norma legal que la creó como entidad de derecho público sometida a lo dispuesto en esa la presente Ley y en sus disposiciones complementarias de desarrollo. Por lo que respecta a las relaciones jurídicas externas, a las adquisiciones patrimoniales y a la contratación, se establecía por ley su sujeción, sin excepciones, al derecho privado. También se indicaba en dicha norma legal que de los acuerdos que dictasen los órganos de gobierno de dicha Empresa Pública conocería la jurisdicción que en cada caso corresponda, sin necesidad de formular la reclamación previa en vía gubernativa. De este último inciso se desprendía que la entidad se encontraba incluso desprovista de las prerrogativas derivadas del procedimiento de reclamación previa al ejercicio de acciones civiles o laborales, establecido por los artículos 120 y siguientes de la Ley 30/1992.

Por ello, no ostentando la responsable del fichero la condición de administración pública, sometida al derecho administrativo, resulta imposible considerar el fichero al que se refiere la consulta como de titularidad pública, siendo un fichero de titularidad privada, sometido a las disposiciones previstas en la LOPD para este tipo de ficheros.

Por otra parte, y en cuanto al criterio para discernir la naturaleza de la actividad desarrollada por la Entidad Pública que formuló la consulta, la cuestión preponderante implicaba atender al ejercicio, en su caso, por la misma, de auténticas potestades administrativas, en el término tradicional del término (tributaria, sancionadora, expropiatoria y disciplinaria); esto es, si la responsable del fichero se encontraba, en el ejercicio de las actividades relacionadas con el fichero, investido de *imperium* , lo que no sucedía en ese caso.

Todo ello aboca a la conclusión ya sostenida, consistente en considerar que el fichero al que se refiere la presente consulta es un fichero de titularidad privada, quedando sometido a las disposiciones contenidas en el Capítulo II del Título IV de la Ley Orgánica 15/1999.

3.2.8. Datos de Facturación de las Oficinas de Farmacia

Con ocasión de una consulta que planteaba si la cesión de los datos contenidos en las facturas giradas por los mayoristas a las oficinas de farmacia, conteniendo simplemente las mismas "datos comerciales como el nombre de los titulares de las farmacias, dirección y número de licenciado, junto a los importes incluidos en facturas y el NIF de los comerciantes farmacéuticos" se encontraba sometida a la Ley 15/1999, se analizó específicamente el alcance de tal norma en relación con dichos establecimientos, efectuando una aplicación concreta de la doctrina antes expuesta en relación con la aplicación de la normativa de protección de datos de carácter personal a comerciantes y empresarios individuales, que como se ha visto, exige una consideración individualizada de cada caso para determinar si los datos se refieren al ámbito profesional del empresario o afectan a su esfera íntima y en consecuencia se afectan en el ámbito de su derecho fundamental a la autodeterminación informativa.

Los datos a que se refería la consultan se relacionaban directamente con las actividades llevadas a cabo por la correspondiente oficina de farmacia, debiendo entonces analizarse la naturaleza de éstas últimas, al margen de la que corresponda al farmacéutico titular de la misma, en su condición de ejerciente de una profesión colegiada.

En este sentido, debe recordarse que la doctrina y las distintas resoluciones e informes de órganos de naturaleza administrativa y jurisdiccional han venido a recalcar la necesaria diferenciación que debe efectuarse entre la persona física del farmacéutico, que ostenta la condición de miembro de una profesión colegiada y el establecimiento del que es titular, que ostenta la condición de establecimiento mercantil.

Así, el informe del Tribunal de Defensa de la Competencia sobre la competencia en el sector farmacéutico, elaborado en 1995, indicaba que "en general, las funciones del farmacéutico tradicional las llevan a cabo hoy los laboratorios farmacéuticos. La tradicional oficina de farmacia va evolucionando hacia un establecimiento comercial de naturaleza mercantil, –cuya titularidad se alcanza mediante la correspondiente licencia administrativa de carácter vitalicio, en el que se venden especialidades farmacéuticas junto con otros productos", indicando más adelante que "el farmacéutico ofrece un servicio, pero también vende un producto, una mercadería", lo que dota al ejercicio de la actividad farmacéutica de una serie de condiciones singulares no detectables en el ejercicio de otras profesiones.

En resumen, se viene a configurar la oficina de farmacia como un establecimiento mercantil, concebido como el conjunto de bienes y servicios que permiten a un empresario desarrollar su actividad empresarial, en los términos previstos en el Código de Comercio o en el Capítulo Segundo de la Ley de 16 de diciembre de 1954 de Hipoteca Mobiliaria y Prenda sin Desplazamiento de la Posesión, o como industria o negocio, en el sentido que definía el artículo 3.2 de la derogada Ley de Arrendamiento Urbanos, de 24 de diciembre de 1964, como "una unidad patrimonial susceptible de ser directamente explotada o pendiente para serlo de meras formalidades administrativas".

Esta conclusión se ve reforzada por el propio régimen regulador de las oficinas de farmacia, contenido, esencialmente en el Real Decreto 909/1978, regulador de su establecimiento, transmisión e integración o de las previsiones contenidas en el artículo 103.4 de la Ley 14/1986, de 25 de abril, General de Sanidad, a cuyo tenor "sólo los farmacéuticos podrán ser propietarios y titulares de las oficinas de farmacia abiertas al público". De este precepto se desprende la necesaria delimitación entre la condición profesional del farmacéutico y su condición de empresario, individual o social, en cuanto titular de la oficina de farmacia. En este mismo sentido, como ya se indicó, el Real Decreto 909/1978 establece, en sus artículos 5 y 6, las condiciones para la cesión, traspaso o venta de una oficina de farmacia, circunstancia que no podría producirse si la misma no ostentase la condición de establecimiento mercantil.

La misma conclusión se alcanza a la vista de la ingente jurisprudencia del Tribunal Supremo, tanto de su Sala de lo Civil como de su Sala de lo Contenicioso-Administrativo, que ha venido a perfilar la naturaleza jurídica de la oficina de farmacia como la de un establecimiento mercantil o un local de negocio, siendo lógica consecuencia la configuración del farmacéutico cuando actúa en su condición de titular de la misma como un auténtico empresario, con independencia de que el mismo revista o no forma societaria, en los términos previstos por los artículo primero y siguientes del Código de Comercio. Pueden citarse, entre otras, la Sentencia TS, 1ª, de 26 de febrero de 1979 o la Sentencia TS, 3ª, de 27 de noviembre de 1998.

3.2.9. Tratamiento de datos de salud

Se han seguido planteando a lo largo de este año numerosas cuestiones en relación con el tratamiento de datos de salud. Particularmente, se han analizado en el ejercicio al que se refiere la presente Memoria la adecuación a la LOPD de distintos supuestos de recogida, tratamiento, comunicación y conservación de datos de salud por centros médicos privados relativos a pacientes del mismo.

En esta materia, de particular interés resulta el examen de la autorización que para el tratamiento de datos de carácter personal relativos a las salud establece el artículo 8 de la Ley, que indica que "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica"

Igualmente, debe considerarse aplicable lo establecido en el artículo 7.6 que indica que los datos de carácter personal relativos a la salud podrán ser objeto de tratamiento cuando el mismo "resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra

personal sujeta asimismo a una obligación equivalente de secreto".

Sin embargo, estas dos últimas especialidades al régimen general, tanto la del artículo 8 como la del artículo 7. 6 no pueden interpretarse de forma genérica o extensiva, (por ejemplo, en el sentido de que baste para el tratamiento de los datos la simple expresión de la opinión de un facultativo en tal sentido), sino que debe restringirse a los dos supuestos en que únicamente será de aplicación, esto es: que una disposición normativa establezca y disponga con carácter específico un tratamiento de tales datos, o bien que el mismo resulte efectivamente necesario e imprescindible, y ello se justifique debidamente en cada caso concreto. Fuera de estos dos supuestos excepcionales, el régimen aplicable con carácter general es el del artículo 7. 3 de la LOPD, que debe recordarse, establece que "Los datos de carácter personal que hagan referencia al origen racial, la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

3.2.10. Acceso a los datos del Padrón por concejales de corporaciones locales.

Ya viene siendo habitual analizar en este apartado de la Memoria anual de la Agencia de Protección de Datos algún aspecto relativo al Padrón Municipal de Habitantes, exponiendo en esta ocasión un supuesto que ha sido planteado en varias ocasiones en este periodo, relativo al acceso por parte de concejales de ayuntamiento a los datos del padrón municipal, extendiendose en ocasiones el contenido de las consultas a la posibilidad de acceso a los datos del censo electoral.

En primer lugar, en cuanto a la cesión a concejales de los datos contenidos en el Padrón Municipal de Habitantes, debe partirse de lo dispuesto en el artículo 11.1 de la LOPD, que indica: "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"; disposición que debe complementarse en el supuesto examinado con lo dispuesto en el artículo 21 de la propia Ley Orgánica, en relación a la cesión de datos entre Administraciones Públicas, estableciéndose que la misma podrá tener lugar siempre que una Ley la prevea o la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

En particular, y en lo referente al Padrón Municipal de Habitantes, el artículo 16.3 de la Ley Reguladora de las Bases del Régimen Local prevé que sólo procederá la cesión de los datos contenidos en el padrón municipal a otras Administraciones en los supuestos en que dicha cesión se refiera a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio.

Considerando el supuesto de que dicha cesión pueda efectuarse a concejales municipales cuando estos lo soliciten, debe valorarse la necesidad propia de los concejales de una corporación municipal de estar debidamente informados, a fin de llevar a cabo su función de control sobre la actividad del equipo de Gobierno del Ayuntamiento. A fin de dar una correcta solución a la cuestión, será preciso tomar en consideración las funciones que la vigente normativa atribuye a los miembros de las corporaciones locales.

Según dispone el artículo 77 de la Ley 7/1985, de 2 de abril de 1985, de Bases de Régimen Local, "todos los miembros de las Corporaciones locales tienen derecho a obtener del Alcalde o Presidente o de la Comisión de Gobierno cuantos antecedentes, datos o informaciones obren en poder de los servicios de la Corporación y resulten precisos para el desarrollo de su función".

Este derecho se encuentra desarrollado por los artículos 14 a 16 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las corporaciones Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre, que especifica el modo en que deberá producirse la solicitud, así como las particularidades para el ejercicio de la consulta.

Tomando en consideración lo anteriormente señalado, y dado que las leyes atribuyen a los concejales la posibilidad de consultar la documentación obrante en el ayuntamiento, en el ejercicio de su actividad de control de los órganos de la Corporación, la cesión de los datos en que consistiría la consulta se encuentra amparada por los artículos 11.2 a) y 21.1 de la Ley Orgánica 15/1999.

En estos supuestos, el cesionario sólo podrá utilizar los datos en el ámbito y para el concreto fin del ejercicio de esta competencia, toda vez que éste es el límite establecido en la LBRL, indicando a su vez el artículo 4.2 de la Ley Orgánica 15/1999 que los datos "no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos", habiéndose en consecuencia informado desfavorablemente supuestos de utilización de los datos del Padrón Municipal Habitantes por parte de miembros de una corporación (incluido el Alcalde) para la remisión de cartas salutatorias a determinados residentes en el municipio.

Respecto a la posibilidad de acceso a los datos del Censo Electoral, debe recordarse como esta Agencia de Protección de Datos ha considerado en diversas ocasiones que el mismo no tiene el carácter de fuente accesible al público, en los términos previstos en el artículo 3 j) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (como tampoco lo era con arreglo a la derogada LORTAD).

El artículo 41.2 de la Ley Orgánica 5/1985, reguladora del Régimen Electoral general establece que "queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral, a excepción de los que se soliciten por conducto judicial".

En este sentido, hay que tener en cuenta que la Junta Electoral Central en fecha 2 de octubre de 1995, en contestación a una consulta formulada por el Director de la Agencia de Protección de Datos, señala que "en virtud de lo establecido en el artículo 41 de la Ley Orgánica del Régimen Electoral General, está prohibida la información particularizada de los datos personales contenidos en el censo electoral, no estando permitida la recopilación de los datos existentes en las mismas por cualquier medio sea manual, fotográfico, informático o de cualquier otra naturaleza, bajo las responsabilidades legales procedentes".

En virtud de todo lo cual, la Agencia de Protección de Datos ha indicado en diferentes ocasiones, de acuerdo con los criterios señalados, que el Censo Electoral no constituye una fuente accesible al público, en los términos de la Ley Orgánica 15/1999.

De forma mas concreta, en cuanto al acceso a los datos del Censo Electoral por parte de concejales municipales, debe indicarse que en cuanto los mismos sean candidatos a las elecciones municipales, el artículo 41.5 de la Ley Orgánica 5/1985, de 19 de junio reguladora del régimen electoral general en la redacción dada por la Ley Orgánica 3/1995 , de 23 de marzo, establece que "Los representantes de cada candidatura podrán obtener el día siguiente a la proclamación de candidaturas una copia del censo del distrito correspondiente, ordenado por Mesas, en soporte apto para su tratamiento informático, que podrá ser utilizado exclusivamente para los fines previstos en la presente Ley".

En consecuencia sí resultaría posible el acceso a los datos censales por parte de los candidatos, pero trayendo dicho acceso causa de lo establecido en la Ley Orgánica anteriormente citada. En efecto, uno de los principios básicos que rige en materia de protección de datos de carácter personal (y que es tutela, no se olvide, de un autentico derecho fundamental como es el de la autodeterminación informativa o privacidad de los datos, reconocido como tal y autónomamente del derecho fundamental a la intimidad de las personas por la Sentencia del Tribunal Constitucional 292/2000) es el de finalidad en el uso de los datos de carácter personal, consagrado en el artículo 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, según el cual "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación en el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

Este principio, junto al resto de los proclamados en la materia y la regulación normativa anteriormente analizada lleva a la Agencia de Protección de Datos a mantener el criterio sostenido en numerosos casos precedentes, y que se ha expuesto con anterioridad, en cuanto a la utilización de cada fichero o registro de datos de carácter personal de acuerdo con la estricta finalidad para la que se creó, y entendiendo que la cesión de los datos incluidos en el mismo habrá de limitarse a los supuestos autorizados por la Ley.

Así, el Censo Electoral conforme a la normativa citada, se cede exclusivamente para los fines previstos en la Ley Orgánica de Régimen Electoral General (comunicación por los candidatos con los electores mediante envíos postales de propaganda electoral, ejercicio por los apoderados e interventores de los candidatos de sus funciones propias de examen y control de las operaciones de voto y escrutinio, etcétera), sin que se integre en tales fines, ni se encuentre amparado por otra norma legal (única que puede habilitar la cesión de este tipo de datos), la utilización del Censo Electoral por concejales municipales ya electos durante su mandato para el ejercicio de sus funciones propias.

4. ANÁLISIS JURISPRUDENCIAL

4.1. Análisis de las principales sentencias de la Jurisdicción Contencioso Administrativa.

Debe comenzarse este epígrafe indicando como en año 2001, hasta la fecha en que se redacta la Memoria de la APD correspondiente a dicho año, se tiene conocimiento de un total de 110 Sentencias dictadas por órganos judiciales de la jurisdicción contencioso administrativa derivadas de recursos interpuestos contra resoluciones del Director de la APD, las cuales, y conforme a lo dispuesto en el artículo 48.2 LOPD, agotan la vía administrativa.

Dichas sentencias han emanado de los Tribunales Superiores de Justicia (concretamente, todas ellas del de Madrid con la única excepción de una sentencia dictada por el TSJ de Cataluña) y de la Audiencia Nacional, órgano judicial que tras la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso Administrativa, asumió la competencia para conocer de dichos recursos que antes de la entrada en vigor de dicha norma correspondía a los primeramente citados.

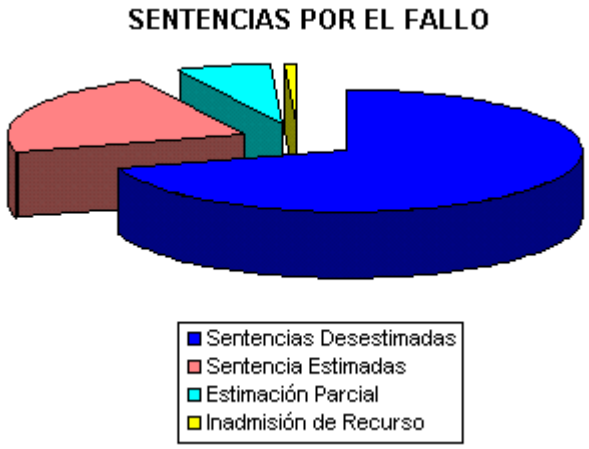
En un único caso se ha pronunciado el Tribunal Supremo (STS, 3ª, 24-5-01), aunque en un recurso interpuesto contra un Auto que acordaba la suspensión de la ejecución de una resolución sancionadora, sin contener la misma pronunciamiento de interés en materia de protección de datos.

De las 110 sentencias referidas, y excluyendo la anteriormente referida, 57 corresponden a la Sala de lo contencioso administrativo de la Audiencia Nacional y otras 52 a Tribunales Superiores de Justicia (51 al de Madrid y una al de Cataluña), pudiéndose extraer dos claras conclusiones al contrastar dichas cifras con las que constan en la Memoria correspondiente al año 2000. En primer lugar, el notable incremento de sentencias recaídas, 112 frente a 54 del año anterior, cifra que denota y se corresponde con el cada vez mayor número de resoluciones dictadas por la APD.

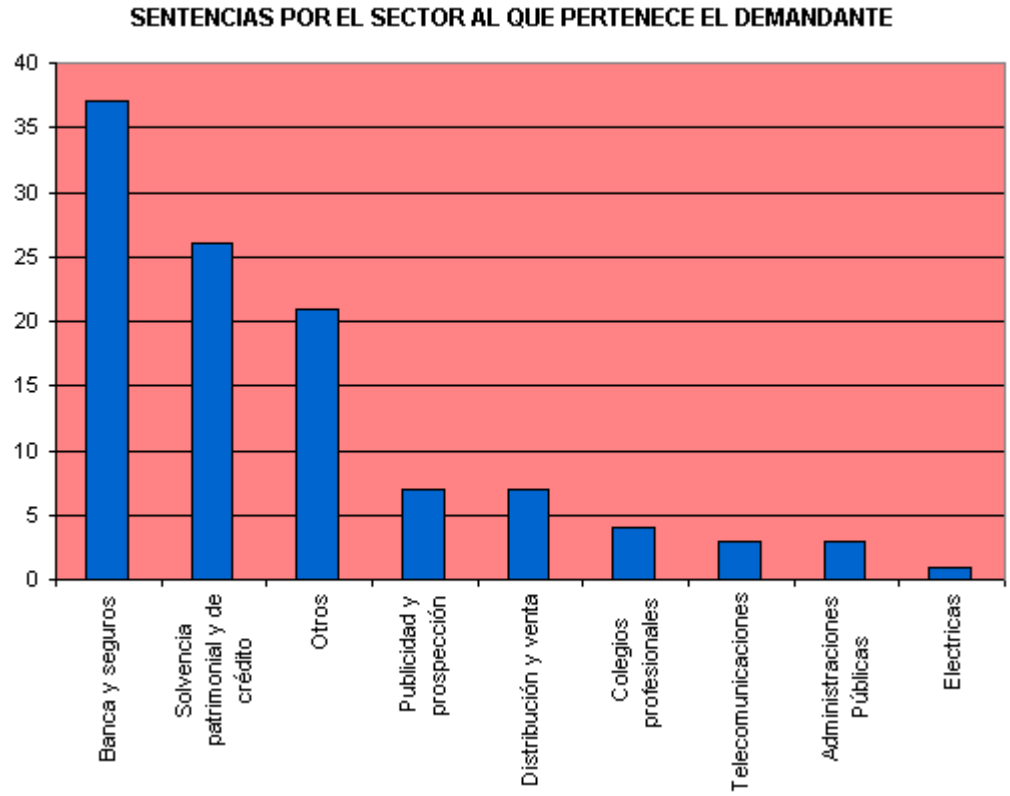
En segundo lugar, la equiparación en cuanto a número de resoluciones entre la Audiencia Nacional y

Tribunales Superiores de Justicia, que acentúa la importancia de la doctrina sentada por aquél órgano jurisdiccional, llamado a configurarse, a medida que se vayan resolviendo los recursos pendientes en los Tribunales Superiores de Justicia, como el único competente en la materia, (sin perjuicio, claro está, del ámbito superior que es propio del Tribunal Constitucional y del Tribunal Supremo). Ello justifica que demos preponderancia en el análisis de las principales resoluciones judiciales del año 2001 que se expondrá a continuación, a las emanadas de dicho tribunal.

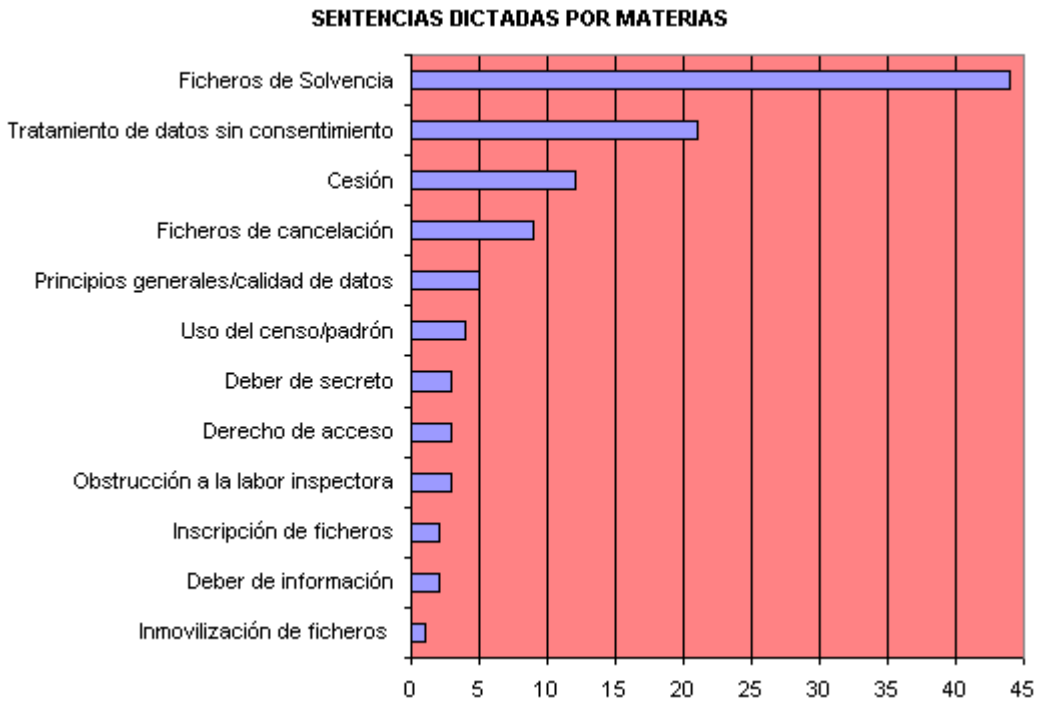
En cuanto al sentido de los pronunciamientos judiciales, señalar que de las 110 sentencias analizadas, 78 fueron desestimatorias, confirmando los actos dictados por la APD, 24 estimaron íntegramente las demandas, 8 de ellas lo hicieron parcialmente, y en un único caso se inadmitió el recurso.



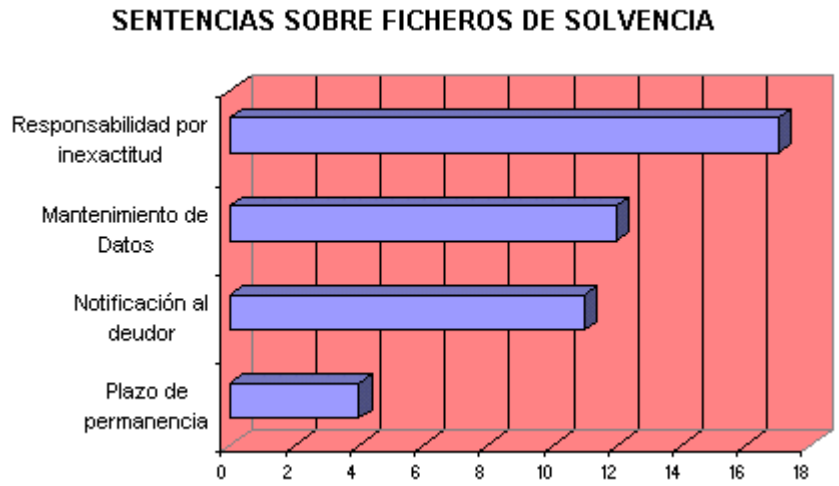
Atendiendo al sector o ámbito de actuación del recurrente, puede establecerse la siguiente distribución de los pronunciamientos judiciales:



Finalmente, atendiendo a la materia objeto del proceso resulta la siguiente distribución:



Al igual que en la memoria correspondiente al año 2000, en este periodo el mayor número de sentencias han tenido por objeto los ficheros de solvencia patrimonial y crédito, siendo de interés examinar qué cuestiones se han tratado, en relación con los mismos, en los procedimientos judiciales finalizados en el año 2001:



4.1.1. Ficheros de solvencia patrimonial y crédito

Durante el año 2001, como se puede comprobar en las estadística anteriores, han seguido siendo las más numerosas las resoluciones judiciales relativas a ficheros de solvencia patrimonial y de crédito, la mayoría de ellas relativas a sanciones impuestas por la APD a responsables de los mismos bien por inclusión de datos inexactos en los mismos (17 sentencias), bien por mantenimiento de dichos datos inexactos (12 sentencias) o bien por falta de comunicación a los afectados de la inclusión de sus datos en los mismos (11 sentencias).

En esta materia concreta se han mantenido los criterios ya sentados por los órganos judiciales al respecto y que fueron

expuestos en la Memoria APD correspondiente al año 2000.

Así, y en relación con las obligaciones inherentes a este tipo de ficheros, la Sección novena del TSJ de Madrid se ha pronunciado en varias ocasiones, pudiéndose citar de entre ellas la Sentencia 28 de mayo de 2001, en la que analizando tanto el artículo 28 de la LORTAD como la Instrucción 1/1995, de la APD, de 1 de marzo, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito, indica "esta Sala y Sección llega a la conclusión de que es al acreedor, en este caso la Entidad Bancaria suministradora del dato al fichero común, a quien incumbe la responsabilidad de la veracidad y calidad de los datos, debiendo comunicar al titular del fichero común –la actora- el dato inexistente o inexacto a fin de que proceda a su cancelación o modificación. Sin embargo, la notificación de la inclusión del dato en el fichero común corresponde al titular de éste, única obligación que, por lo que aquí interesa, le es exigible, así como la de proceder a la cancelación o modificación del dato una vez es requerido para ello por el acreedor cedente del mismo (...) En definitiva es a los acreedores cedentes de los datos registrados en el fichero común a los que incumbe la obligación de comunicar al titular del mismo el dato inexistente o inexacto a fin de que proceda a su cancelación o modificación para las que carece de competencia el titular de aquel".

Esta Sentencia, confirmando el criterio de la Agencia al respecto, igualmente recuerda, en relación con el mantenimiento de datos erróneos en dichos ficheros que "esta sección se pronunciado al respecto en diversas resoluciones estableciendo en definitiva la obligación de la Entidad Bancaria de efectuar barridas u operaciones de seguimiento respecto de los datos que hayan comunicado al fichero común, entre otras en Sta. nº. 1031 de 15-XII-2000 con objeto de satisfacer la exigencia prevista en el citado artículo 4.3 de la L.O. 5/1992 de 29-X"

En relación con las consecuencias del mantenimiento de datos erróneos o inexactos, se ha apreciado la concurrencia de un perjuicio al afectado en supuestos de denegación de un crédito bancario al mismo. Así, la Sentencia del Tribunal Superior de Justicia de Madrid de 30 de mayo de 2001 indica que la denegación de un crédito al afectado por la subsistencia de un apunte adverso determinó que "los derechos de la denunciante, de hecho, se vieran afectados, siendo irrelevante para la calificación de grave o leve de la infracción el que la inclusión de una deuda en un fichero de información de solvencia patrimonial no implique necesariamente la denegación de un préstamo, extremo que, obviamente, queda al libre criterio de la entidad prestamista, pero es razonable pensar que los clientes de estos ficheros de información de morosos consultan los mismos con el propósito de cerciorarse de la solvencia de sus potenciales clientes". Se ratifica así el criterio también seguido por la APD al respecto.

4.1.2. Otras cuestiones de Interés

4.1.2.1. Inclusión de un dato notorio pero no público en una base de datos sin el consentimiento del interesado

La Sentencia de la Audiencia Nacional de 28-9-01 desestimó el recurso interpuesto contra la sanción impuesta a una empresa de servicios turísticos, por incluir en sus bases de datos, junto a los datos personales obtenidos de una fuente accesible al público, otro relativos a pertenencia de una persona a un partido político, que aun siendo notorio y de público dominio, no constaba en aquella fuente.

La Sala invoca la STC 292/2000, que señala que el derecho fundamental a la protección de datos "alcanza a aquellos datos personales públicos, que por el hechos de serlos, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de los datos... el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquéllos que identifiquen o permitan la identificación de una persona".

Considera que conforme a esta doctrina constitucional, el carácter notorio de un dato personal no determina la inaplicación al mismo de la Ley de Protección de Datos y por tanto, no puede admitirse que dicho dato (en este caso la pertenencia o simpatía de una persona a un partido político) pueda tratarse automatizadamente sin consentimiento del afectado. Excluir de la protección legal aquellos datos públicos y notorios implicaría establecer peligrosas excepciones a la tutela de derechos fundamentales carentes de apoyo constitucional y legal.

4.1.2.2. Graduación de sanciones y proporcionalidad.: aplicación retroactiva del artículo 45.4 LOPD a sanciones impuestas bajo la vigencia de la LORTAD

Un tema tratado en numerosas resoluciones ha sido el relativo a la aplicación retroactiva no sólo del artículo 45.4 LOPD (criterios para la graduación de la cuantía de las sanciones), sino también del 45.5 (aplicación de la cuantía correspondiente a la escala de infracción inmediatamente menos grave cuando se aprecie una cualificada disminución de la antijuridicidad del hecho o de la culpabilidad del imputado).

Así, en la Sentencia de la Audiencia Nacional de 25 de mayo de 2001 se analiza la cuestión (que, en todo caso, debe ser considerada individualmente en cada supuesto, pues la atenuación en la graduación de la sanción que implica la aplicación retroactiva de la norma citada exige una ponderación de la culpabilidad, elemento subjetivo que ha de estar presente en toda actuación infractora para que proceda la aplicación de la sanción, aun a título de mera falta de diligencia).

La Sentencia comentada, después de recordar que el principio de proporcionalidad "comporta que cualquier actuación de los poderes públicos limitativa o restrictiva de derechos responda a los criterios de necesidad y adecuación al fin perseguido, dicho en términos legales, debe de existir una `debida adecuación entre la gravedad del hecho constitutivo

de la infracción y la sanción aplicada´ (artículo 131.3 de la Ley 30/1992)", analiza el elemento subjetivo presente en el hecho sancionado por la APD así como las consecuencias de la actuación infractora e indica. "Si bien es cierto, como ya se ha dicho, que la cesión de datos de carácter personal constituye una infracción muy grave que lleva aparejada una severa sanción, sin embargo en este caso concurren una serie de singularidades que revelan una cualificada disminución de la culpabilidad, y que determinan la aplicación del artículo 45.5 de la Ley Orgánica de 1999. En efecto, las consecuencias derivadas de la cesión han sido que el afectado ha tenido conocimiento de un plan de pensiones que no pensaba conocer, por tanto, el perjuicio ocasionado por la cesión de datos no es grave, a juicio de esta Sala. Por otro lado, las dudas del Colegio Profesional recurrente sobre los límites de su conducta en esta materia, que le llevaron a platear una consulta ante la Agencia de Protección de Datos, y a dar una confusa interpretación de la respuesta dada por la expresada Agencia, unido a una interpretación literal de las funciones propias de los colegios profesionales, al amparo de las cuales consideraba lícita su actuación, revelan esa cualificada disminución de la culpabilidad que rebaja el reproche social de su conducta y determina la aplicación retroactiva de la facultad estable - cida en el artículo 45. 5 de la Ley Orgánica de 1999"

Frente a lo anterior, y sobre la misma cuestión, la Sentencia también de la Audiencia Nacional, de 5 de mayo de 2001 indica:

"La cuestión que se suscita en autos no es nueva para esta Sala, quien ya en alguna sentencia recaída sobre actos administrativos que sancionaban hechos acaecidos con anterioridad a la entrada en vigor de la Ley 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, ha aplicado la previsión de su artículo 45.5 en cuanto esta aplicación favorecía al infractor.

Ahora bien, en autos valoradas las actuaciones, la Sala llega a la conclusión de que no se dan esas circunstancias que exige la norma, y que conllevan una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho.

La parte actora pretende justificar tal concurrencia en el hecho de que el único tratamiento realizado ha sido la inclu - sión de la Sra. XXX, y que tales datos no han sido objeto de cesión, comunicación o cualquier otro tipo de actuación por la actora. Pues bien, la actora, como indica en el Hecho quinto de su demanda, es una *empresa dedicada a la publi - cidad y al marketing directo,* y en el ejercicio de su actividad ha vulnerado el principio de consentimiento consagrado en el artículo 6 de la L.O. 5/1992, quedando su actuación dentro de las previsiones del artículo 43.3, como se razona en el Fundamento tercero. Ninguna circunstancia se aprecia sobre el hecho por el que ahora ha sido sancionada –sea o no el único dato que ha obtenido irregularmente- a la hora de atender la nueva pretensión, sino es la insistencia en pretender desvirtuarlo, en lugar de reconocerlo y lamentarlo. Las restantes circunstancias que señala se proyectan hacia el futuro y, en su caso, podrían originar una agravación del tipo sancionador.

En conclusión, la actuación dolosa, e igual de haberse estimado que era gravemente negligente, ha llevado a la Admi - nistración a sancionarla, fijando la cuantía de la multa en el mínimo permitido, y estimamos que en tan favorable determinación quedan recogidas las razones que aduce ahora la parte actora para aplicar la previsión del art. 45.5 de la nueva normativa; pretensión basada en cualificada disminución de la culpabilidad o antijuridicidad que la parta no ha entrado a concretar analizar y justificar; y que la Sala, como hemos dicho, no aprecia."

4.1.2.3. Carácter público de las actuaciones judiciales.

Varias han sido las resoluciones que, con ocasión del análisis de ficheros comunes de morosidad, han reseñado que las actuaciones judiciales y su plasmación en los diversos modos de constancia y publicidad no constituyen, a los efectos del artículo 3 j) de la LOPD fuente accesible al público, es decir, "aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin mas exigencia que, en su caso, el abono de una contraprestación...".

Estos pronunciamientos tienen gran importancia en relación con los ficheros creados por entidades dedicadas a la prestación de servicios de información sobre solvencia patrimonial y crédito, regulados en el artículo 29 de la LOPD, cuyo apartado primero limita el origen de los datos incluidos en los mismos al indicar que quienes se dediquen a pres - tar estos servicios "solo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento".

Así, la Sentencia de la Audiencia Nacional de 29 de noviembre de 2001 que analiza un supuesto de inclusión de datos personales en un fichero automatizado sin haber recabado previamente el consentimiento de los interesados, indica:

"También aquí la demandante pretende acogerse a lo dispuesto en el artículo 6.2 que, como ya sabemos, determina la inexigibilidad del consentimiento de los interesados cuando los datos provengan de fuentes accesibles al público, y a tal efecto la empresa recurrente afirma que los datos a que se refieren estas dos resoluciones provienen de los **Libros de Registro de los Juzgados**. Pues bien, por las razones que seguidamente expondremos esta sala entiende que los libros de registro de los órganos judiciales no pueden ser considerados fuentes accesibles al público a los efectos señalados en el artículo 6.2 de la Ley Orgánica 5/1992.

La publicidad de las actuaciones judiciales viene afirmada de manera reiterada en diferentes preceptos de la Ley Orgánica del Poder Judicial (véanse, entre otros, los artículos 232, 235 y 266.1 LOPJ). En particular, nos interesa destacar que según el artículo 235 LOPJ *los interesados tendrán acceso a los libros, archivos y registros judiciales que no tengan carácter reservado, mediante las formas de exhibición*, *testimonio o certificación que establezca la Ley*. Y el

artículo 266.1 LOPJ determina en su último inciso que se permitirá a cualquier interesado el acceso al texto de las sentencias. Ahora bien, el tenor en apariencia concluyente de estos preceptos no autoriza a afirmar –por más que así lo pretenda la demandante- que los libros del registro y archivos judiciales sean una **fuente accesible al público** en el sentido que confiere a esta expresión el artículo 6.2 antes citado de la Ley Orgánica 5/1992.

Por lo pronto, precisamente con relación a lo dispuesto en los artículo 235 y 266 LOPJ acerca de la publicidad de las actuaciones y el acceso a los datos de los libros y archivos judiciales el Tribunal Supremo tiene declarado en su **STS de 3 de marzo de 1995** que < la publicidad procesal, en su vertiente de derecho a la información y de acceso a las sentencias ya depositadas, requiere, como hemos anticipado, por parte de quien la invoca y ejercita, la concurrencia de la condición de "interesado" sin que, hemos también de apresurarnos a esta precisión, la expresión "cualquier interesado" empleada por el artículo 266.1 respecto a las sentencias añada matiz alguno ampliatorio al básico concepto de interesado, por tratarse de mera enunciación reduplicativa y quizás dirigida a no constreñirla a quienes han sido partes o intervenido de cualquier forma (testigos, peritos, etc.) en el proceso al que la sentencia o sentencias han puesto fin. Pues bien, el interés legítimo que es exigible en el caso solo puede reconocerse en quien, persona física o jurídica, manifiesta y acredita, al menos "prima facie" ante el órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso –y por ende, de la sentencia que lo finalizó en la instancia-, bien con alguno de los actos procesales a través de los que aquel se ha desarrollado y que están documentados en autos...>>.
Partiendo de estas consideraciones la sentencia del Tribunal Supremo concluye que no cabe reconocer a tales efectos la condición de "interesado" a una entidad que –al igual que sucede con la demandante en el **presente** litigio- es una empresa cuya actividad mercantil se centra en la confección de una base de datos informatizada que pone a disposición de terceros datos de carácter económico afectantes a partes intervenientes en procesos civiles, para que los destinatarios de la información conozcan las circunstancias de solvencia patrimonial de las personas físicas o jurídicas a las que se refieren tales datos.

Desde otro punto de vista, viene a converger con la doctrina jurisprudencial a que acabamos de referirnos la definición de "**datos accesibles al público"** contenida en el Real Decreto 1332/1994, de 20 de junio, de desarrollo de la Ley Orgánica 5/1992. Según el artículo 1.3 del mencionado Real Decreto son datos accesibles al público <los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo>> . Pues bien, los datos contenidos en los libro y registros judiciales no se encuentran a disposición del público de forma enteramente libre e indiscriminada ya que el acceso a los mismos está regulado y en cierta medida restringido. De un lado, por la apelación que hacen los citados artículo 235 y 266.1 de la Ley Orgánica del Poder Judicial a la condición de "interesado", de cuya significación y alcance ya conocemos la interpretación jurisprudencial. De otra parte, porque el acceso a tales libros y archivos está mediatizado por la necesaria intervención del Secretario Judicial y la preceptiva sujeción al trámite de solicitud y autorización regulado en los artículos 1 a 5 del Reglamento 5/1995, de 7 de junio, del Consejo General del Poder Judicial, sobre aspectos accesorios de las actuaciones judiciales (BOE nº. 166 de 13 de junio de 1995).

No se ha cuestionado en este proceso si los datos que la empresa demandante afirma haber tomado de los libros de registro de los Juzgado fueron obtenidos con observancia de las normas y trámites que acabamos de mencionar. Pero en realidad tal cuestión resulta irrelevante para la resolución del litigio. Lo que procede aquí destacar es que la propia existencia de esa regulación y de los requisitos y trámites que en ella se establecen lleva a la conclusión de que los datos contenidos en los libros y archivos judiciales no son subsumibles en la definición de "datos accesibles al público" contenida en el ya citado artículo 1.3 del Real Decreto 1332/1994, de 20 de junio. Ello nos conduce a afirmar que no opera aquí la dispensa del requisito del consentimiento prevista en el artículo 6.2 de la Ley Orgánica 5/1992 y que, en consecuencia, al no haber recabado el consentimiento de los interesados que exige el artículo 6.1 de dicha Ley, la empresa demandante incurrió efectivamente en sendas infracciones graves tipificadas en el artículo 43.3 d) de la propia Ley Orgánica 5/1992"

La doctrina que se recoge en esta Sentencia aplicando la LORTAD, entendemos es perfectamente trasladable a los supuestos análogos que puedan acaecer bajo la vigencia de la LOPD.

Comentada la anterior, debe sin embargo hacerse igualmente referencia a la Sentencia también de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 13 de junio de 2001, que examinando un supuesto en que una empresa dedicada a análogas actividades de prestación de servicios de información sobre solvencia patrimonial y crédito incluyó en sus ficheros datos obtenidos del Registro de la Propiedad y de tablones de anuncios de los juzgados establece lo siguiente (que debe en todo caso considerarse desde la perspectiva de que la norma aplicada fue la LORTAD, con las modificaciones que, frente a ella y en relación con Registros públicos ahora incluidos en el ámbito de la Ley de protección de datos, introdujo la LOPD), indica:

"A juicio de la APD los datos obtenidos de anotaciones del Registro de la Propiedad, aunque procedan de una base de datos pública, en virtud de la Instrucción de 12 de junio de 1985 de la Dirección General del Notariado, norma 5ª, que considera carentes de interés legítimo a quienes pretendan acceder a la información contenida en los libros del registro con la finalidad de comercializar por cualquier procedimiento la propia información obtenida, carecen de cobertura legal para el tratamiento informático.

De la misma forma, considera que el que no sea interesado carece de interés legítimo para tratar los datos recogidos de los tablones de anuncios de los Juzgados y cederlos posteriormente, pues dicha información se está no sólo compilando sino proporcionando a personas físicas o jurídicas para las que en principio no iba destinada, por no ser intere-

sados en esas causas judiciales.

Sin embargo la Sala no puede compartir la tesis de la Agencia de Protección de Datos, porque claramente el artículo 6. 2 de la LORTAD señala que " **No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público..."**

La restricción con que interpreta el precepto la APD, al entender que la utilización de los datos registrales de personas incorporadas en masa a los ficheros, como los datos publicados en los tablones de anuncios de los Juzgados, que en cualquier caso necesita para su tratamiento el consentimiento previo de los mismos, deja sin contenido el precepto, porque todas las fuentes accesibles al público, entre las que se pueden citar también, boletines oficiales, periódicos, guías telefónicas, listados colegiales, repertorios de jurisprudencia, etc., encontrarán con (sic) el obstáculo de que los datos de ellos obtenidos no han sido publicados con la finalidad de hacer de ellos un tratamiento informático con objeto de su comercialización.

La propia Ley no contempla semejante limitación.

Si acudimos a la nueva Ley 5/1999, de 13 de diciembre, que no es aplicable al caso de autos, sus preceptos homónimos de la Ley anterior 5/1992, son el art. 6.2 que establece que " no será preciso el consentimiento cuando... los datos figuren en fuentes accesibles al público **y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"**; y el artículo 29. 1 que dispone que: "Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito solo podrán tratar automatizadamente datos de carácter personal **obtenidos de los registros y las fuentes accesibles al público establecidos al efecto...".**

De un lado parece exigirse un interés legítimo para el responsable del fichero y de otro que los registros y las fuentes de acceso estén establecidas al efecto.

Con independencia de la interpretación que pueda darse a estos preceptos de la nueva Ley de Protección de Datos, sobre si contienen o no mayores restricciones para quien se dedica a la prestación de este tipo de servicios de información, lo cierto es que en élla el legislador ha pretendido acentuar o subrayar los límites del contenido a la excepción de consentimiento del afectado para el tratamiento automatizado de datos, que se produce cuando estos se recogen de fuentes accesibles al público, dando mayor claridad a unos contornos que antes aparecían mas difuminados.

Y que duda cabe que de existir semejantes restricciones no estaban contempladas en la Ley que aplicamos.

La propia Agencia de Protección de Datos no considera necesario el consentimiento cuando los datos son obtenidos de diarios oficiales. Es decir, en caso de las publicación de un edicto en distintos Boletines Oficiales (Estado, Comunidades Autónomas o Provincias), acordando cualquier incidencia en un procedimiento judicial, remate, subastas, adjudicación, etc., se pueden tratar automatizadamente los datos obtenidos en esa fuente. Ahora bien, si estos mismos datos se obtienen de los edictos publicados en los tablones de los Juzgados, se precisa el consentimiento de los afectados, si no se obtiene da lugar dicha conducta a sanción, cuando la única variante es el vehículo utilizado para dar a conocerlos.

Por esa razón carece de sentido distinguir entre los distintos medios en que se produce la divulgación de los datos, a los que cualquiera, sin restricción, puede acceder.

Siendo así que los datos que conformaron los ficheros sobre insolvencia patrimonial de la entidad actor, fueron obtenidos de fuentes accesibles al público, como son el Registro de la Propiedad y los tablones de anuncios de los Juzgados, tal y como establece el artículo 6.2 de la LORTAD, no es preciso el consentimiento del afectado".

El interés de traer a colación esta Sentencia, aun cuando rectifica en parte un criterio mantenido por la APD, deriva de la constatación de la apreciación judicial del cambio acaecido en la regulación de las fuentes accesibles al público tras la promulgación de la LOPD y frente a lo que establecía la LORTAD. Reiterar, finalmente, lo ya expuesto en cuanto a que conforme a aquélla, el Registro de la Propiedad ya no se encuentra excluido del ámbito de la Ley, por un lado, y la taxativa enumeración de lo que debe considerarse fuente accesible al público por otro –con las consecuencias en orden a la apreciación como tal de los Registros de la propiedad y mercantiles, por ejemplo-, significando igualmente que nada se dice que contradiga lo indicado en la sentencia citada en primer lugar en este epígrafe en orden a la carencia de la naturaleza de fuente accesible al público de las sentencia judiciales

4.1.2.4. Envío por colegios profesionales de información a colegiados

Varias han sido en el año 2001 las sentencias de la Audiencia Nacional que han resuelto recursos interpuestos contra resoluciones sancionadoras de la APD a colegios profesionales por cesión de datos de sus colegiados o el envío a estos de propaganda e información sobre productos diversos (hasta cuatro sentencias), que han venido, ratificando el criterio de la APD, a delimitar dicha posibilidad.

A modo de ejemplo cabe citar la Sentencia de la Audiencia Nacional de 25 de mayo de 2001 que establece al respecto:

"Las funciones de los Colegios Profesionales, establecidas en la Ley 2/1974, de 13 de febrero, a los efectos de la protección de los datos de carácter personal y cuando el afectado ha manifestado expresa y reiteradamente su negativa a recibir publicidad, deben ser interpretadas en sentido estricto, dicho de otra forma, las expresadas funciones de los colegios profesionales, a estos efectos, coinciden con la esencia de su actividad y no puede ser interpretado, como pretende la recurrente al amparo de la propia Ley 2/1974, en un sentido amplio comprensivo de cualquier acción para la mejora de los colegiados. Acorde con ello, se permite el envío a colegiados de las publicaciones o circulares que tengan directa relación con el ejercicio profesional; es decir, que revistan el carácter de necesarios e imprescindibles para el desarrollo de la profesión médica en este caso. Ahora bien, ello no puede servir de excusa para que al socaire de tal función se pueda enviar otro tipo de documentación que guarda una relación indirecta, y a veces remota, con la profesión médica. Este es el caso, según ya recogimos en el primer fundamento, de la publicidad remitida sobre telefonía móvil, exposiciones de cultura, cursos de ingles y programa del Xacobeo 99".

4.1.2.5. Acumulación de procedimientos administrativos por organismo público

Se han formulado en el año 2001 denuncias ante la APD contra órganos administrativos que en la tramitación de procedimientos (concretamente recursos en vía administrativa) acordaron la tramitación acumulada de los mismos de acuerdo con el artículo 73 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Al conceder plazo de alegaciones a los interesados, se les puso de manifiesto la totalidad de los expedientes acumulados, lo que determinó la denuncia ante la APD por parte de alguno de los interesados instando que por la misma se paralizase la tramitación administrativa que, a su juicio, lesionaba sus derechos fundamentales.

La Audiencia Nacional, en sendas resoluciones confirma la decisión de la APD de archivar las denuncias ante ella presentadas al considerar que no se produjo vulneración de los derechos fundamentales en la actuación de la Administración denunciada. La sentencia de 11 de mayo de 2001 señaló al respecto: "Pues bien, la resolución de la Agencia de Protección de Datos impugnada, al archivar las actuaciones iniciadas por los recurrentes en su escrito de 14 de marzo de 2000 –en el que se solicitaba que cesaran las actuaciones administrativas infractoras de los derechos fundamentales y se depuraran las responsabilidades derivadas de la infracción denunciada- y en la medida en que no atendió la expresa denuncia de los recurrentes, no ha vulnerado los derechos fundamentales que se alegan, por las razones que a continuación se exponen.

Esta tramitación conjunta del procedimiento de lesividad –en virtud del principio de eficacia en la actuación administrativa, reconocido en el artículo 103. 1 de la CE- y el reconocimiento de todos los reclamantes –terceros interesados en el procedimiento administrativo- acerca de los demás que se encuentran en su misma situación no supone vulneración alguna del derecho al honor, la intimidad personal, y a la protección de los datos, pues a falta de mayores precisiones en la demanda sobre la alegada lesión, debe señalarse que el derecho fundamental a la intimidad reconocido en el artículo 18. 1 de la CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (artículo 10. 1 CE), frente a la acción y conocimiento de los demás (STC 231/1988 y 115/2000), sean los poderes público o particulares. Por tanto, si este es el objeto de protección en el expresado derecho, el ámbito reservado de su vida dado a conocer en este caso aunque es íntimo, pues se refiere a su nombre, domicilio y al importe de una reclamación contra la Hacienda Pública, sin embargo tales extremos no han sido divulgados a terceras personas, sino a terceros interesados en el expediente administrativo, que siguieron similares reclamaciones (.. ´)

Por último, la protección de datos que se reconoce en el artículo 18. 4 de la CE, a la que se alude en la demanda bajo la invocación que se hace al uso de la informática, extiende su protección no a los datos íntimos de la persona –que se protegen en el derecho a la intimidad- sino a los datos de carácter personal (STC 292/2000), por tanto, la garantía de la vida privada de la persona y su reputación poseen una dimensión positiva que excede del ámbito del artículo 18. 1 CE y que se traduce en un derecho al control sobre los datos. Se pretende garantizar ahora a la persona mediante el control sobre sus datos personales, sobre su uso y destino con el propósito de impedir su tráfico ilícito y lesivo para la dignidad del afectado.

Esta "garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de información sin las debidas garantías" (STC 292/2000). De lo dicho se infiere que este derecho fundamental no resulta vulnerado en el caso debatido pues la Agencia de Protección de Datos al archivar la denuncia, como ya se ha adelantado, no ha vulnerado los derechos fundamentales invocados, toda vez que la Administración Tributaria no ha hecho un uso indebido de esos datos cuando procede a la acumulación de reclamaciones en un recurso de lesividad, y confiere un trámite de audiencia común a todos los interesados en el procedimiento seguido para la declaración de lesividad".

En igual sentido se había pronunciado dicha Sala de la Audiencia Nacional en sentencia de 20 de abril de 2001.

5. COMPARECENCIAS PARLAMENTARIAS

Dentro del marco de relaciones institucionales que caracterizan parte de la actividad de la Agencia de Protección de Datos, en el año 2001 el Director de la misma ha comparecido en tres ocasiones ante las Cortes Generales, al objeto de informar acerca de las diferentes cuestiones que constituyeron, en cada caso, el Orden del Día.

Del diverso contenido de cada una de ellas se infiere su diferente fin, por cuanto que, mientras la primera y la última se

produjeron ante la Comisión de la Sociedad de la Información y del Conocimiento del Senado, la segunda se mantuvo ante la Comisión Constitucional del Congreso de los Diputados.

1. SENADO

La primera de las comparecencias a que se ha hecho referencia tuvo lugar el 17 de abril de 2001, centrándose la intervención del Director de la Agencia en el análisis de cuatro grandes cuestiones, a saber: la labor llevada a cabo por la dicha Agencia de Protección de Datos para su incorporación a la Sociedad de la información, el examen de la legislación aplicable en materia de protección de datos al comercio electrónico, las actividades llevadas a cabo por la Agencia en relación con este tipo de comercio y, en fin, la inspección de oficio realizada recientemente por ésta en relación con las denominadas "tiendas virtuales".

El propio compareciente extrajo la conclusión de que, si bien resultan evidentes los avances conseguidos en cada una de las facetas objeto de estudio, son muy diversos aún los incumplimientos en materia de protección de datos, requiriendo del concurso de todos los agentes implicados, y en especial de las patronales y asociaciones profesionales, a los efectos de conseguir un cumplimiento más fiel de la normativa vigente, elaborándose las correspondientes recomendaciones y debiéndose llegar, en algunas ocasiones, a la apertura de expedientes sancionadores.

El examen de las actividades realizadas por la Agencia en relación con el comercio electrónico se refieren en el apartado de esta Memoria relativo a las actividades propias de la Subdirección General de Inspección de Datos, remitiéndonos en este punto al contenido de dicho capítulo, evitando así una innecesaria reiteración.

A continuación la Presidencia de la Comisión abrió un turno de preguntas en favor de los Grupos Parlamentarios quienes, en general, valoraron muy positivamente el trabajo desarrollado por la Agencia de Protección de Datos, si bien intentaron obtener del compareciente alguna puntualización en relación con la problemática planteada en su exposición.

Especial mención merece la duda expresada por los representantes de los partidos políticos en relación con la posible existencia de lagunas en la regulación de la materia relativa a Protección de Datos de carácter personal, máxime en consideración al surgimiento de nuevos problemas como los relativos al tránsito de "datos genéticos", la inseguridad en los pagos realizados a través de la red, la generación de archivos a partir de los cuales se pretende obtener las características de la personalidad de los individuos, y la elaboración de "listas únicas" de exclusión de los usuarios en evitación, entre otros tratamientos, del denominado "spam", esto es, la publicidad masiva no deseada.

Asimismo, se denunció por los Senadores interpelantes la publicación de datos completos de clientes de ciertos productos o empresas, vulnerándose su derecho a la protección de sus datos personales, sugiriendo al compareciente la adopción de medidas prácticas que favorezcan la seguridad de los usuarios frente a prácticas generalizadas, como la de la instalación de "cookies" sin autorización en los ordenadores de los usuarios.

De otra parte, se indagó la opinión del Director de la Agencia de Protección de Datos acerca de las medidas a adoptar a fin de que las empresas puedan realizar el legítimo comercio al que tienen derecho protegiendo, al tiempo, a los usuarios que no quieren figurar en lista alguna, así como acerca del grado de cumplimiento de la Sentencia 292/2000 del Tribunal Constitucional en lo relativo al intercambio de archivos entre Administraciones.

Puntualmente, se planteó la cuestión relativa a las "páginas blancas" de Telefónica, en la medida en que recopilan datos que, al combinarlos con un plano de direcciones, cambian sustancialmente la finalidad de aquél repertorio, por lo que, en ocasiones pudieran producirse efectos no deseados por desvío de su primitiva finalidad.

Los interpelantes hicieron especial hincapié en la existencia de archivos a través de los cuales se puede identificar a una persona y sus datos protegidos, no ya a partir de preguntas directas acerca de su ideología, religión o costumbres, sino a través de los pedidos que realizan en sus compras, demandándose algún tipo de solución en aras de preservar la intimidad de las personas afectadas por esta práctica.

En otro orden de cosas, se interpeló al Director de la Agencia de Protección de Datos acerca de la vigencia de las recomendaciones de 1997 sobre el uso de Internet, así como sobre el manejo de los monederos electrónicos, requiriéndose su opinión acerca del incremento de los usuarios de la red en España, y sobre si se realiza o no desde la Agencia algún seguimiento de las apuestas, juegos y sorteos a los que se accede a través de Internet.

En un segundo turno de intervenciones, se plantearon tres nuevas cuestiones, que la interpelante interpretó como carencias que pudieren justificar una reforma legal.

En primer lugar, la senadora interviniente planteó que, en tanto que la Unión Europea mandata que el usuario pueda dar un consentimiento expreso para el uso de sus datos personales, en la Ley de 1999 el consentimiento expreso se convierte en la negación expresa. En segundo lugar, denunció que, mientras los ficheros públicos no se pueden compartir entre administraciones, las compañías de seguros pueden intercambiar ficheros privados, y esa práctica de "cartera de clientes compartida" se está extendiendo a otro tipo de empresas.

Finalmente, se propuso la necesidad de modificar la cuantía de las multas incorporadas al procedimiento sancionador de la ley, persiguiendo los archivos ilegales y el tratamiento masivo de datos cuyo objeto es la busca de perfiles ("Data Mine" y "Data Warehouse").

En respuesta a las dudas expresadas por los Senadores, el Director de la Agencia de Protección de Datos abordó las cuestiones planteadas, pudiendo deducirse de su exposición las siguientes conclusiones.

2. LAGUNAS LEGISLATIVAS E INCUMPLIMIENTOS DE LA NORMATIVA VIGENTE

El Director de la Agencia expresó su idea de que nuestro país dispone de la legislación más garante de toda la Unión Europea en materia de protección de datos, siendo asimismo las actuaciones de la Agencia las que ofrecen mayores garantías dados los instrumentos legales que el legislador nacional le ha atribuido. Tanto es así que los países del este y centro de Europa han escogido nuestro sistema como modelo para adecuar su normativa y establecer su autoridad de control.

En cuanto al cumplimiento de la legislación por parte de las Administraciones Públicas, siguiendo el cauce de las denuncias de los ciudadanos, y por medio de planes sectoriales, se han elaborado las correspondientes "recomendaciones", inspeccionándose los ficheros de la Policía Nacional, de la Guardia Civil, de la Hacienda Pública y de diversas administraciones autonómicas y ayuntamientos.

En lo relativo al incumplimiento de la Ley 15/1999, de 13 de diciembre, por la publicación indiscriminada de datos, se dio cuenta de los expedientes abiertos a Terra y ADSL. De otra parte, la navegación "dejando rastro" aconseja el manejo de un programa y de un servidor seguros para evitar que los datos personales sean captados. Este mismo argumento resulta predicable respecto de las "cookies" que son detectables si se posee la suficiente experiencia.

En relación con los "datos genéticos", el Director de la Agencia compartió las inquietudes del interpelante, añadiendo que debería ponerse especial cuidado en su manejo. No obstante, la protección otorgada por el artículo 7 de la Ley Orgánica parece suficiente para proteger este tipo de datos. Lo que nunca puede permitirse, a juicio del compareciente, es que se produzca una discriminación de los ciudadanos precisamente por conocer sus datos genéticos.

En orden a la protección respecto de la publicidad masiva no deseada ("spam"), resulta recomendable la adopción del sistema de "lista única", susceptible de refundir las diversas listas que se hubieren creado, al objeto de que pueda ser gestionada por la propia Administración, de tal suerte que se facilite a todos el acceso, evitando el envío publicitario a las personas incluidas en dicha lista.

De otra parte, las recomendaciones sobre Internet redactadas por la Agencia en 1997 continúan plenamente vigentes, sin perjuicio de la incorporación de otras complementarias en orden a la información y mejor protección de los derechos de los ciudadanos.

En otro orden de cosas, cabe aseverar que las multas establecidas por el procedimiento sancionador de la ley 15/1999 de 13 de diciembre son, con diferencia, las más importantes de la Unión Europea. Cuando la Audiencia Nacional revisa las resoluciones de la Agencia de Protección de Datos suele rebajar el importe de las sanciones, por lo que, en este punto, no parece procedente la elevación de la cuantía de las mismas.

De todo lo anterior se deduce que la normativa vigente sobre protección de datos de carácter personal resulta adecuada y claramente suficiente, si bien deviene necesario un nuevo desarrollo reglamentario, toda vez que continúan vigentes los reglamentos aprobados con anterioridad a la entrada en vigor de la ley 15/1999 de 13 de diciembre.

3. EFECTOS PRÁCTICOS DE LA NAVEGACIÓN POR INTERNET Y SEGURIDAD EN LA RED

Subviniendo a las dudas expresadas por los senadores, el Director de la Agencia expresó su opinión de acuerdo con la cual, resulta esencial el conocimiento del medio para decidir libremente en orden a la protección de los datos personales. La mejor de las recomendaciones es la información. Para ello la Agencia ha publicado algunos consejos para navegar en Internet, desarrollando jornadas y seminarios sobre comercio electrónico, como las que tuvieron lugar en Mérida.

De otra parte, la incorporación de "datos de plano" y de "guía electrónica" a las Páginas Blancas de Telefónica ha de estudiarse a la luz de lo dispuesto en el artículo 50 de la Ley de Telecomunicaciones y el Real Decreto que desarrolla su reglamento, que establecen la posibilidad de decisión por parte del ciudadano, en el sentido de estar o no en una guía, estar parcialmente, excluirse de la misma, etcétera.

Este tema, tratado y debatido en el ámbito de la Agencia, tiene su base en que el callejero no es identificativo del edificio, por lo que se considera que, al ser una fuente accesible al público, sólo se debe incorporar en aquellos supuestos en que el ciudadano facilita su domicilio, y en este caso lo único que permite el plano es una mejor llegada al mismo, sin aportar ninguna identificación.

En lo relativo a la utilización de canales seguros para las transacciones económicas a través de Internet, lo aconsejable es la utilización exclusiva de programas y servidores seguros, con base en los Códigos Tipo elaborados por las empresas, exigiendo un grado de calidad en la protección de datos, lo que redundará, en fin, en beneficio de aquéllas compañías cuyo grado de seguridad resulte más conveniente.

En otro orden de cosas, la práctica relativa al cruce de datos para obtener, sin consentimiento del afectado, un perfil de su personalidad infringe claramente la Ley, por lo que contra ella sólo cabe la apertura de los correspondientes expedientes sancionadores.

En respuesta a la pregunta relativa a la validez y uso de los monederos electrónicos, el Director de la Agencia mostró su opinión claramente positiva, por cuanto, según expresó, son útiles y poseen la virtualidad de facilitar la adquisición de bienes y/o servicios de forma anónima.

Consentimiento del interesado en el tratamiento de sus datos

El compareciente expresó la idea de que la ley vigente es más garantista que la anterior LORTAD, que no hacía ninguna referencia al consentimiento, estableciendo el artículo 3. h) de la nueva Ley 15/1999 que el consentimiento es toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernan. Cuestión distinta, a juicio del Director de la Agencia, es el modo en que pueda prestarse dicho consentimiento, existiendo diversas posibilidades en función del tipo de datos. Así, como regla general, la Ley exige el consentimiento tácito, lo que no es óbice para que, en relación con supuestos de especial protección, se reclame el consentimiento expreso.

PONENCIA CONSTITUIDA EN EL SENO DE LA COMISIÓN DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO DEL SENADO

Constituida una Ponencia en el seno de la Comisión de la Sociedad de la Información y del Conocimiento del Senado, para el estudio de los derechos de los concursantes y audiencia en relación con concursos, juegos y apuestas, el Director de la Agencia fue convocado a comparecer ante la misma con fecha 27 de noviembre de 2001.

El Director informó sobre los expedientes sancionadores tramitados en relación con el tratamiento de datos en concursos y, tras responder a las dudas planteadas por los Senadores, suscitó la posibilidad de realizar una inspección de oficio para analizar el cumplimiento de la ley en el tratamiento de datos de concursantes y de la audiencia que participa en ellos. Dicha propuesta fue asumida por los miembros de la Ponencia.

CONGRESO DE LOS DIPUTADOS

La comparecencia, de fecha 7 de noviembre de 2001, ante la Comisión Constitucional del Congreso de los Diputados, tuvo por principal objeto la información sobre la memoria de la Agencia de Protección de Datos correspondiente al año 2000.

Como en anteriores ocasiones, el Director facilitó el control parlamentario de la actividad de la Agencia, en aras de garantizar su funcionamiento independiente. Uniéndose a esta inquietud, los grupos parlamentarios interpelaron al ponente en relación con dos importantes cuestiones que se incorporaron al Orden del Día, a saber: las medidas adoptadas por la Agencia para evitar la reiterada y escandalosa vulneración de la confidencialidad de datos de carácter personal de los ciudadanos por parte de las administraciones públicas y, en especial, por la Agencia Estatal de Administración Tributaria, y la circular de la Dirección General de la Policía que prevé la creación de archivos informáticos especiales sobre inmigrantes.

La primera parte de la comparecencia respetó la pauta expositiva de años anteriores, refiriéndose el Director, en primer lugar, al registro de protección de datos, para continuar con una especial referencia a las transferencias internacionales, la tramitación e inscripción de códigos tipo, actividades propias de la secretaría general de la Agencia, especialmente en lo relativo a la resolución de consultas, continuando con la exposición de las actuaciones de inspección e instructoras llevadas a cabo en 2000 y, en fin, entrando en el análisis de la actividad de la Agencia por sectores.

Sectorialmente, el compareciente diversificó la actividad de la Agencia de Protección de Datos distinguiendo, de una parte, los planes sectoriales de oficio, de otra parte, la actividad más relevante en el ámbito de ficheros de titularidad pública y, en último lugar, refiriendo la actuación más relevante de la Agencia en el ámbito de los ficheros de titularidad privada.

A continuación el Director de la Agencia se refirió a la actividad y seguimiento de otros sectores, como los relativos a la prestación de solvencia patrimonial y crédito (ficheros de morosos), al incumplimiento de la normativa por parte de ciertas entidades financieras, finalizando su exposición con un exhaustivo estudio de las actuaciones de la Agencia en el ámbito internacional.

A continuación la Presidencia de la Comisión abrió un turno de intervenciones a los Grupos Parlamentarios, quienes expusieron sus dudas e inquietudes en relación con una extensa variedad de temas, intentando obtener del compareciente la concreción de algún punto en relación con su exposición y expresando su opinión acerca de los temas tratados por el Director de la Agencia.

Buena parte de las cuestiones planteadas hicieron referencia a la aplicación práctica de la sentencia 292/2000 del Tribunal Constitucional, especialmente en cuanto a los errores detectados por la Agencia de Protección de Datos en relación con la norma que los sujetos cedentes suponían habilitante para la cesión de datos. Si bien es cierto que, en la mayoría de los casos, la cesión se realiza a favor de órganos administrativos con la misma competencia, o bien al amparo de una norma con rango de Ley, se plantea la cuestión de qué hacer en el resto de supuestos.

Asimismo, se evidenció la necesidad de desarrollar el nuevo reglamento de la ley, garantizando de forma muy especial el derecho de oposición.

Los interpelantes hicieron hincapié en que la normativa vigente no incluye a Internet como fuente de datos accesibles al

público, obligando a que exista un consentimiento inequívoco, específico e informado del afectado para realizar tratamientos con sus datos personales publicados en Internet. Asimismo, se refirieron al importante grado de discrecionalidad de la Agencia en relación con las transferencias internacionales de datos y a cómo, a partir del Tratado de Niza se produce una clara incorporación al derecho comunitario originario del derecho fundamental a la protección de los datos personales.

En concreto, se interrogó con insistencia acerca del desarrollo del censo promocional, sugiriéndose por los diferentes interpelantes su definitiva implantación y uso.

De otra parte, los Diputados intervinientes se interesaron por el grado de cumplimiento del reglamento de medidas de seguridad en Internet, así como por la temática atinente al mantenimiento en fichero del denominado "saldo cero" por parte de las entidades de prestación de servicios de información sobre la solvencia patrimonial y el crédito.

Finalmente, se solicitó del compareciente alguna ampliación en relación con la información ofrecida sobre las inspecciones realizadas en relación con los operadores de telefonía móvil, tratamiento y cesión de datos sanitarios, y aplicación de los principios de puerto seguro en las actuaciones de ámbito internacional.

El resto de la comparecencia sirvió para plantear y dar respuesta a dos importantes cuestiones presentadas por los grupos parlamentarios. De una parte, se denunció la cesión indebida entre administraciones de datos personales, relativos al ámbito de la Seguridad Social, Asuntos Exteriores, Ministerio de Defensa y, especialmente, los referidos a la Agencia Tributaria, invocándose la existencia de un insuficiente nivel de protección en todos estos supuestos y, de otra parte, se cuestionó la licitud de la creación, por parte de la Dirección General de la Policía, de archivos informáticos especiales sobre inmigrantes, referidos especialmente a la actividad delictiva perpetrada por nacionales colombianos y ecuatorianos con vulneración, a juicio del interpelante, de la Ley de Protección de Datos, invadiendo dichas actuaciones la intimidad personal y los derechos de los extranjeros.

El Director de la Agencia de Protección de Datos abordó las cuestiones planteadas, pudiendo deducirse de su exposición la siguiente serie de conclusiones.

Cumplimiento de la normativa vigente por parte de las administraciones públicas

La Agencia de Protección de Datos tiene planes para atajar los problemas que puedan producirse en caso de incumplimiento de la normativa vigente por parte de las administraciones públicas.

En lo relativo a la cesión indebida de datos entre dichas administraciones, la Agencia de Protección de Datos ha desarrollado actividades de carácter preventivo y represivo, articuladas respectivamente a través de la promoción de foros y seminarios, y mediante la incoación de los correspondientes expedientes sancionadores.

A consecuencia de esta actividad informativa, cuyo paradigma es la emisión de recomendaciones, se ha multiplicado la inscripción de ficheros, al tiempo que se han adaptado los ya existentes a las exigencias de la sentencia 292/2000 del Tribunal Constitucional, realizándose inspecciones de oficio a la Agencia Estatal de la Administración Tributaria, y a la Dirección General de Tráfico, entre otros.

En relación con la Agencia Tributaria, se detectaron ciertas disfunciones para cuya corrección se dictaron las oportunas recomendaciones, lo cual no fue óbice para su sanción en supuestos puntuales y concretos.

Transferencias internacionales de datos

En cuanto a las transferencias internacionales de datos, la Agencia ha dictado la instrucción 1/2000 con la intención de adecuar el sistema, sobre todo recopilando la regulación que las diversas situaciones propician para la protección de datos en el supuesto de transferencias, y con ello facilitar a los que deben cumplir la ley qué es lo que deben hacer.

De otra parte, los principios sobre puerto seguro resultan preocupantes habida cuenta que, en definitiva, habilitan la transmisión de datos a un país como Estados Unidos, que no tiene una legislación de protección de datos a nivel de todo el Estado, sino sólo sectorial.

Ello no obstante, en lo que respecta a nuestro país, se han solicitado transferencias internacionales de datos, no invocando el puerto seguro, sino a través del sistema de garantías contractuales al que se ha hecho referencia en otras comparecencias.

Censo promocional

El desarrollo del censo promocional será positivo, e incidirá en beneficio de los derechos individuales por cuanto que, de una parte, se posibilitará que las empresas ejerzan lícitamente el comercio, sin interferir en el derecho de los ciudadanos y, de otra parte, se facilitará la posibilidad de darse de baja o de alta en dicho censo.

Internet y comercio electrónico

El Director de la Agencia comparte la opinión de que Internet no es una fuente accesible al público, por cuanto la ley tasa con claridad las que han de tener dicha consideración, no incluyendo a la red entre ellas.

En relación con los datos sanitarios, las recomendaciones en general se han cumplido, no existiendo denuncias al respecto por parte de los ciudadanos. Idénticas consideraciones cabe inferir respecto a los "datos genéticos", que se entienden suficientemente protegidos a la luz de la normativa vigente.

Saldo cero en ficheros de morosos

La imposibilidad de mantener un fichero con saldo cero se deriva de la aplicación de la legislación vigente, en concreto de lo dispuesto en el artículo 29 de la ley 15/1999. Los ficheros de morosos son un elemento importante para mantener un sector financiero saneado, pero existen razones de peso para considerar que el saldo cero ya no es posible en un registro de morosos. Sobre todo apoyándonos en la nueva legalidad, en estos momentos la Agencia está considerando que mantener el saldo cero respecto de quien ha pagado ya una deuda no resulta posible.

Circular de la Dirección General de la Policía que prevé la creación de archivos informáticos especiales sobre inmigrantes

Del análisis de dicha circular de la Policía se deduce que se trata de ficheros de las Fuerzas y Cuerpos de Seguridad o policiales a los que, conforme a lo dispuesto en el artículo 22.3 de la Ley de Protección de Datos, les resulta de aplicación el régimen de protección que dicha ley establece.

En todo caso, a juicio de la Agencia de Protección de Datos, la posible infracción de la Ley no estaría tanto en la elaboración de la Circular, sino en la ejecución práctica de la misma, por lo que el Director asumió el compromiso de realizar una inspección de oficio al respecto.

MEMORIA DE 2001 - ASPECTOS INTERNACIONALES DE LA PROTECCIÓN DE DATOS. ANÁLISIS DE LAS TENDENCIAS LEGISLATIVAS, JURISPRUDENCIALES Y DOCTRINALES.

1. UNIÓN EUROPEA. GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES CREADO POR EL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE1

La Directiva 95/46/CE2 en su artículo 29 creó el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, comúnmente denominado Grupo del Artículo 29, con carácter consultivo e independiente. Se compone de un representante de la Autoridad o Autoridades de Control designadas por cada Estado miembro, por un representante de la Autoridad o Autoridades creadas por las instituciones y organismos comunitarios3 así como por un representante de la Comisión. Cada miembro del Grupo es designado por la Autoridad a la que representa. Si un Estado miembro designa a varias Autoridades de Control, éstas nombrarán a un representante común.

A las reuniones del Grupo de Trabajo pueden acudir, como observadores, representantes de las Autoridades de Control de los países que forman parte del Espacio Económico Europeo –Noruega, Islandia y Liechtenstein- así como representantes4 de las Autoridades de Control de los 13 países candidatos a formar parte de la Unión Europea: Bulgaria, Chipre, República Checa, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, Rumania, República Eslovaca, Eslovenia y Turquía.

El Grupo de Trabajo se reunió por primera vez en febrero de 1997 y ha mantenido un total de 31 reuniones –la última tuvo lugar el 13 de diciembre de 2001-, habiendo aprobado hasta dicha fecha un total de 53 documentos, en forma de Decisiones, Dictámenes, Documentos de Trabajo, Informes o Recomendaciones. La Agencia de Protección de Datos española interviene activamente en las reuniones del Grupo así como en los encuentros y foros preparatorios de las mismas.

En el presente año, la Agencia de Protección de Datos, además de participar en las cinco reuniones del plenario, también formó parte de los subgrupos creados al objeto de preparar distintos documentos en el ámbito de los datos laborales y las cláusulas contractuales tipo para la transferencia internacional de datos personales. Estos subgrupos se reunieron en tres ocasiones cada uno.

La Directiva atribuye al Grupo las siguientes funciones:

* Analizar cualquier tema relativo a la aplicación de las disposiciones nacionales que incorporan a derecho interno el contenido de la Directiva 95/46/CE, con objeto de posibilitar y contribuir a una interpretación y puesta en práctica uniforme y homogénea en el territorio de la Unión.
* Emitir dictámenes destinados a la Comisión sobre el nivel de protección existente dentro de la Unión y en los países terceros.
* Asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva 95/46/CE o cualquier proyecto que afecte a los derechos y libertades de las personas físicas en lo que respecta al tratamiento de sus datos personales.
* Emanación de dictámenes sobre códigos de conducta.
* Elaborar, formular y aprobar recomendaciones, documentos de trabajo, y dictámenes sobre cualquier asunto relacionado con la protección de las personas en lo relativo al tratamiento de datos personales. Tales documentos se transmiten a la Comisión y al Comité del Artículo 315 de la Directiva. A su vez, la Comisión informa al Grupo del Artículo 29 acerca del trámite y curso que se da a sus documentos.
* Elaborar informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en los distintos países.

En el transcurso del año 2001 el Grupo de Trabajo ha aprobado los documentos relacionados a continuación:

* Dictamen 1/2001 sobre el Borrador de Decisión de la Comisión de cláusulas contractuales para la transferencia de Datos Personales a terceros países, de conformidad con el artículo 26 (4) de la Directiva 95/46/CE, aprobado el 26 de enero de 2001.
* Dictamen 2/2001 sobre el nivel adecuado de protección de la ley canadiense *Personal Information and Electronic Documents Act*, aprobado el 26 de enero de 2001.
* Dictamen 3/2001 sobre el nivel de protección que proporciona la Ley australiana de 2000, aplicable al sector privado, sobre protección de la vida privada, aprobado el 26 de enero de 2001.
* Dictamen 4/2001 acerca del proyecto de Convenio del Consejo de Europa sobre el ciberdelito, aprobado el 22 de marzo de 2001.
* Recomendación 1/2001 sobre datos de evaluación de los empleados, aprobado el 22 de marzo de 2001.
* Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, aprobada el 17 de mayo de 2001.
* Dictamen 5/2001 sobre el Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo a raíz del proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, aprobado el 17 de mayo de 2001.
* Cuarto Informe Anual, correspondiente al año 1999, sobre la situación relativa a la protección de las personas físicas en relación con el tratamiento de datos personales en la Unión Europea y en terceros países.
* Dictamen 7/2001 sobre el Borrador de Decisión de la Comisión sobre cláusulas contractuales para la transferencia de datos personales a encargados de tratamiento establecidos en terceros países, de conformidad con el artículo 26 (4) de la Directiva 95/46/CE, aprobada el 13 de septiembre de 2001.

* Dictamen 8/2001 sobre tratamiento de datos personales en el contexto laboral, aprobada el 13 de septiembre de 2001.
* Documento de trabajo relativo a la Práctica recomendada IATA 1774 "Protección de la vida privada y los flujos transfronterizos de los datos personales utilizados en el transporte aéreo internacional de pasajeros y mercancías", aprobado el 13 de septiembre de 2001.
* Dictamen 9/2001 sobre la Comunicación de la Comisión relativa a la "Creación de una sociedad de información segura a través de la mejora de la seguridad de las infraestructuras de la información así como a través de la lucha contra el delito informático", aprobado el 5 de noviembre de 2001.
* Decisión 1/2001 relativa a la participación de representantes de las Autoridades de Control de la Protección de Datos de los países candidatos en las reuniones del Grupo de Trabajo del Artículo 29, aprobada el 13 de diciembre de 2001.
* Dictamen 10/2001, relativo a la necesidad de un criterio adecuado en la lucha contra el terrorismo, aprobado el 14 de diciembre de 2001.

Así mismo, en materia de transferencias internacionales deben tenerse en cuenta las Decisiones de la Comisión de las Comunidades Europeas, números 2001/497/CE y 2002/16/CE, de 15 de junio y 27 de diciembre, publicadas en el Diario Oficial de las Comunidades Europeas L 181/19 de 4 de julio y DOCE L 6/52 de 10 de enero de 2002 respectivamente. La primera aprueba las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE y la segunda aprueba las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. En este punto debe recordarse que el Grupo del Artículo 29, tal y como se ha mencionado con anterioridad, procedió en el año 2001 a analizar y emitir su criterio en relación con los entonces Borradores de Decisión de la Comisión en relación con dicha materia.

Además, el Diario Oficial de las Comunidades Europeas ha publicado el pasado 4 de enero en la serie L 2/13 la Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act*, respecto a lo que el Grupo de Trabajo del Artículo 29 también se pronunció en su día, tal como se refleja en la lista de documentos aprobados en el transcurso de 2001.

Hay que destacar así mismo la activa participación desarrollada por parte de la Agencia de Protección de Datos española en los Subgrupos de Trabajo cuya creación se acordó en el seno del Plenario del Grupo del Artículo 29 dirigidos a preparar los dos Dictámenes en materia de cláusulas contractuales tipo así como a elaborar el Dictamen referido al tratamiento de datos en el contexto laboral. Este Subgrupo continuará sus trabajos en el transcurso de 2002.

1.1. Análisis de la existencia de un nivel adecuado de protección en terceros Estados.

Los criterios y requisitos que el Grupo de Trabajo estima necesarios con el fin de analizar, apreciar y determinar acerca de la existencia de un nivel de protección de datos adecuado en terceros Estados, no miembros de la Unión Europea, se contienen en el Documento de Trabajo sobre Transferencias de datos personales a terceros países y aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998 -WP 12-.

Los objetivos de un sistema de protección de datos son básicamente:

* Asegurar un nivel satisfactorio de cumplimiento de las normas.
* Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos.
* Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

En el transcurso del pasado año, el Grupo de Trabajo se ha pronunciado en relación con el nivel de protección otorgado por las leyes de protección de datos australiana y canadiense respectivamente. En relación con Canadá ha recomendado a la Comisión y al Comité del Artículo 31 de la Directiva, a la luz de la normativa canadiense, que cualquier resolución sobre la idoneidad del nivel de protección de la ley canadiense -*Personal Information and Electronic Documents Act*-, refleje sus limitaciones en cuanto a su ámbito y calendario de aplicación, ya que dicha Ley sólo se aplica a organismos privados que recogen, utilizan o divulgan datos personales en sus actividades comerciales. El 20 de diciembre de 2001 se ha publicado en el DOCE, tal y como se ha mencionado con anterioridad.

El Grupo también se ha pronunciado en relación con la solicitud de Australia para que se la declarase país con un nivel de protección adecuado. Para ello analizó la Ley australiana de 2000, aplicable al sector privado, sobre protección de la vida privada. El Grupo entiende que aún existen algunos puntos en los que se estima debería producirse una mayor y mejor adecuación del nivel de protección otorgado por dicha normativa, por lo que se manifiesta abierto a colaborar con la Comisión, a seguir de cerca el proceso y a estudiar e informar nuevamente el caso en cuanto se produzca cualquier avance o cambio.

1.2. Tratamiento de datos personales en el ámbito laboral

En el transcurso del pasado año, el tratamiento de datos personales en el ámbito laboral ocupó, y sigue ocupando en la actualidad, una parte importante de la actividad del Grupo, en cuyo seno se constituyó un Subgrupo de trabajo que se ha reunido en varias ocasiones y al que le fue encomendado el estudio, elaboración y propuesta de documentos en relación con la protección de datos en el entorno laboral.

El mayor obstáculo al que se ha enfrentado el Subgrupo ha sido el de la diferencias existentes entre la normativa y prácticas nacionales de los distintos Estados miembros, además de la falta de legislación adecuada sobre la materia,

como ocurre frecuentemente en el ámbito de las nuevas tecnologías, en este caso en lo relativo a la utilización de comunicaciones electrónicas en el lugar de trabajo. Y aunque la principal norma a nivel comunitario, la Directiva 95/46/CE no aborde específicamente la vigilancia o la protección de los datos de empleo, sí que es de aplicación en dicho ámbito.

El Grupo de Trabajo del Artículo 29 ha aprobado dos documentos a este respecto en el transcurso del pasado año. El primero directamente relacionado con el tratamiento de datos personales en el ámbito laboral, como su propio título indica –Dictamen 8/2001, anteriormente enunciado-, y el segundo referido a los datos de evaluación de los empleados –Recomendación 1/2001-. referido también al entorno laboral.

La Recomendación 1/2001 es un breve documento encaminado a señalar explícitamente que la definición de datos personales engloba cualquier dato personal, tanto de carácter objetivo como subjetivo, es decir, cualquier elemento o circunstancia que contenga información personal de un determinado individuo y que, por ello, los datos sobre evaluaciones subjetivas de los trabajadores incluidos en los ficheros de las empresas, están sujetos a las leyes nacionales de protección de datos y, en concreto, al ejercicio del derechos de acceso.

Por su parte, el Dictamen 8/2001 determina que la utilización de las comunicaciones electrónicas en el lugar de trabajo, tal y como se ha mencionado anteriormente, recae en el ámbito de aplicación de la Directiva 95/46/CE. Realiza un estudio y aplicación de los principios básicos de la protección de datos al ámbito del empleo, ya que muchas actividades realizadas en el entorno laboral implican tratamiento de datos de los trabajadores. El Dictamen repasa por lo tanto los principios de finalidad, consentimiento, transparencia, legitimidad, proporcionalidad, actualización y conservación de los datos, seguridad de los sistemas, régimen de las transferencias internacionales de datos de los trabajadores, formación e información del/al personal empleado, así como su interacción con el ejercicio de las potestades de control y dirección empresarial atribuidas legalmente y con el ejercicio de los derechos y deberes de los trabajadores así como la participación de los mismos a través de sus representantes, de conformidad con la regulación laboral en vigor. El Dictamen estudia, desde el punto de vista de protección de datos, los intereses, potestades, deberes y derechos de los trabajadores y los empresarios.

En dicho documento se reitera la obligatoriedad de que los datos laborales sean tratado teniendo siempre en cuenta los principios esenciales de protección de datos:

* Finalidad. Los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.
* Transparencia. Como mínimo, los trabajadores deben saber qué datos recoge el empresario sobre ellos (directamente o de otras fuentes) y cuáles son los fines de las operaciones de tratamiento previstas o realizadas con estos datos en la actualidad o en el futuro. La transparencia también puede garantizarse otorgando al interesado el derecho de acceso a los datos personales que le afectan y obligando al responsable del tratamiento a notificar a las autoridades supervisoras según lo previsto en la legislación nacional.
* Legitimidad. El tratamiento de los datos personales de los trabajadores deberá ser legítimo. El artículo 7 de la Directiva enumera los principios relativos a la legitimación del tratamiento de datos.
* Proporcionalidad. Los datos personales deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. Suponiendo que se ha informado a los trabajadores sobre el tratamiento y que dicho tratamiento es legítimo y proporcionado, este tratamiento también deberá ser leal con el trabajador.
* Exactitud y conservación de los datos. Los registros profesionales deberán ser exactos y, cuando sea necesario, actualizados. El empresario deberá tomar 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.
* Seguridad. El empresario deberá implantar medidas adecuadas de carácter técnico y organizativo en el lugar de trabajo para garantizar la seguridad de los datos personales de sus trabajadores. Deberá preverse una protección especial en lo que respecta al acceso o difusión no autorizados.
* Formación del personal. El personal encargado del tratamiento de datos personales de otros trabajadores o con responsabilidades en este ámbito deberá tener conocimientos sobre protección de datos y recibir una formación adecuada. Si el personal encargado del tratamiento de datos personales no recibe una formación adecuada, no podrá garantizarse el respeto de la vida privada de los trabajadores en el lugar de trabajo
* Consentimiento. El Grupo de Trabajo del Artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.
* Interesados. Los trabajadores son afectados o interesados que se benefician de los derechos que confiere la Directiva sobre protección de datos. El más importante de estos derechos es el derecho de acceso, previsto en el artículo 12 de la Directiva.
* Interacción entre legislación laboral y legislación sobre protección de datos. El Grupo de Trabajo señala que la legislación sobre protección de datos no se aplica de forma independiente del Derecho del trabajo y las prácticas laborales y que éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debería contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.
* Vigilancia y control. Los requisitos de protección de datos se aplican a la vigilancia y control de los trabajadores tanto en términos de utilización de correo electrónico, acceso a Internet, cámaras de vídeo o datos de localización. Cualquier control deberá ser una respuesta proporcionada del empresario ante los riesgos potenciales, teniendo en cuenta el

derecho a la vida privada y otros intereses de los trabajadores. Cualquier dato personal que se posea o se utilice a efectos de control deberá ser adecuado, pertinente y no excesivo respecto a los fines que justifiquen dicho control.
* Transferencia de datos de los trabajadores a terceros países. El artículo 25 de la Directiva establece que las transferencias de datos personales a un tercer país, fuera de la Unión Europea, sólo podrán efectuarse si este país garantiza un nivel de protección adecuado. Cabe recordar que, cualquiera que sea la base de la transferencia en el marco de los artículos 25 y 26, el tratamiento que se efectúe en la transferencia deberá satisfacer siempre lo dispuesto en los artículos 6 a 8 y en las demás disposiciones de la Directiva.

1.3. La protección de datos y el cibercrimen.

Otro asunto importante y de gran interés que ha ocupado la labor del Grupo de Trabajo del Artículo 29 durante el pasado año ha sido el cibercrimen o ciberdelito y su incidencia y relación con la protección de datos, al ser una materia de gran trascendencia, sensibilidad y muy novedosa.

Las nuevas tecnologías, junto con las evidentes ventajas y avances que han aportado a la sociedad actual, han creado nuevas situaciones, hasta ahora inexistentes y por tanto desconocidas, tales como la posibilidad de comisión de infracciones penales nuevas o de delitos tradicionales a través de nuevas vías, disponibles tras la aparición de tales técnicas.

A finales del pasado año el Consejo de Europa abordó esta materia a través del Convenio del Consejo de Europa sobre el ciberdelito. El Grupo de Trabajo del Artículo 29 estudió los proyectos presentados por el Consejo con objeto de dar su visión al respecto.

En su Dictamen 4/2001 acerca del proyecto de Convenio del Consejo de Europa sobre el ciberdelito, el Grupo recomendaba de forma contundente la importancia de que el Convenio tuviera en cuenta los preceptos en materia de protección de datos con inclusión de una serie de preceptos referidos a los principios de necesidad, procedencia y proporcionalidad. El Grupo ha apoyado y continúa apoyando los esfuerzos dirigidos a la lucha contra el ciberdelito, ya que ello contribuye a mejorar el nivel de seguridad de los ciudadanos, y señala la importancia de equilibrarlo con la protección de los derechos fundamentales de la persona a la vida privada y a la protección de sus datos personales.

En concreto, el Grupo de Trabajo concluía destacando la importante función que el Consejo de Europa desempeñaba desde hace décadas como eficaz guardián de los derechos y libertades fundamentales y opinaba que ésta institución, al fomentar la cooperación internacional en materia de ciberdelito más allá de sus propios miembros, tenía que prestar especial atención a la protección de los derechos y libertades fundamentales y, señaladamente, del derecho a la protección de la vida privada y los datos personales.

El Grupo consideraba, pues, que era necesario aclarar el texto de los artículos del Proyecto de Convenio porque su redacción resultaba con frecuencia demasiado vaga y confusa, y podría no constituir fundamento suficiente para las leyes y medidas vinculantes destinadas a limitar legalmente los derechos y libertades fundamentales. Las explicaciones de la Exposición de Motivos no pueden suplantar la claridad jurídica del propio texto.

También señalaba que la mayor parte de los preceptos del Proyecto de Convenio tienen una repercusión enorme sobre los derechos fundamentales de la persona a la vida privada y la protección de los datos personales. De hecho, hasta cierto punto, anticipan el resultado del examen que es necesario efectuar si el derecho fundamental a la vida privada (artículo 8 del Convenio Europeo de Derechos Humanos6) y otros van a ser objeto de limitaciones. Uno de los problemas básicos al respecto es determinar cuándo es necesaria una medida en un caso concreto y, si lo es, cuándo es procedente, proporcionada y no excesiva. Algunos de los elementos del Proyecto de Convenio son completamente nuevos y su repercusión en los derechos fundamentales, especialmente en el derecho fundamental a la protección de los datos personales, podría no haberse evaluado de manera suficiente por la Comisión de Expertos en infracciones penales en el ciberespacio (PC-CY).

El Grupo de trabajo consideraba que era preciso mejorar la justificación de las medidas previstas desde el punto de vista de la necesidad, la procedencia y la proporcionalidad tal como exigen los instrumentos citados anteriormente en materia de derechos humanos y protección de datos.

El Grupo de Trabajo recomendaba enérgicamente que el proyecto de convenio incorporara preceptos en materia de protección de datos, que esbocen la protección que debe proporcionarse a los sujetos de la información susceptible de tratamiento en relación con las medidas contempladas en el proyecto de convenio. La inclusión de estos preceptos ayudaría a codificar y aclarar los requisitos de necesidad, procedencia y proporcionalidad que exige el acervo del Consejo de Europa y los Estados miembros de la UE.

El Grupo de Trabajo opinaba, además, que debía incluirse en el preámbulo la referencia al Convenio 108, aunque no tenga carácter vinculante, así como invitarse a los signatarios del Convenio sobre el ciberdelito a firmar el Convenio 108 sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Grupo de Trabajo manifestaba además que los signatarios del Convenio debían aceptar la debida responsabilidad de proteger adecuadamente los derechos fundamentales de las personas afectadas, desde el momento que los datos sobre ellas procedan de los Estados miembros de la Unión Europea y el Consejo de Europa y que de ninguna manera debía suprimirse la posición propuesta en el Proyecto estudiado de Convenio (versión pública 25) de no imponer a los signatarios la obligación de apremiar a los proveedores de servicios la retención de los datos de tráfico de todas las comunicaciones.

En relación con esta misma materia, el 5 de noviembre del pasado año, el Grupo de Trabajo aprobó la Opinión 9/2001, sobre la Comunicación de la Comisión de 26 de enero de 2001 al Consejo y al Parlamento Europeo titulada "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" En dicha Opinión, el Grupo de Trabajo manifiesta la oportunidad de tal Comunicación de la Comisión, y señala que cualquier medida llevada a término con la finalidad de combatir el cibercrimen deberá respetar los derechos y libertades fundamentales, incluyendo el derecho a la intimidad y a la protección de datos, por lo que cualquier restricción o limitación que se efectúe sobre los derechos fundamentales deberá ser justificada. En ningún caso debería admitirse la realización de cualquier tipo de vigilancia a los ciudadanos, sin proceder a la utilización de estrategias alternativas, bajo el pretexto de la lucha contra el cibercrimen.

El Grupo de Trabajo finalizaba su Dictamen destacando el carácter equilibrado de la Comunicación de la Comisión y recomendando la mayor vigilancia para que el conjunto de medidas concretas destinadas a luchar contra la delincuencia informática integre los imperativos de protección de los derechos y libertades fundamentales y, concretamente, los derechos a la protección de los datos y a la intimidad.

Asimismo, insistía en la necesidad de mantener un debate público y transparente que diera comienzo lo más rápidamente posible en el que intervinieran todas las partes interesadas y, en particular, expertos en protección de datos y sugería a la Comisión que evaluara si es verdaderamente oportuno inspirarse en los trabajos que se han llevado a cabo en el Consejo de Europa y que han culminado en el proyecto de Convenio sobre delincuencia en el ciberespacio.

1.4. Recogida de datos personales a través de Internet

El 17 de mayo del pasado año, el Grupo de Trabajo aprobó la Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales de la Unión Europea. Dicha Recomendación se basa en dos documentos, también del Grupo de Trabajo, a saber: "Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea", de 21 de noviembre de 2001, así como "Dictamen 4/2000, de 16 de mayo de 2000, sobre el nivel de protección que proporcionan los Principios de Puerto Seguro".

El objetivo de la Recomendación 2/2001 es el de contribuir a la aplicación eficaz y homogénea de las disposiciones nacionales adoptadas de conformidad con las Directivas de protección de datos personales7, aportando indicaciones concretas sobre la materia en que deberían aplicarse las normas establecidas en las Directivas a las tareas de tratamiento más habituales llevadas a cabo a través de Internet. Tal tratamiento se produce, especialmente, durante el primer contacto entre un usuario de Internet y un sitio web, ya sea únicamente para buscar información o bien para concluir una transacción comercial. El documento ofrece indicaciones referidas a la recogida de datos personales en una página web con el fin de que los agentes participantes apliquen las medidas apropiadas para garantizar la licitud y legalidad del tratamiento. Se trataría de aportar un valor añadido para la puesta en práctica de los principios establecidos en la Directiva. Constituye una iniciativa para detallar, a escala europea, un conjunto mínimo de obligaciones que puedan seguirse por parte de los sitios web operativos que sean responsables de tratamientos, que, en todo caso, deberán cumplir sus legislaciones y normativas nacionales.

La Recomendación es de aplicación si el responsable del tratamiento está establecido en un Estado miembro de la Unión Europea. En este caso, la legislación nacional del Estado miembro en cuestión será de aplicación para el tratamiento de datos personales en el marco de las actividades de dicho establecimiento. La Recomendación también se aplicará cuando el responsable del tratamiento no esté establecido en territorio comunitario pero, para fines de tratamiento de datos personales, recurra a medios, automatizados o no, situados en el territorio de uno de los Estados miembros de la UE. Este tratamiento quedará cubierto por la legislación nacional del Estados miembro donde estén situadas dichas instalaciones o medios técnicos8.

Es preciso distinguir claramente este caso de la cuestión de si los datos personales se pueden transferir legítimamente desde la UE hasta un tercer país, que se aborda en los artículos 25 y 26 de la Directiva 95/46/CE, y de las decisiones correspondientes de la Comisión Europea sobre la adecuación del nivel de protección de un tercer país. Por ejemplo, si un sitio web estadounidense utiliza medios dentro de la UE para recoger y tratar datos personales, la legislación del país europeo en cuestión será aplicable a dicha recogida, así como a las operaciones de tratamiento, independientemente de si se considera o no que esta entidad ofrece un nivel de protección adecuado de conformidad con la decisión de la Comisión Europea relativa al Puerto Seguro. El hecho de que el destinatario de los datos se haya adherido al Puerto Seguro solamente será relevante para la legalidad de la transferencia ulterior a dicha entidad de datos personales por parte de una entidad establecida en la UE.

La recomendación se dirigía en particular:

* A los responsables del tratamiento que recogen datos en línea, a los que se facilita una guía práctica que enumera un conjunto mínimo de medidas concretas que deberán aplicar.

* A los usuarios individuales de Internet para que se estén informados sobre sus derechos y puedan ejercerlos.

* A los organismos que deseen conceder etiquetas que certifiquen la adecuación de los procedimientos de tratamiento utilizados con las Directivas europeas sobre protección de datos, proporcionándoles criterios de referencia para conceder dichas etiquetas en relación con la información que deben proporcionar y la recogida de datos personales. Por supuesto, a la hora de conceder etiquetas, además de estos criterios de referencia, deberán tenerse en cuenta necesariamente otros criterios relativos a distintas obligaciones y derechos. El Grupo de Trabajo elaborará más adelante un documento completo sobre este asunto.

* A las autoridades europeas de protección de datos, para facilitarles un marco de referencia común para su tarea de verificar el cumplimiento de las disposiciones nacionales adoptadas por los Estados miembros de conformidad con las Directivas antes mencionadas.

Además, el Grupo opinaba que debería servir como referencia cuando se desarrollaran nuevas normas para *software* y *hardware* destinados a la recogida y tratamiento de datos en Internet.

La Recomendación hacía especial hincapié sobre los aspectos relativos a qué información y en qué momentos se debe proporcionar la misma al afectado y cómo debe facilitarse la misma. A este respecto consideraba necesario que el responsable del tratamiento:

* declarare la identidad y las direcciones postal y electrónica del responsable y, en su caso, la del representante designado en virtud del apartado 2 del artículo 4 de la Directiva
* indique claramente para qué fines de tratamiento se recogen los datos
* informe si la información solicitada es opcional u obligatoria
* mencione la existencia de los derechos de consentimiento u oposición, según el caso, respecto al tratamiento de datos personales y las condiciones para ejercerlos así como los derechos de acceso, rectificación y eliminación de datos así como la persona o el servicio al que acudir para ejercer estos derechos y, en segundo lugar, sobre la posibilidad de ejercerlos tanto en línea como en la dirección postal del responsable del tratamiento
* enumere los destinatarios o las categorías de destinatarios de la información recopilada
* si se prevé que el responsable de los datos transfiera dichos datos a países no miembros de la Unión Europea, indique si estos países ofrecen una adecuada protección en cuanto al tratamiento de sus datos personales
* proporcione el nombre y la dirección (postal y electrónica) del servicio o la persona responsable de responder a las preguntas relacionadas con la protección de los datos personales
* mencione con claridad la existencia de procedimientos automáticos de recogida de datos, antes de usar dichos métodos
* destaque las medidas de seguridad que garantizan la autenticidad del sitio, la integridad y la confidencialidad de la información transmitida a través de la red y que se hayan tomado en aplicación de la legislación nacional en vigor
* proporcione la información en todos los idiomas utilizados en el sitio y, en particular, en los lugares donde vayan a recogerse datos personales.

Además, respecto de cómo debe suministrarse esta información el Grupo de Trabajo consideraba que el núcleo fundamental de la misma debe mostrarse directamente en la pantalla antes de la recogida para garantizar el tratamiento leal de los datos. Adicionalmente, en el caso de los métodos automáticos de recogida de datos, esta información podría facilitarse mediante la técnica de una ventana «emergente».

Asimismo, el Grupo de Trabajo consideraba que en la página inicial del sitio y en todos los lugares donde se recojan datos personales en línea, debería poderse acceder directamente a información completa sobre la política de protección de la intimidad (incluida la forma de ejercer el derecho de acceso). El título del encabezado que debería seleccionarse con el ratón debería estar resaltado, ser explícito y específico, de manera que transmita al usuario de Internet una idea clara del contenido que se le va a mostrar.

Por otra parte, se realizaban una sería de recomendaciones en relación con la aplicación de otros derechos y obligaciones, en particular sobre los principios de minimización en la recogida de datos, el tratamiento legítimo de los mismos, la garantía efectiva del ejercicio de los derechos, la promoción de la consulta anónima de los sitios comerciales y la admisión de la posibilidad del uso de seudónimos, la definición de un periodo de almacenamiento de los datos recogidos, la satisfacción de las garantías establecidas en el artículo 17 de la Directiva 95/46/CE a la hora de encargar un tratamiento a un tercero, la notificación del tratamiento a la Autoridad de Control si la legislación aplicable así lo exige, la diligencia necesaria en relación con las transferencias de datos personales a terceros países y la recopilación de direcciones con fines de publicidad directa por correo electrónico y el envío de boletines de información.

1.5. Códigos de conducta

El artículo 27 de la Directiva 95/46/CE señala que tanto los Estados miembros como la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, de acuerdo con las especialidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros.

Los proyectos de código comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes podrán ser sometidos a examen del Grupo de Trabajo del Artículo 29, que puede pronunciarse sobre la conformidad de los proyectos que le sean sometidos así como recoger las observaciones de los interesados o de sus representantes.

Por tanto, como puede apreciarse del contenido del mencionado artículo, la autorregulación es voluntaria, por lo que si una asociación decide no acogerse a este posibilidad, no hay incumplimiento alguno. La forma de los instrumentos pueden ser acuerdos o códigos privados, estándares de privacidad o sellos de confidencialidad. Podrá considerarse elemento válido con garantías de protección adecuada si se cumplen los siguientes requisitos:

* Vinculación a todos los miembros que participen y que sean susceptibles receptores de datos personales.

* Que se incluyan los Principios de Protección de Datos.

* Que ofrezca garantías de cumplimiento.

* Que reconozca derechos de los interesados.

* Que incluya mecanismos de reparación al afectado.

En el marco y en línea con lo expuesto, el 14 de septiembre del pasado año 2001, el Grupo de Trabajo del Artículo 29 aprobó un Documento de trabajo relativo a la Práctica recomendada IATA 1774 "Protección de la vida privada y los flujos transfronterizos de los datos personales utilizados en el transporte aéreo internacional de pasajeros y mercancías".

IATA presentó al Grupo de Trabajo su iniciativa en 1997, con la finalidad de que fuera aprobado como Código de Conducta comunitario del artículo 27 de la Directiva 95/46/CE, aunque, finalmente, se desechó tal propósito. Tras mantener diversas reuniones y realizar varios estudios, la IATA aprobó en octubre de 2000 la Práctica Recomendada RP1774, respecto de la que el Grupo de Trabajo se pronuncia en el mencionado Documento de trabajo de 14 de septiembre pasado. Dicha Práctica Recomendada, por su propia naturaleza, no es vinculante, por lo que no existen mecanismos para instar su cumplimiento. Se trata de una sugerencia-marco, dentro del cual cada miembro actúa y aplica de conformidad a los preceptos nacionales y a sus propias prácticas comerciales. De hecho, finalmente la RP 1774 no fue concebida por sus propios promotores –salvo en estadios iniciales- como un código de conducta definitivo de las compañías aéreas que forman parte de IATA, sino para destacar algunos de los aspectos primordiales de la Directiva 95/46/CE y para servir de guía a sus miembros en la preparación de un código de conducta que deba ser presentado ante las correspondientes autoridades de protección de datos. En la RP se abordan definiciones, ámbito, principios de calidad de los datos, y cuestiones como las transferencias de datos a terceros países, acceso general a los datos sobre las reservas, legitimidad del tratamiento, información, categorías especiales de datos, notificación a las autoridades de control y la seguridad de los datos.

El Grupo de Trabajo del artículo 29 ha manifestado su satisfacción con la iniciativa de IATA y sugiere que siga avanzándose en esta labor, especialmente en lo relativo a las transferencias internacionales, punto en el que sería interesante contar con miembros de IATA de terceros países para trabajar en la consecución de un marco que ofrezca una protección adecuada. Así mismo, alienta a IATA a que se incluya en el billete de avión una mención a la protección de datos y la vida privada. También señala la conveniencia de que se informe a los viajeros asiduos las finalidades del tratamiento de sus datos, la manera concreta en que se utilizan los mismos y por quién, de manera que los pasajeros puedan oponerse. Las compañías aéreas deben asegurarse de que tan sólo tengan acceso a los datos personales aquellas personas que participen directamente en la prestación del servicio solicitado por el pasajero y no la totalidad de participantes potenciales en programas de este tipo.

1.6. Protección de los datos personales y el acceso del público a los documentos dentro de las Instituciones y Órganos comunitarios.

En virtud del artículo 30 de la Directiva 95/46/CE, el Grupo de Trabajo del Artículo 29 puede formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Unión Europea. Dicho artículo es la base normativa en la que se funda el Dictamen 5/2001, aprobado el 17 de mayo de 2001 por el Grupo de Trabajo del artículo 29 y referido a la protección de los datos personales y el acceso de los ciudadanos a los documentos oficiales de las Instituciones y Órganos comunitarios.

El Grupo de Trabajo ha manifestado en anteriores ocasiones que los datos personales contenidos en un documento oficial o en poder de una administración u organismo público conservan dicho carácter de personal, por lo que deben protegerse de conformidad con la legislación en materia de protección de datos, siempre que el tratamiento de dichos datos pertenezca al ámbito de aplicación de tal normativa9

El Grupo entiende que el derecho de acceso de los ciudadanos a los documentos oficiales es un elemento importante para la responsabilidad de los órganos públicos de cara a los ciudadanos así como para la transparencia del proceso de toma de decisiones por parte de dichos órganos.

Por ello, para responder a la pregunta de si una administración o un organismo público tiene la obligación de revelar los datos personales que conserva cuando los interesados no hayan dado explícitamente su consentimiento para ello, deberían tenerse en cuenta las consideraciones siguientes, que son pertinentes desde el punto de vista de la protección del derecho fundamental a la vida privada.

* Un análisis debe determinar si la difusión debe considerarse un tratamiento leal y lícito, según las circunstancias que concurran en cada caso. Además, la difusión no debe ser incompatible con los fines originales para los cuales los datos fueron recogidos y tratados posteriormente por la administración o el organismo público.

* Para que la divulgación sea legítima en el caso que nos ocupa, debe responder en general a una de las razones expuestas en el artículo 7 de la Directiva:

* El interesado ha dado su consentimiento de forma inequívoca

* El tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento. Conviene observar, no obstante, que la obligación de divulgación que impone la legislación relativa al acceso del público a los documentos administrativos no establece obligación absoluta de transparencia. La legislación

más bien supedita la obligación de garantizar el acceso a los documentos al respeto del derecho a la vida privada. Por tanto, no justifica una divulgación ilimitada o sin restricciones de los datos personales. Por el contrario, de la lectura conjunta de la legislación relativa al acceso del público y la relativa a la protección de la vida privada se desprende la necesidad de analizar individualmente las circunstancias de cada caso para encontrar un equilibrio entre ambos derechos. En particular, al término de este análisis, la legislación sobre el acceso del público a los documentos puede prever la aplicación de normas distintas a las diversas categorías de datos o tipos de interesados

* El tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos. Puede haber casos en los que, aunque la divulgación no sea una obligación específica del organismo público, éste no puede razonablemente cumplir las exigencias que la legislación le impone sin hacer públicos los datos personales que obran en su poder.

* El tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección. La necesaria evaluación de los derechos e intereses que concurren en una determinada situación debe realizarse individualmente, teniendo en cuenta todas las circunstancias. Si se considera que prevalece el derecho de acceso del público, deberán revelarse los datos personales. Si es el respeto de la vida privada el que prevalece, deberá rechazarse la divulgación de estos datos.

Dado que los dos derechos que confluyen en este tema – el de la protección de datos personales/respeto a la vida privada y el de acceso a los documentos oficiales - son de la misma naturaleza e importancia, el criterio del Grupo de Trabajo es la necesidad de que caso a caso, previo estudio y exhaustivo análisis de las circunstancias que intervengan en cada supuesto, traten de conciliarse y equilibrarse ambos derechos. Se prestará una muy especial atención –el Grupo de Trabajo expone a tal efecto, como hemos señalado, diferentes sugerencias y criterios en el documento- a los casos en los que órganos públicos reciban solicitudes de acceso a documentos que incluyan datos personales cuyos interesados no hayan otorgado explícitamente su consentimiento para ello.

1.7. Lucha contra el terrorismo y protección de datos.

El Grupo de Trabajo del Artículo 29 emitió el 14 de diciembre del pasado año 2001 el Dictamen 10/2001, titulado "Necesidad de llegar a una propuesta equilibrada en la lucha contra el terrorismo".

Los hechos que originaron la preparación y aprobación de dicho documento fueron los atentados terroristas ocurridos contra las "Torres Gemelas" en Nueva York el 11 de septiembre del pasado año 2001.

En dicho documento el Grupo señala la importancia y necesidad de conciliar y compatibilizar la lucha contra el terrorismo en particular, y criminalidad en general, con la debida protección de los derechos y libertades fundamentales de los individuos, en particular el derecho fundamental a la protección de datos, garantizado y reconocido por la normativa comunitaria (Directivas 95/46/CE y 97/66/CE así como en el Convenio Europeo de Derechos Humanos).

De ahí la importancia de garantizar en todo momento el principio de proporcionalidad, de limitar al máximo cualquier medida que pueda suponer una restricción de los derechos fundamentales, teniendo siempre en consideración que cualquier medida que se ponga en práctica para luchar contra el terrorismo no tiene por qué reducir el standard de protección de derechos fundamentales que caracteriza a las sociedades democráticas –la normativa comunitaria de protección de datos ya prevé excepciones basadas en la lucha contra la criminalidad- y debiendo especificar tal medida con claridad las circunstancias y el margen en el que se autorice a la autoridad pública a proceder a tal restricción.

1.8. Participación en el Grupo de Trabajo del Artículo 29 de países candidatos a la Unión Europea.

El pasado mes de diciembre se aprobó la Decisión 1/2001, de 13 de diciembre, del Grupo de Trabajo sobre la participación en las reuniones del Grupo del Artículo 29 de representantes de las Autoridades de Control de los países candidatos a la Unión Europea.

Se decidió que el Grupo de Trabajo, a través de su Presidente, puede invitar a las Autoridades de Protección de Datos de los 13 países que han solicitado adhesión a la Unión Europea a participar, en calidad de observadores, en las reuniones del Grupo, que se reserva la decisión acerca de su asistencia a los puntos del orden del día de las reuniones que estime pertinentes.

1.9. Decisiones de la Comisión Europea sobre Cláusulas Contractuales Tipo para la transferencia de datos personales a terceros países que no garantizan un nivel de protección adecuado

Durante el año 2001, el Grupo de Trabajo del Artículo 29 se ha ocupado en dos ocasiones de sendos Proyectos de Decisión de la Comisión Europea que, en uso de las competencias que le atribuye el artículo 26.4 de la Directiva 95/46/CE, declaraban que un determinado conjunto de cláusulas contractuales tipo ofrecían, en los términos establecidos en el apartado 2 del mismo artículo, las garantías suficientes para permitir la transferencia de datos personales a países que no ostentan un nivel de protección adecuado.

El primero de dichos proyectos declaraba la adecuación de un conjunto de cláusulas contractuales tipo para la transferencias internacionales desde un responsable de tratamiento establecido en un Estado miembro de la UE a otro responsable de tratamiento establecido en un país del cual no se hubiera declarado que ofrecía garantías suficientes. El Proyecto de Decisión excluía expresamente de su ámbito de aplicación las transferencias cuyo destinatario realizara

las funciones de un encargado de tratamiento para el responsable establecido en territorio europeo.

Como ya se informó en la Memoria correspondiente al año 2000, el Grupo de Trabajo había sido consultado anteriormente respecto de un primer proyecto sobre el que tuvo la oportunidad de pronunciarse y emitir comentarios en dicho año. Por lo tanto, en el nuevo Dictamen 1/2001, se constataba la satisfacción del Grupo por el hecho de que una gran parte de los comentarios realizados se hubieran tenido en cuenta. Por ello, aun apoyando el nuevo texto presentado por la Comisión, se reafirmaba la opinión emitida anteriormente y se realizaban nuevos comentarios.

En primer lugar, respecto de la legitimidad de la transferencia conforme al Derecho nacional, se dejaba claro en el Dictamen que toda transferencia es, en sí misma, una operación de tratamiento y que, por lo tanto, su licitud está sujeta a lo que la legislación nacional de transposición de la Directiva 95/46/CE disponga.

A continuación, se puntualizaba que el Grupo de Trabajo deseaba dejar clara la necesidad de que se pudieran prohibir o suspender las transferencias a aquellos países en los que su legislación pudiera impedir la exigencia de la ejecución de las obligaciones contenidas en el contrato.

Esta posibilidad de suspender o prohibir las transferencias también debía estar presente cuando existiera algún mandato imperativo en virtud de la legislación del Estado del importador por el cual se impusieran restricciones a los derechos fundamentales de los ciudadanos que fueran más allá de las que pudieran resultar necesarias en una sociedad democrática en las situaciones contempladas en el artículo 13 de la Directiva 95/46/CE.

Respecto de las obligaciones del importador de datos, se señalaba el carácter fundamental e indispensable de tres principios esenciales: principio de finalidad, restricciones a las transferencias ulteriores y el compromiso del importador de garantizar los derechos de acceso, rectificación y cancelación.

Es absolutamente necesario que el importador se comprometa a utilizar los datos personales estrictamente para las mismas finalidades especificadas en el contrato, dado que la legitimidad de dicho tratamiento bajo el Derecho nacional del exportador sólo se ha verificado en relación a dichas finalidades.

La complejidad y casuística que puede aparecer en las transferencias ulteriores es enorme. Por ello, el Grupo se mostraba partidario de incluir una fórmula simple en las cláusulas mediante la cual se prohibiera toda transferencia ulterior en virtud de las cláusulas contractuales. Si dicha transferencia ulterior resultase necesaria, se debería realizar un nuevo contrato entre el exportador establecido en el Estado miembro de la UE y el nuevo importador o bien sería necesario que el afectado diera su consentimiento al exportador para esta nueva transferencia.

Una de las posibilidades que el Proyecto de Decisión de la Comisión preveía era que las operaciones de tratamiento que realizara el importador con los datos procedentes de la UE se rigieran conforme a un conjunto de principios obligatorios contenidos en la propia Decisión. A este respecto, el Grupo mostraba su acuerdo siempre y cuando dichos principios se interpretasen conforme a lo que eran: principios que nacían de la Directiva 95/46/CE. Además, recomendaba firmemente que se incluyera un principio sobre decisiones automatizadas, sobre todo teniendo en cuenta las actividades de las agencias de información de crédito situadas en terceros países que recibirían datos desde Europa.

También se preveía la posibilidad de que dichos tratamientos se rigieran por lo establecido en la legislación de protección de datos de un tercer país respecto del cual la Comisión Europea hubiera declarado su adecuación. El Grupo consideraba que una Decisión de Adecuación no se toma sólo en base a una ley específica sino que tiene en consideración todo el entorno legal y constitucional del país, por lo que dicha opción sólo podría ser admisible si se aplicaba a importadores establecido en el país de cuya legislación se tratase y ésta hubiera sido considerada adecuada sólo para ciertos sectores, el importador no perteneciera a estos sectores y, en todo caso, fueran de aplicación las consideraciones realizadas anteriormente sobre el principio de finalidad, las transferencias ulteriores y el ejercicio de los derechos de los ciudadanos.

Respecto de las garantías para la aplicación de las cláusulas, el Grupo reiteraba que la responsabilidad solidaria del exportador y el importador era la única posibilidad de resolver adecuadamente las dificultades que la solución contractual genera en relación con la efectiva garantía de los derechos de los ciudadanos y las indemnizaciones por los daños que les puedan ser ocasionados.

En relación con la cláusula de jurisdicción, el Grupo, aun estando de acuerdo con las opciones que en ella se presentaban y que incluían el recurso ante los tribunales del exportador, recomendaba la posibilidad que los recursos también pudieran ser presentados en los tribunales del país de residencia del afectado, recomendación que, finalmente, no se incluyó en el texto definitivo.

El documento finalizaba dando un dictamen positivo al Proyecto de Decisión siempre y cuando se tuvieran en cuenta los comentarios y sugerencias realizadas por el Grupo de Trabajo.

Finalmente, el 15 de junio de 2001, la Comisión Europea aprobaba una Decisión sobre cláusulas contractuales (2001/497/CE)10 que se publicaba en el Diario Oficial L 181, de 4 de julio de 2001.

A pesar de que en dicha Decisión no se recogieron todos los comentarios y recomendaciones realizados por el Grupo de Trabajo, se puede decir que la misma otorga, en general, garantías suficientes para la transferencia de datos a países que no gozan de un nivel de protección adecuado.

Como ya se ha comentado previamente, la Decisión 2001/497/CE sólo trataba el caso en que la transferencia internacional de datos ocurría entre dos responsables de tratamiento. Una vez aprobada la Decisión anterior, la Comisión Europea volvió a someter a la consideración del Grupo de Trabajo un nuevo proyecto que abarcaba las transferencias entre un responsable de tratamiento establecido en la Unión Europea y un encargado de tratamiento establecido en un país en el que no se garantizara un nivel adecuado de protección de datos.

Al igual que en el caso anterior, el Grupo consideró que el mismo Subgrupo, del que formaba parte la Agencia española, que había trabajado con los servicios de la Comisión en el proyecto anterior, se ocupara de avanzar los trabajos del nuevo Proyecto de Decisión.

Como resultado de dicho proceso, la Comisión Europea sometió a la consideración del Grupo de Trabajo un Proyecto de Decisión sobre el que el Grupo emitió el Dictamen 7/2001.

El Grupo de Trabajo comenzaba resaltando que el cumplimiento, por parte del responsable del tratamiento, de las disposiciones nacionales adoptadas en virtud de lo previsto en el artículo 17 de la Directiva 95/46/CE, no satisface en sí mismo la exigencia señalada en el artículo 26.2 de la Directiva, esto es, el ofrecer garantías suficientes para que un Estado miembro pueda autorizar una transferencia o una serie de transferencias a tenor de lo establecido en el artículo 26.2, puesto que los contratos considerados deben suplir la falta de una protección adecuada en el país de destino, lo cual no es el objeto del artículo 17 de la Directiva 95/46/CE.

Además, y por norma general, la vida privada de las personas queda potencialmente expuesta a mayores riesgos cuando los servicios de tratamiento de datos se subcontratan fuera de la Comunidad que cuando se realizan dentro de la misma. Si los datos están físicamente localizados en terceros países, resulta considerablemente más difícil hacer cumplir el contrato o las decisiones de las autoridades supervisoras.

Finalmente, y tal como el Grupo señaló ya en su Dictamen 1/2001, siempre existe la posibilidad de que los encargados del tratamiento en terceros países se vean sometidos a intervenciones de los poderes públicos que vayan más allá de lo que se considera necesario en una sociedad democrática.

Respecto a las medidas de seguridad, el Grupo de Trabajo opinaba que el importador debe aplicar las medidas de seguridad que se definan en el ordenamiento jurídico del Estado miembro en el que esté establecido el exportador, lo cual es coherente tanto con el principio general con arreglo al cual el importador de los datos queda vinculado por la legislación del país del exportador, como con el hecho de que el exportador dé instrucciones al importador de conformidad con lo previsto en su propia legislación.

El Grupo de Trabajo entendía los motivos que llevaban a la Comisión a desear introducir en su proyecto una mayor flexibilidad en lo que respecta a las medidas de seguridad, sobre todo cuando el importador recibía datos personales de exportadores establecidos en diferentes Estados miembros, pero constataba que la Directiva no ofrece muchas posibilidades a este respecto. Por ello, recomendaba a la Comisión y al Comité del Artículo 31 que aprobaran cláusulas contractuales tipo en las que se estipulara, por un lado, que las medidas de seguridad deberán especificarse y, por otro, que la adecuación de tales medidas deberá determinarse a la luz de la legislación aplicable, esto es, aquella a la que esté sujeto el exportador de los datos. No obstante, podría resultar útil que, en el futuro, la Comisión presentara al Grupo de Trabajo propuestas pormenorizadas que permitan responder a dicho problema.

Al igual que ya había sucedido en la tramitación de la Decisión 2001/497/CE, el Grupo atribuyó una importancia extraordinaria a la inclusión de una cláusula de terceros beneficiarios, dando la posibilidad a los interesados a exigir la ejecución de aquellas cláusulas del contrato que les afectaban aunque no fueran parte del mismo. Por ello, el Grupo en su Dictamen acoge favorablemente la inclusión de esta cláusula en la Decisión.

En relación con las transferencias ulteriores, el Grupo de Trabajo opina que (al igual que ocurrió con la Decisión 497/2001) es extremadamente difícil definirlas de forma plenamente satisfactoria. En consecuencia, proponía modificar el Proyecto de Decisión de tal manera que quedara claro que las transferencias posteriores a terceros sólo serían posibles si son conformes a la legislación sobre protección de datos aplicable, a las cláusulas y a las instrucciones dadas por el exportador de datos.

El Grupo de Trabajo aprobaba la idea de considerar excepcionalmente responsable al importador de los datos en el limitado número de casos especificados en las cláusulas contractuales tipo, es decir, cuando el exportador estuviera en quiebra o hubiera quedado jurídicamente extinguido y, además, el importador hubiera incurrido en falta al incumplir las obligaciones que le imponen las cláusulas, causando así un perjuicio a los interesados. El Grupo de Trabajo recomendaba, asimismo, que se dejara claro en los considerandos de la Decisión de la Comisión que los derechos derivados del contrato (derechos de terceros beneficiarios) habían de ejercerse, en primer lugar, contra el exportador de datos, y sólo excepcionalmente contra el importador.

También apoyaba el Grupo la posibilidad de que las autoridades responsables de la protección de los datos pudieran ejercer sus facultades de investigación. Si bien es a todas luces improbable que se realicen con frecuencia auditorías en los países terceros en los que estén establecidos los encargados del tratamiento de datos y cabe esperar que éstas se limiten a casos realmente graves y excepcionales en que los derechos fundamentales de las personas puedan verse seriamente perjudicados, el Grupo de Trabajo deseaba poner de relieve que la garantía dada por el importador de datos a este respecto en las cláusulas es plenamente coherente con la sujeción de éste a la legislación del país del exportador y, por consiguiente, es un elemento muy importante si se desea que las cláusulas contractuales tipo ofrezcan garantías suficientes a efectos de lo previsto en el artículo 26.2 de la Directiva.

Por todo ello, sin perjuicio de las anteriores recomendaciones, el Grupo de Trabajo emitió un dictamen favorable en relación con el proyecto de Decisión de la Comisión.

La Decisión de la Comisión 2002/16/CE11, notificada con el número C(2000)4540, de 27 de diciembre de 2001, publicada en el Diario Oficial de las Comunidades Europeas L 6, de 10 de enero de 2002, aprobó un conjunto de cláusulas tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que tuvieron en cuanta la mayor parte de las recomendaciones realizadas por el Grupo en su Dictamen.

2. CONSEJO DE EUROPA

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal o Convenio 108 del Consejo de Europa, firmado en 1981 y ratificado por España en 1985, es el primer instrumento internacional que vincula a los Estados signatarios del mismo para adoptar la legislación nacional necesaria que introduzca en su Derecho interno los principios y garantías establecidos en dicho Convenio.

Este Convenio, en el cual se han inspirado todas las legislaciones europeas posteriores en materia de protección de datos, permitía, en principio, el libre flujo de datos personales entre los Estados que son parte del mismo, flujo que sólo podría impedirse en los supuestos en que dichos Estados dejen de ser parte del Convenio o en caso de que la protección de datos en el país en cuestión, aún habiendo sido firmado el Convenio, no sea equivalente o en caso de que los datos se transfieran a un tercer Estado que no sea signatario del mismo.

El Convenio crea un Comité Consultivo (T-PD), compuesto por los representantes de los Estados que son parte en el mismo. Este Comité es el encargado de la interpretación de las normas, cuidando asimismo del cumplimiento del Convenio.

Los principios contenidos en el Convenio deben adaptarse e interpretarse en función de los diferentes sectores implicados en la actividad. La actividad del Consejo de Europa con este fin se ha desarrollado mediante la aprobación de diversas recomendaciones, dado que su procedimiento de adopción es sencillo y se adaptan mejor a las circunstancias cambiantes de la protección de datos. Estas recomendaciones, a pesar de su carácter no vinculante, son tenidas en cuenta por las Partes del Convenio y son una referencia de gran valor para la aplicación del Convenio a distintos sectores y situaciones.

Con el fin de elaborar estas recomendaciones el Comité de Ministros creó en 1976 un Comité de Expertos sobre protección de datos, que se convirtió después en el Grupo de Proyectos sobre protección de datos (CJ-PD). Este Comité se compone de expertos de los todos los Estados Miembros del Consejo de Europa, que desempeñan tareas de responsabilidad en relación con la protección de datos en sus respectivos países.

La Agencia de Protección de Datos española forma parte de este Comité, participando activamente en los diferentes debates y trabajos preparatorios de los distintos documentos elaborados por el mismo.

Debido a que el mandato de este Comité expira en el año 2002 y a problemas presupuestarios y de racionalización de las actividades de protección de datos dentro del Consejo de Europa, se están dando los pasos necesarios para reunificar las actividades de ambos comités dentro del T-PD.

Uno de los problemas que deberán resolverse es la posibilidad de participación, al menos como observadores, de los Estados miembros del Consejo de Europa que, por el hecho de serlo, envían representantes al CJ-PD, pero que no pueden participar en el T-PD, reservado a la representación de aquellos Estados que han ratificado el Convenio 108.

En relación con los trabajos del CJ-PD, este Comité se reunió sólo en una ocasión en el año 2001, centrándose sus trabajos en la redacción de un documento de directrices sobre la protección de las personas en relación con la recogida y tratamiento de datos personales por medio de la videovigilancia, un primer debate sobre un documento de principios que deben informar el tratamiento de datos personales en relación con el uso de tarjetas inteligentes y el examen de los trabajos que están siendo realizados en distintos comités del Consejo de Europa: tratamiento de datos personales en los sectores policial y judicial; acceso a documentos oficiales; genética, bioética, biomedicina y derechos humanos y cibercriminalidad.

Otro hecho digno de especial mención fue la entrada en vigor y comienzo del proceso de firma y ratificación del Protocolo Adicional al Convenio 108 en relación con autoridades de control y transferencias internacionales de datos personales. El Protocolo fue adoptado el 23 de mayo de 2001 y quedó abierto para su firma y ratificación el 8 de noviembre de 200112.

Este Protocolo adicional viene a reforzar las garantías especificadas en el Convenio 108 mediante el requerimiento de que las Partes del Convenio que ratifiquen dicho Protocolo deban crear autoridades de supervisión que ejerzan sus funciones con completa independencia, ya que estas Autoridades son un elemento capital para la efectiva protección de las personas en relación con el tratamiento de sus datos personales.

Estas autoridades de control deberán tener poderes de investigación e intervención así como capacidad legal para intervenir en procedimientos legales y jurisdiccionales. Deberán tramitar las reclamaciones y denuncias presentadas por los ciudadanos y sus decisiones serán recurribles ante los tribunales.

Por otra parte, dado el incremento de intercambios de datos personales entre distintos países y la carencia de un marco adecuado que regulara esta materia en el Convenio 108, resulta también necesario en estos casos el asegurar la efectiva protección de los derechos y libertades fundamentales y, en particular, el derecho a la protección de datos, por lo que el Protocolo establece que las transferencias a Estados u organizaciones que no sean Partes del Convenio sólo podrán realizarse, con carácter general, si dichos Estados u organizaciones aseguran un nivel adecuado de protección de datos para la transferencia de que se trate.

Como excepciones a dicha regla general se contemplan el que el Derecho nacional lo permita en base a un interés específico del interesado o siempre y cuando prevalezcan intereses públicos importantes. También se podrían realizar dichas transferencias si el exportador, a través de determinadas cláusulas contractuales, suministra garantías que las autoridades de protección de datos consideren adecuadas.

En otro orden de cosas, el Consejo de Europa y el Inspector General para la Protección de Datos de Polonia, con motivo del vigésimo aniversario del Convenio 108, organizaron en Varsovia una Conferencia Europea sobre protección de datos con el lema "Presente y futuro del Convenio 108".

Los puntos principales que se trataron durante la conferencia fueron:

* Leyes de protección de datos: respuestas presentes y futuras a los retos de la Sociedad de la Información
* La relevancia de los principios de protección de datos establecidos en el Convenio 108 y su Protocolo Adicional
* Mecanismos para la implantación y cooperación internacional en el contexto de la protección de datos: mecanismos existentes y mecanismos que deberían establecerse
* La posición de los individuos en un mundo de información globalizada: derechos y obligaciones.

El Director de la Agencia de Protección de Datos pronunció una ponencia dentro del apartado de cooperación internacional, en la cual se daba cuenta de la experiencia práctica española en este aspecto tanto en su vertiente bilateral como multilateral y se comentaban las principales iniciativas y problemas encontrados por la Agencia de Protección de Datos en este campo.

Asimismo, también se hizo especial hincapié en que el mayor reto al que se enfrenta la protección de datos personales es la extensión del enfoque que podríamos llamar "europeo", esto es, la consideración de la protección de datos personales como un derecho fundamental de la persona humana y, por ello, digno de ser defendido mediante la existencia de una legislación que precise sus principios esenciales y establezca los derechos de los ciudadanos, a otras áreas geográficas, y, en especial a los países iberoamericanos ya que son un área con la que Europa, en general, y España, en particular, tienen una relación privilegiada.

No se puede terminar de revisar la actividad del Consejo de Europa sin mencionar la aprobación y entrada en vigor del Convenio sobre Cibercrimen que, sin ser específicamente un asunto de protección de datos, ha concitado toda una serie de reacciones y comentarios por parte de los distintos comités, conferencias y autoridades en los que están representadas las autoridades de control de protección de datos.

Como ya en otro lugar de esta Memoria se incluyen las menciones a los documentos aprobados por el Grupo de Trabajo del Artículo 29 sobre esta materia, baste aquí mencionar su aprobación por el Consejo de Ministros del Consejo de Europa y el comienzo del proceso de firma y ratificación del mismo el día 23 de noviembre de 2001 en Budapest. Este Convenio permite el acceso al mismo no sólo los Estados miembros del Consejo de Europa, sino que también está abierto a la adhesión de terceros países que han participado en su redacción como Canadá, Estados Unidos, Japón y Sudáfrica

3. AUTORIDAD COMÚN DE CONTROL DEL SISTEMA DE INFORMACIÓN SCHENGEN

El objetivo del Convenio de Aplicación del Acuerdo de Schengen es permitir la supresión de los controles en las fronteras comunes en la circulación de personas entre los Estados miembros (en la actualidad Alemania, Austria, Bélgica, España, Francia, Grecia, Italia, Luxemburgo, Países Bajos, Portugal, así como los países nórdicos que se integraron en marzo de 2001: Noruega, Suecia, Finlandia, Dinamarca e Islandia), manteniendo en el interior del territorio Schengen creado un nivel de seguridad al menos igual al que ya existía.

Entre las medidas compensatorias previstas en el Convenio que persiguen este objetivo, se encuentran la armonización de la política en materia de expedición de visados, una política común en materia de determinación del Estado responsable del examen de la solicitud de asilo, la mejora de la cooperación policial y judicial, la intensificación de la lucha contra el tráfico ilegal de estupefacientes, la armonización del nivel de control de las fronteras exteriores del territorio Schengen y la creación del Sistema de Información Schengen (SIS).

El principal objeto del SIS es, con la ayuda de la información que se transmite en el sistema, preservar el orden y la seguridad públicos, incluida la seguridad del Estado, así como la aplicación de las disposiciones previstas en el Convenio relativas a la circulación de personas en los territorios de los países que conforman el territorio Schengen. El SIS consta de una parte nacional (NSIS) en cada uno de los países que aplican el Convenio y de una unidad de apoyo técnico central ubicada en Estrasburgo (CSIS), estableciéndose de esta forma una conexión entre todos los Estados miembros que permite a los usuarios del sistema la posibilidad de disponer en tiempo real de la información necesaria para sus misiones. Esta información está disponible al efectuar controles en la frontera, así como cuando se realizan

otros controles de policía y de aduanas; en el caso de los extranjeros, la información está disponible a efectos del procedimiento de expedición de visados, de expedición de permisos de residencia y de la administración de aquéllos en el marco de la aplicación de las disposiciones sobre la circulación de personas.

En el Capítulo Tercero del Título IV del Convenio se establecen los principios y mecanismos destinados a garantizar una adecuada protección de los datos de carácter personal residentes en el SIS. En su artículo 114 figura que en cada país debe designarse una autoridad de control que, respetando el Derecho nacional, se encargue de ejercer un control independiente sobre la parte nacional del SIS y de comprobar que el tratamiento y la utilización de los datos introducidos en el SIS no atentan contra los derechos de la persona que se trate. Asimismo, se indica que toda persona tendrá derecho a solicitar a esta autoridad que compruebe los datos referentes a ella integrados en el SIS, así como el uso que se haga de dichos datos. El artículo 10 del Real Decreto 428/1996, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, encomienda a ésta el ejercicio del control aquí mencionado.

Por otra parte, el artículo 115 del Convenio establece la creación de una Autoridad de Control Común (ACC) encargada del control de la unidad de apoyo técnico del SIS; esta autoridad está compuesta por dos representantes de cada autoridad nacional de control. También el artículo 10 del Real Decreto mencionado establece que el Director de la Agencia designará a los dos representantes que formarán parte de la Autoridad de Control Común.

La delegación española ha asistido a las cuatro sesiones plenarias que ha celebrado la ACC durante el año 2001 en la sede del Consejo de la Unión Europea en Bruselas.

A continuación se exponen algunos de los temas que trató la ACC durante el año 2001, incluyéndose también en anexo el quinto Informe de Actividades elaborado por esta Autoridad y que cubre el periodo comprendido entre marzo del año 2000 y diciembre del 2001.

3.1. Integración del Reino Unido e Irlanda

Estos dos países son los únicos de la Unión Europea que no aplican el acervo de Schengen. El artículo 4 del Protocolo Schengen ofrece la posibilidad al Reino Unido y a Irlanda, que no están vinculados por el acervo de Schengen, de solicitar su participación en algunas de las disposiciones de dicho acervo o en todas.

El Reino Unido ya había invocado dicha disposición para aplicar una parte del acervo de Schengen, en particular, la relativa al SIS. El proyecto de Decisión prevé que el régimen de protección de datos del Convenio de Schengen sea aplicable al Reino Unido en la medida en que este país aplique el acervo, previéndose en la actualidad que únicamente debería excluirse del ámbito de aplicación el artículo 96 del Convenio, relativo a extranjeros no admisibles a territorio Schengen. La ACC también concedió el estatuto de observador al Reino Unido, razón por la que representantes de este país ya participan en las sesiones de esta Autoridad.

Respecto de Irlanda, se está estudiando su solicitud dirigida a participar en una parte de las disposiciones del acervo de Schengen.

Durante el año 2002 se realizarán las comprobaciones pertinentes para verificar en estos países las condiciones previas a la puesta en aplicación del acervo de Schengen, verificaciones en las que desearía participar la ACC.

3.2. Proyecto de Resolución del Consejo relativa a las normas sobre protección de datos personales en los instrumentos del tercer pilar de la Unión Europea

La ACC tras estudiar el proyecto de Resolución del Consejo relativa a las normas sobre protección de datos personales en los instrumentos del tercer pilar de la Unión Europea, elaborado por el Grupo "Sistemas Informáticos y Protección de Datos", concluyó que lamentaba que este instrumento sólo tuviera un valor orientativo, con lo que difícilmente serviría para armonizar las normas sobre protección de datos en el tercer pilar, objetivo inicial de la elaboración de dicha Resolución.

3.3. Evolución del SIS

La ACC participó inicialmente en los trabajos que se realizaron para el desarrollo del futuro SIS II, el cual solucionará las deficiencias del actual SIS. Posteriormente, se han formulado diferentes propuestas destinadas a ampliar las funcionalidades del SIS. Algunas de éstas implican una modificación de las disposiciones existentes en el acervo de Schengen, sobre las que subsisten diferencias de opinión entre los Estados miembros.

La ACC considera que para que las propuestas tengan una buena acogida entre los Estados miembros, estas diferencias de opinión deberán superarse rápidamente. Asimismo, la ACC está muy pendiente de las nuevas funcionalidades que puedan incluirse en el SIS II, que no han sido todavía formalmente definidas, con el fin de verificar que las mismas respetan los principios de protección de los datos de carácter personal.

3.4. Página Internet de la ACC

La ACC está pendiente de que su página web se incluya en los servidores del Consejo, en la que se incluirá información dirigida a los ciudadanos de los derechos de protección de datos que les asisten. Durante el año 2001 está página ha sido mantenida de forma provisional por la autoridad portuguesa, pudiendo ser consultada en la dirección: http://www.cnpd.pt/schengen.

4. AUTORIDAD COMÚN DE CONTROL DE EUROPOL

El Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol)13, cuya adopción recomienda el Consejo de la Unión Europea en su Acto 95/C 316/01, de 26 de julio de 1995 y que fue ratificado por el Reino de España en el año 1997, tiene como objetivos, según establece su artículo 2, *"(...) mejorar, en el marco de la cooperación entre los Estados miembros de conformidad con el punto 9 del artículo K.1 del Tratado de la Unión Europea, por medio de las actividades que se enumeran en el presente Convenio, la eficacia de los servicios competentes de los Estados miembros y la cooperación entre los mismos con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional, en la medida en que existan indicios concretos de una estructura delictiva organizada y que dos o más Estados miembros se vean afectados por las formas de delincuencia antes mencionadas, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados miembros"*.

Además, el Convenio Europol establece unos requisitos mínimos en materia de protección de datos personales que deberán cumplir los Estados Miembros que sean Parte del mismo. En concreto, cada Parte deberá adoptar las disposiciones nacionales necesarias para conseguir un nivel de protección de datos que sea, como mínimo, equivalente al resultante de los principios del Convenio del Consejo de Europa de 28 de enero de 1981 (Convenio 108), teniendo en cuenta la Recomendación R(87) 15, de 17 de septiembre de 1987, del Comité de ministros del Consejo de Europa encaminada a regular la utilización de datos de carácter personal en el sector de la policía14.

Adicionalmente, en el artículo 24, se crea una Autoridad Común de Control independiente cuyo cometido será vigilar la actividad de Europol, con el objeto de garantizar que el almacenamiento, el tratamiento y la utilización de los datos de que dispongan los servicios de Europol no vulneren los derechos de las personas y controlar la licitud de la transmisión de los datos que procedan de Europol. Esta Autoridad Común de Control estará integrada, como máximo, por dos miembros o representantes de las autoridades nacionales de control (la Agencia de Protección de Datos en el caso español).

Para llevar a cabo sus tareas, la Autoridad Común de Control de Europol (en adelante, ACC-Europol) se reunió en siete ocasiones durante el año 2001, durante las cuales se abordaron diversos aspectos de su competencia que pasamos a resumir a continuación, además de las reuniones y actuaciones realizadas por los distintos subgrupos que tienen encomendadas tareas específicas y que realizan una labor previa a las discusiones del plenario15.

En primer lugar, la ACC-Europol siguió emitiendo los dictámenes preceptivos respecto de las Órdenes de Creación de Ficheros con Fines de Análisis que, tal y como establece el artículo 12.1 del Convenio, Europol sometió a su consideración. En dichos dictámenes se ha informado a Europol de todas aquellas dificultades que la ACC-Europol ha observado en las distintas órdenes, solicitándose aclaraciones de Europol cuando se ha considerado necesario16.

Otro aspecto importante lo han constituido la evacuación de dictámenes en relación con las negociaciones de Acuerdos entre Europol y Terceros Países y Organismos. La ACC-Europol debe emitir dictámenes al comienzo de las negociaciones para pronunciarse sobre la existencia o no de obstáculos insalvables para el comienzo de las mismas17. En el año 2001 se han emitido dictámenes favorables al inicio de negociaciones con Suiza, la República Checa, y, sujeto a un número de consideraciones sobre los puntos que deberían tenerse muy en cuenta durante las mismas, los Estados Unidos de América.

Asimismo, la ACC-Europol debe también pronunciarse sobre los proyectos de Acuerdo entre Europol y Terceros Países y Organismos con carácter previo a la firma de los mismos18. En este sentido, la ACC-Europol ha emitido dictámenes favorables a los Proyectos de Acuerdo celebrados con Noruega, Islandia, Suiza, República Checa, Polonia, Hungría, Eslovenia y Estonia así como un informe desfavorable al Proyecto de Acuerdo entre Europol y la Organización Internacional de Policía Criminal (INTERPOL), salvo que se remediaran las deficiencias observadas en el mismo y que se detallaban en el Dictamen de la ACC-Europol.

Otro aspecto importante en relación con la transmisión de datos a terceros países y organismos, ha sido la propuesta de modificación, presentada por Europol, de las Normas que rigen la transmisión de datos personales a terceros Estados y organismos (Acto del Consejo 1999/C 88/01). El objetivo perseguido era que las organizaciones internacionales pudieran, en determinadas circunstancias, retransmitir los datos que recibían de Europol a los Estados miembros de las mismas, comunicación prohibida por la normativa existente. En concreto, la modificación prevista preveía que se pudieran comunicar datos a aquellos Estados miembros de dichas organizaciones internacionales que ya hubieran suscrito un Acuerdo en dicho sentido con Europol además de cuando se dieran las circunstancias excepcionales previstas en el artículo 2.1 b) del Acto del Consejo 1999/C 88/01: salvaguardar los intereses fundamentales de los Estados miembros dentro del ámbito de los objetivos de Europol o a fin de prevenir un peligro inminente de comisión de delito.

La ACC-Europol fue consultada sobre las modificaciones propuestas y evacuó un dictamen en el que se establecían las condiciones para que dicha modificación fuera aceptable, en concreto, que salvo que pudieran aplicarse las excepciones prevista en caso de urgencia o grave daño a los intereses fundamentales de un Estado miembro, la retransmisión sólo debería ser posible si en el acuerdo celebrado entre Europol y el tercer organismo se prevé dicho reenvío y sólo a aquellos Estados que proporcionen garantías adecuadas.

Además, en el caso de aplicar el procedimiento de urgencia debido a circunstancias excepcionales, el Director de Europol debería garantizar y justificar que el nivel de protección del tercer Estado que recibe los datos es el adecuado y deberá llevar un registro de cada caso de reenvío, amén de contar con el consentimiento del Estado miembro que suministró la información a Europol.

Dado que las observaciones realizadas por la ACC-Europol fueron incorporadas al texto final del Proyecto de Modificación, ésta emitió Dictamen favorable sobre el mismo.

Otro hecho digno de mención es la finalización del proceso comenzado con la primera auditoría que la ACC-Europol realizó a Europol a finales de 2000. En el año 2001 se produjo la aprobación del texto definitivo del Informe de Inspección elaborado por el equipo de expertos que realizaron la auditoría -que contaba con un Inspector de la Agencia de Protección de Datos- tras tener en cuenta los comentarios realizados por Europol. Dicho informe que, en líneas generales, evaluaba favorablemente el nivel de adecuación de Europol a lo que el Convenio establece en materia de protección de datos, señalaba aquellos puntos en que se encontraron algunas deficiencias y realizaba las recomendaciones oportunas para subsanarlas. El Informe de Inspección, una vez aprobado por el plenario de la ACC-Europol, se remitió al Consejo de Administración y al Director de Europol.

Asimismo, la ACC-Europol ha aprobado la realización de una segunda auditoría a Europol en el primer semestre del año 2002 que tendrá como objetivos fundamentales comprobar la efectiva implantación de las recomendaciones realizadas en el Informe de Inspección, profundizar en el conocimiento y operativa del Sistema de Análisis y verificar el nuevo Sistema de Información que Europol tiene previsto implantar en el año 2002.

Otro asunto que ha ocupado la atención de la ACC-Europol durante el año 2001 han sido los llamados Proyectos Operativos de los Estados Miembros con Apoyo de Europol (POEMAE). Durante la inspección realizada en Europol en noviembre de 2000, se constató la existencia de proyectos de análisis operativos cuyas Órdenes de Creación no habían sido sometidas al informe preceptivo de la ACC-Europol.

Al solicitar una explicación a Europol sobre este hecho, se puso de manifiesto que Europol estaba dando soporte, mediante sus recursos técnicos y humanos, a proyectos de análisis bajo el concepto denominado "Estado miembro líder", mediante el cual dos o más Estados miembros iniciaban un proyecto de análisis común basado en la cooperación bilateral o multilateral fuera del alcance del Convenio Europol en el cual, a pesar de estar todos los datos personales almacenados en los equipos de Europol, se consideraban datos nacionales bajo la jurisdicción del Estado miembro líder y se trataban en base a la legislación nacional de dicho Estado, que era el único responsable de la legalidad o no de los mismos.

La ACC-Europol ha manifestado en diversas ocasiones que aunque entre los fines genéricos del Convenio figure el mejorar la cooperación entre las autoridades competentes de los Estados miembros, la realización de proyectos de análisis tiene una regulación propia y específica en el Convenio, por lo que todos los proyectos deberían de reflejarse en una Orden de Creación que se sometiera al dictamen de la ACC.

No obstante, también mostraba su comprensión por las dificultades operativas que la tramitación especificada en el Convenio de dichas órdenes, larga y compleja, acarrea en la práctica, por lo que comunicó a Europol su disponibilidad para estudiar el problema y buscar los mecanismos más adecuados para agilizar el proceso global respetando el marco legal establecido en el Convenio.

Finalmente, el Subgrupo de Tecnologías de la Información que lidera la Agencia española, ha preparado tres informes que han sido aprobados por el plenario de la ACC-Europol.

El primero de ellos se refería a un Sistema de Información Provisional que Europol tenía intención de poner en marcha. Por diversos motivos Europol no había desarrollado todavía el Sistema de Información previsto en el Convenio y el sistema que se venía utilizando resultaba poco eficaz.

Aunque el Sistema de Información definitivo se ha estado desarrollando a lo largo del año 2001, Europol desarrolló con su propio personal un prototipo que, aunque de funcionalidad limitada, podría ayudar a solventar la urgente necesidad detectada por Europol de poder compartir la información de una manera eficaz y respetuosa con las previsiones del Convenio.

El dictamen se basó en la información disponible que no permitía una evaluación profunda del sistema que requeriría más información técnica o, incluso, una auditoría presencial.

No obstante, el dictamen hacía hincapié en la necesidad de respetar en todo caso las restricciones en el contenido de la información como si del sistema definitivo se tratara, así como las previsiones relativas a los informes sobre las consultas (artículo 16), las competencias de la ACC (artículo 24) y las medidas de seguridad (artículo 25).

Como aspectos particulares se mencionaban la necesidad de tener especial cuidado con los campos de texto libre, debiéndose establecer los controles necesarios para evitar que se deslice información no autorizada; la necesidad de tener en cuenta el Dictamen de la ACC-Europol sobre los *logs* de acceso; el respeto a las reglas de recepción y transmisión de información a terceros así como los Dictámenes de la ACC en esta área; la imposibilidad de añadir categorías de datos fuera de lo que prevé el Convenio y la necesidad de prestar especial atención a las cancelaciones de oficio.

El segundo se refería a una petición de informe preceptivo por parte de Europol respecto de un proyecto de Decisión sobre la elaboración de informes para la recuperación de datos personales en el Sistema de Información, conforme a la propuesta del Consejo de Administración de Europol.

El dictamen aprobado por el plenario de la ACC-Europol ponía de manifiesto que el mismo era conforme a lo establecido en el Convenio Europol si bien hacía hincapié en la necesidad de arbitrar algún método que garantice la posibilidad de conocer quien introdujo cada dato personal en el Sistema de Información y, por tanto, sería recomendable comenzar a trabajar en cómo esta disposición va a ser aplicada en todo el Sistema Informatizado de Europol.

Además, se añadía que en algunos casos no es suficiente con conocer si los datos personales de alguien fueron o no consultados, sino que resulta necesario saber qué datos específicos fueron accedidos por lo que si existen varios registros sobre la misma persona, se debe identificar cual de ellos fue objeto de examen.

Por último, también presentó un informe sobre la visita de trabajo realizada por el Subgrupo a Europol en la que les fue presentada la nueva política de Europol respecto al uso de la tecnología de la información con fines de análisis y el llamado Nuevo Concepto del Sistema de Análisis (NCSA).

El primer hecho relevante a tener en cuenta es que en ningún caso se trataba de procesar nuevos tipos o categorías de datos personales sino de utilizar aquellas herramientas de Tecnologías de la Información existentes en el mercado que pudiera ayudar a obtener una mayor eficiencia y fruto de las labores de análisis de Europol.

Puesto que las principales novedades del procedimiento consistían en la introducción de un nuevo paso en el proceso de análisis mediante el que se filtra la información que no se considera suficientemente relevante para introducirla en los ficheros de trabajo de análisis y en la unificación de la información en un formato homogéneo que facilite su posterior tratamiento, el Dictamen de la ACC-Europol fue favorable siempre y cuando se garantizaran los derechos de los ciudadanos en relación con los datos utilizados en la fase de análisis previo.

No obstante, dado que existe la intención por parte de la ACC-Europol de llevar a cabo una nueva auditoría en el año 2002, este sería un buen momento para revisar completamente este sistema y cerciorarse de que su funcionamiento está completamente alineado con lo que especifica el Convenio Europol.

4.1. Comité de Recursos

Previsto en el artículo 24, apartado séptimo, del Convenio Europol ya citado, el Comité de Recursos de la Autoridad común de control tiene por misión tramitar examinar y decidir sobre los recursos que se interpongan por los ciudadanos contra las resoluciones de Europol cuanto entiendan que ésta no ha atendido correctamente el ejercicio de sus derechos de acceso (artículo 19. 7 del Convenio) o de rectificación y cancelación (artículo 20. 4 del Convenio) de los datos de carácter personal.

Durante el año 2001, el Comité de Recursos ha abierto dos procedimientos que se encuentran pendientes de resolución.

El primero de ellos, Recurso 1/01, tiene origen en la queja presentada por un ciudadano británico que ejercitó su derecho de acceso solicitado a Europol que le remitiese información sobre posibles datos personales suyos que estuviesen almacenados en sus registros, contestando Europol que, conforme al artículo 19 del Convenio Europol y habiendo verificado sus archivos, no había tratado ningún dato relativo a su persona "al que sea posible acceder". Dicha denuncia fue admitida a trámite, encontrándose en la actualidad pendiente la decisión del Comité de la remisión por Europol de las alegaciones que le han sido solicitadas.

En cuanto al Recurso 2/02 obedece a una denuncia presentada por un ciudadano residente en Países Bajos, y reproduce casi con total exactitud el objeto del recurso anteriormente comentado, al recurrirse por el afectado una respuesta de idéntico tenor dada por Europol ante el ejercicio de su derecho de acceso. Este recurso se encuentra actualmente en la fase preliminar del procedimiento.

5. AUTORIDAD COMÚN DE CONTROL DEL SISTEMA DE INFORMACIÓN ADUANERO

Con el objetivo de contribuir a prevenir, investigar y perseguir las infracciones graves de las leyes nacionales en materia aduanera aumentado la eficacia de las administraciones aduaneras de los Estados miembros mediante la rápida difusión de información y la mejora de la cooperación entre las mismas, se estableció, mediante el Acto del Consejo 95/C 316/02, de 26 de julio de 1995 y en base al K.3 del Tratado de la Unión Europea, el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros (en adelante Convenio SIA)19.

El Convenio SIA, siguiendo la estructura del resto de instrumentos legales existentes en el marco del III Pilar, crea una Autoridad de Supervisión Común20, con la finalidad de supervisar el funcionamiento del Sistema de Información Aduanero y examinar todas las dificultades de aplicación o interpretación que puedan surgir en su funcionamiento.

Dicha Autoridad de Supervisión Común (en adelante ASC-SIA), celebró su sesión constituyente en el año 2001. En dicha sesión se procedió a discutir el Proyecto de Reglamento de la misma, que, a petición de la Presidencia del Consejo, había sido preparado con anterioridad en el seno del Grupo de Trabajo sobre Ficheros Policiales de los Comisionados Europeos de Protección de Datos, con objeto de agilizar la puesta en marcha de la ASC-SIA.

En dicha discusión se constató la necesidad de clarificar algunos puntos relativos al quórum y la aplicación de las reglas de mayoría en las votaciones así como la conveniencia de alinear en lo posible el nuevo reglamento con los ya existentes de Europol y Schengen.

No obstante, para que la ASC-SIA pudiera proceder al inicio de sus trabajos y obtener los medios necesarios para el correcto funcionamiento de los mismos, se procedió a la aprobación provisional y por unanimidad, del Proyecto de Reglamento.

Tras ello, se solicitó a las delegaciones que realizaran por escrito aquellos comentarios que juzgaran oportunos para proceder a la aprobación definitiva del nuevo texto en la próxima reunión, estando también prevista para la segunda reunión la elección de Presidente y Vicepresidente de la ASC-SIA.

6. EURODAC

El Reglamento (CE) Nº 2725/200021 del Consejo, de 11 de diciembre de 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín22, crea un sistema, denominado "Eurodac", cuya finalidad es ayudar a determinar el Estado miembro responsable, con arreglo al Convenio de Dublín, del examen de las solicitudes de asilo presentadas en los Estados miembros y, además, facilitar la aplicación del Convenio de Dublín en las condiciones que el mismo establece.

A efectos de la aplicación del Convenio de Dublín, resulta necesario determinar la identidad del solicitante de asilo y de las personas interceptadas con ocasión del cruce irregular de fronteras exteriores de la Comunidad. Además, resulta conveniente que cada Estado miembro pueda comprobar si los extranjeros ilegalmente presentes en su territorio han solicitado asilo en otro Estado miembro, siendo las impresiones dactilares un elemento de suma importancia para determinar la identidad exacta de dichas personas, para lo cual resulta necesario crear un sistema central que ofrezca la posibilidad de comparar sus datos dactiloscópicos.

Para ello, se crea una Unidad Central en la Comisión Europea que será la encargada de gestionar una base de datos central informatizada en la que se registrarán exclusivamente los datos especificados en el Reglamento que contienen, en particular, los dactiloscópicos.

Además, el Reglamento Eurodac, en su artículo 20, dispone que se creará una Autoridad Común de Control independiente que tendrá como misión controlar las actividades de la Unidad Central del Sistema Eurodac para garantizar que los derechos de las personas interesadas no sean vulnerados por el tratamiento o la utilización de los datos de que dispone la Unidad Central. Esta Autoridad Común de Control supervisará la legalidad de la transmisión de los datos personales de la Unidad Central a los Estados miembros y será competente para estudiar las dificultades que puedan plantearse con los controles efectuados por las autoridades nacionales de control y elaborar recomendaciones que permitan hallar soluciones comunes a los problemas que existan.

La Autoridad Común de Control estará integrada por, como máximo, dos representantes de las autoridades de control de cada Estado miembro, y se disolverá cuando se constituya el organismo de vigilancia independiente (Supervisor Europeo de Protección de Datos) mencionado en el artículo 286.2 del Tratado de las Comunidades Europeas que la sustituirá en sus funciones.

Durante el año 2001, la Dirección General de Extranjería e Inmigración del Ministerio del Interior notificó a la Agencia de Protección de Datos la solicitud recibida de la Comisión Europea para que se procediera al nombramiento de los representantes españoles en la Autoridad Común de Control con vistas a su constitución dado que se preveía que el sistema Eurodac estuviese operativo a lo largo del año 2002.

Dada que la Disposición Transitoria Primera (Tratamientos creados por Convenios Internacionales) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece que *"La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio"*, el Director de la Agencia de Protección de Datos procedió a notificar los nombramientos de los miembros españoles de dicha Autoridad al Director General de Extranjería e Inmigración para su traslado a la Comisión.

Por ello, se prevé que a lo largo de los primeros meses del año 2002 tenga lugar la convocatoria de la primera reunión de dicha Autoridad Común de Control.

7. GRUPO DE PROTECCIÓN DE DATOS EN TELECOMUNICA-CIONES (GRUPO DE BERLÍN)

Como es habitual, durante el 2001 se han celebrado dos reuniones del grupo de trabajo de protección de datos en telecomunicaciones (Bangalore, 15 y 16 de febrero de 2001 y Berlín, 28 de agosto de 2001) en las que se han elaborado dos documentos. El primero de ellos relativo a la privacidad e información de localización en los servicios de comunicaciones móviles y el segundo relativo a la protección de datos y voto electrónico en las procesos electorales públicos: elecciones al Parlamento y otros órganos gubernamentales.

El contenido de dichos documentos es el siguiente:

Posición Común sobre privacidad e información de localización en los servicios de comunicaciones móviles

Las redes de comunicaciones móviles generan y tratan, desde su implantación, información relativa a la localización de los usuarios a través de sus terminales móviles. El objeto de este tratamiento es el de establecer la comunicación con dichos terminales, por lo que la citada información reside únicamente en las redes de telecomunicaciones de los operadores, estando, en la mayoría de los países, sujetos a normativas muy estrictas que imponen el secreto de las telecomunicaciones. La precisión de la información sobre localización depende fundamentalmente del tamaño de las denominadas *"celdas"* definidas a la hora de diseñar e implantar las redes de comunicaciones móviles, también denominadas *redes celulares* .

En parte, obligados por disposiciones legales que imponen una localización más precisa de los terminales móviles en servicios de emergencia, los operadores de redes de telecomunicaciones móviles han comenzado a adaptar la infraestructura técnica de sus redes con el fin de facilitar dicha información. Ello supone, a corto plazo, que estas redes generarán una información mucho más precisa sobre la localización de los terminales móviles. En este sentido, los fabricantes de los equipos utilizados en estas redes han anunciado que con la tecnología actual es posible obtener resoluciones de hasta 5 metros utilizando sistemas asistidos de GPS (Sistemas de Posicionamiento Global). Al mismo tiempo, se prevé que el desarrollo del comercio electrónico sobre tecnología de comunicaciones móviles llevará a la aparición de numerosos servicios de valor añadido basados en el conocimiento de la localización precisa del usuario. Previsiblemente, estos servicios de valor añadido no serán proporcionados en exclusiva por los operadores de telecomunicación, sino también por terceros que pueden no estar sujetos a las obligaciones de secreto en las telecomunicaciones.

La mayor precisión de la información de localización y su disponibilidad para terceros, distintos de los operadores de las redes de telecomunicaciones móviles, puede llevar a la aparición de riesgos para la privacidad de los usuarios de estos servicios. Por este motivo, el Grupo de Trabajo cree necesario que la tecnología para la localización de los terminales móviles sea diseñada de forma que su impacto sobre la privacidad del usuario sea mínima.

En este sentido, se deberían tener en cuenta los siguientes aspectos:

* El diseño y la selección de los dispositivos técnicos que se vayan a utilizar para dichos servicios debe de realizarse con el objetivo de no recabar, ni tratar datos personales o, en su defecto, los mínimos posibles.

* La información precisa de localización no debería ser generada como una característica normal del servicio, sino exclusivamente *"previa petición"*, es decir, cuando sea necesario para proporcionar un determinado servicio que precise de la localización de los terminales móviles de los usuarios.

* El usuario debe de disponer del control sobre la información precisa de localización de su terminal que se vaya a generar. En este sentido, existen soluciones en las que la generación de esta información se realiza bajo control del terminal móvil del usuario, mientras que en otras soluciones la citada información se genera de forma automática bajo control de la propia red. Las primeras ofrecen un mayor grado de privacidad que las segundas, ya que en estas últimas el control del usuario se limita a decidir acerca de si la citada información será o no comunicada a terceros.

* Los usuarios deberían disponer de la posibilidad de inhibir la determinación de su localización precisa en cualquier instante, sin que para ello sea necesario desconectar el terminal de la red. También se debería permitir al usuario poder graduar el nivel de precisión de la información de localización que vaya a ser facilitada a terceros (por ejemplo, a nivel de edificio, calle, ciudad o estado).

* La información de localización debería estar disponible únicamente para los proveedores de servicios de valor añadido a los que el usuario haya prestado el correspondiente consentimiento informado. Este consentimiento puede estar restringido a una única transacción o a determinados proveedores de servicios de valor añadido. En relación con la información de localización, el usuario debería poder acceder a modificar y cancelar sus datos de configuración, incluso cuando estos datos no se encuentren almacenados en su terminal móvil sino dentro de la propia red.

* La creación por parte de los operadores de telecomunicaciones o de los proveedores de servicios de valor añadido de perfiles en base a los desplazamientos del usuario utilizando la información de localización debería ser prohibida por la Ley, a menos que sea necesario para proporcionar un determinado servicio y siempre que el usuario haya prestado un consentimiento inequívoco.

* Los datos de localización representan una información altamente sensible. Por este motivo, el acceso, tratamiento y comunicación de dicha información debería estar sujeta a los mismos controles que los establecidos para la información protegida por el secreto de las telecomunicaciones. En este sentido, el Grupo de Trabajo quiere hacer referencia a la Posición Común adoptada anteriormente por el Grupo y relativa a los Controles Públicos en relación con las Comunicaciones Privadas (Hong Kong el 15 de abril de 1998; disponible en http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm).

* Siempre que sea posible, los operadores de redes de telecomunicaciones móviles no deberían facilitar los datos de localización junto con los datos identificativos de los usuarios a los proveedores de servicios de valor añadido, debiendo sustituir los datos identificativos por seudónimos. La información de identificación personal (por ejemplo el identificador del terminal móvil) sólo debería estar disponible para los proveedores de servicios de valor añadido si se

dispone para ello del consentimiento informado del usuario. La información de localización debería ser cancelada una vez que haya dejado de ser necesaria para la prestación del servicio.

* El proveedor no debería poder condicionar la prestación de un servicio, ni los términos de dicha prestación, a que el usuario facilite su consentimiento para el tratamiento de su información personal de localización si ésta no es necesaria para la prestación de dicho servicio.

Documento de trabajo sobre Protección de datos y voto electrónico en las elecciones públicas (Parlamento y otros Órganos gubernamentales23)

Las nuevas tecnologías de telecomunicación, en particular Internet, pueden ser utilizadas como un medio adicional de votación en los procesos electorales, contribuyendo de esta manera a fomentar la participación ciudadana en dichos procesos, ya sea a nivel local, regional, nacional o supranacional. En este sentido, en diferentes foros públicos de debate empiezan a acuñarse términos como *"voto on-line"*, *"voto electrónico"* y *"e-democracy"*. Recientemente, diversos países han procedido a modificar su normativa electoral con el fin de incorporar la posibilidad de sistemas de voto electrónico. A modo de ejemplo, se han realizado experiencias en universidades para la elección de representantes estudiantiles a sus órganos de gobierno.

Básicamente, podemos clasificar los sistemas de voto electrónico en dos categorías:

* Sistemas de voto electrónico que utilizan equipos y programas informáticos certificados y ubicados en los colegios electorales (también denominados *"sistemas cerrados"* o sistemas *"end to end"*);

* Sistemas de voto electrónico que utilizan diferentes tipos de dispositivos de entrada, como por ejemplo ordenadores personales, teléfonos móviles, etc., junto con programas informáticos no certificados (también denominados *"sistemas abiertos"*).

Los sistemas de voto electrónico del tipo *"sistemas abiertos"* pueden dar lugar a una menor participación electoral de los ciudadanos que los sistemas del tipo *"sistemas cerrados"*, al no quedar garantizado el secreto del sufragio en el hogar o en lugar de trabajo al mismo nivel que en el colegio electoral.

En este contexto, cualquier tecnología que pretenda utilizarse debería de cumplir los requerimientos constitucionales básicos que rigen todo proceso electoral democrático. En este sentido, la libertad, la igualdad y el secreto de voto se constituyen como principios generalmente aceptados en los sufragios públicos. Al mismo tiempo, el procedimiento electoral debe ser transparente y sujeto a análisis público.

La confidencialidad del voto es fundamental en el caso de sufragios electorales para la elección de los miembros de parlamentos o de otros órganos institucionales y debe compaginarse con los principios de transparencia y auditoria del proceso electoral en su totalidad.

La experiencia de procesos electorales amañados o controlados en sociedades no democráticas pone en tela de juicio la confianza en los sistemas políticos. Los procedimientos electorales electrónicos no presentan la misma transparencia que los procesos electorales tradicionales con papeletas de voto, aunque los primeros puedan llegar a ser más seguros incluso que los segundos. Sin embargo, los procesos electorales no solo han de ser seguros sino que han de ser percibidos también como tales.

Determinados métodos de cifrado, como por ejemplo la *"firma ciega",* así como la segregación de tareas y funciones entre servidores, unos para comprobar el registro de votantes y otros diferentes para la recogida y recuento de votos, son aspectos objeto del debate actual. Si bien, la puesta en práctica de dichos aspectos puede resultar altamente compleja, no cabe duda que ayudaría a compensar la falta de transparencia.

Estas propuestas deberían ser estudiadas detenidamente y sometidas a debate público. Por ello, se hace necesario proceder con precaución dado que la confianza del votante es esencial en los procesos electorales democráticos. Las elecciones presidenciales celebradas en EEUU en 2000 ocasionaron un intenso debate público en relación con las nuevas tecnologías utilizadas en el mismo. Si las tecnologías implicadas en el proceso no resultan seguras, o frustran las expectativas del público en relación a la votación, recuento o al proceso de control, puede generarse desconfianza en la opinión pública.

Como consecuencia de lo expuesto, el Grupo de Trabajo quiere realizar las siguientes recomendaciones:

* La complejidad de los aspectos técnicos con respecto a la fiabilidad del proceso, incluyendo la seguridad y la disponibilidad de los sistemas de votación electrónica (protección contra los accesos no autorizados y los ataques de *"denegación del servicio"*), deberían ser resueltos como paso previo a su utilización en procesos electorales para la elección de representantes públicos. En este sentido, los sistemas utilizados deberían ser sometidos a procedimientos de análisis de riesgos y ser debidamente comprobados24.

* Los procedimientos utilizados en los procesos electrónicos con el fin de determinar si el elector tiene derecho de voto antes de permitirle su emisión, así como para evitar el cómputo múltiple del voto y asegurar al mismo tiempo el secreto del mismo, no deberían ser menos seguros que los procedimientos utilizados en los procesos tradicionales con papeletas.

* Los sistemas deberían informar al elector acerca de si su voto no ha sido registrado o transmitido correctamente. Se debería asegurar que la emisión del voto no genera ningún tipo de marca identificativa con el fin de reducir el riesgo de posibles injerencias sobre los electores, en base a si han ejercido o no el derecho de voto. No debería quedar constancia de que un elector ha emitido un voto una vez éste ha sido computado.

* Tanto los equipos como los programas de ordenador, incluidos los códigos fuentes de dichos programas, deberían ser convenientemente documentados y sometidos a análisis público.

* Deberían habilitarse procedimientos de certificación con las garantías suficientes, tanto para los equipos como para los programas informáticos utilizados en los procesos electorales electrónicos.

8. CONFERENCIA DE PRIMAVERA DE AUTORIDADES DE PROTECCIÓN DE DATOS (ATENAS, 10 Y 11 DE MAYO DE 2001)

La Conferencia de Primavera de los Comisionados Europeos de Protección de Datos la forman los Comisionados de la Unión Europea además de los representantes de las Autoridades de Control de Noruega, Islandia, Suiza, Hungría, República Checa y Polonia, así como de representaciones de la Comisión de las Comunidades Europeas y del Consejo de Europa. Se celebra anualmente en un país distinto y se ocupa del análisis de aquellos desarrollos legislativos o tecnológicos que pueden afectar a la privacidad de los ciudadanos europeos en aras de buscar soluciones armonizadas en dicho ámbito.

La correspondiente al año 2001 se celebró en Atenas, organizada por la Autoridad Griega de Protección de Datos y en la misma se trataron los siguientes temas:

* Desarrollos desde la última Conferencia de Primavera: seguimiento de las discusiones de Estocolmo y del cuestionario estadístico de actividades de las autoridades nacionales

* Crimen en el ciberespacio y protección de datos

* Protección de datos en el sector de las telecomunicaciones / Internet

* Protección de datos de los trabajadores

* Tecnologías de mejora de la privacidad (PET)

* La noción de "consentimiento" como base legal para la protección de datos

* Listas negras

* Comercio electrónico / Comercio de datos personales

* La "oficina electrónica" para la protección de datos

* Informe sobre los talleres relativos a la tramitación de reclamaciones en La Haya (octubre 2000) y Oslo (marzo 2001)

La delegación española contribuyó con dos ponencias a los trabajos de la conferencia, aparte de participar activamente en todos los debates de la misma, especialmente en los relativos a la protección de datos de los trabajadores, la noción del consentimiento como base legal para la protección de datos y en la discusión de las declaraciones de la Conferencia, en particular, en la configuración del derecho a la protección de datos personales como diferenciado del de la intimidad en la Carta de Derechos Fundamentales de la Unión Europea.

En concreto, el Director de la Agencia de Protección de Datos, pronunció una conferencia con el título "Comercio electrónico / Protección de datos", en la que presentó los resultados más relevantes del Plan de Inspección Sectorial realizado por la Agencia a cuarenta y cuatro empresas dedicadas al comercio electrónico a través de Internet.

En la misma se pusieron de manifiesto tanto la metodología empleada como los resultados obtenidos tras la realización de una inspección de oficio al sector del comercio electrónico.

El análisis se circunscribió a las entidades que comercian a través de la Red, por lo que las conclusiones mencionadas, se han obtenido como resultado de las actuaciones de inspección practicadas en las denominadas "tiendas virtuales", entendiendo como tales las *webs* que permiten al usuario la compra, directa o indirectamente, de un producto o servicio, de forma tal que la transacción comercial (a excepción de la entrega del bien adquirido) quede cerrada on-line, habiéndose analizado cuarenta y cuatro *webs* con estas características.

Entre las conclusiones de la auditoría merecen destacarse que se han detectado deficiencias en la información que se ofrece a los usuarios (un 27% no ofrece ninguna información en relación con la protección de datos personales) y en la notificación de los ficheros al Registro General de Protección de Datos (un 36% de las mismas no constaban como inscritas en el mismo).

Asimismo se ha detectado un cierto grado de deficiencia en lo que respecta a la identificación de los distintos respon-

sables de tratamientos que pueden concurrir cuando se lleva a cabo una transacción electrónica, a la satisfacción de los requisitos contractuales que marca la LOPD cuando se realizan tratamientos por encargo y a la información que se suministra cuando se comunican datos a terceras partes.

Por otro lado, también hay que hacer constar que se ha constatado un buen nivel de cumplimiento respecto del ejercicio de los derechos de acceso, rectificación, cancelación y oposición así como de la puesta en marcha de las medidas establecidas por el Real Decreto 994/1999, por el que se aprueba el Reglamento de medidas de seguridad para los ficheros que contengan datos de carácter personal.

Finalmente, hay que hacer constar que, como resultado de las conclusiones de la auditoría, la Agencia de Protección de Datos dirigirá unas Recomendaciones al Sector del Comercio Electrónico para conseguir una mejor adecuación de las prácticas en dicho sector a lo que establece la legislación de protección de datos personales.

Asimismo, D. Jesús Rubí Navarrete, Adjunto al Director de la Agencia de Protección de Datos, expuso una ponencia con el título "Protección de datos en el sector de las telecomunicaciones (modificación de la directiva 97/66/CE)", en la que informó sobre la experiencia española sobre la aplicación de algunos aspectos relevantes de la Directiva 97/66/CE con el fin de formular algunas reflexiones que pudieran ser útiles tanto para la incorporación de la Directiva al sistema jurídico de los Estados miembros como para el debate sobre la propuesta de una nueva Directiva en esta materia.

Además, la Conferencia aprobó por unanimidad dos declaraciones que se transcriben a continuación, la primera de ellas relativa a la retención de los datos de tráfico por los proveedores de servicios de Internet y la segunda sobre el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Declaración de la Conferencia Europea de Autoridades de Control de Protección de Datos sobre la retención de datos de tráfico por los Proveedores de Servicios de Internet (PSI)

La Conferencia de Primavera del año 2001 de Autoridades de Control Europeas de Protección de Datos Personales nota con creciente preocupación las propuestas relativas a que los PSI deban retener obligatoriamente y de forma rutinaria los datos de tráfico más allá de las necesidades derivadas de la facturación con el fin de posibilitar el acceso a los mismos por parte de las autoridades policiales competentes.

La Conferencia quiere poner de relieve su punto de vista, ya expresado en Estocolmo, de que sería una invasión impropia de los derechos fundamentales garantizados a las personas por el artículo 8 del Convenio Europeo de Derechos Humanos y en relación con lo dispuesto en 1981 por el Convenio del Consejo de Europa para la Protección de las personas en relación con el tratamiento automatizado de datos personales (Convenio 108). La Conferencia manifiesta que tal retención podría también invadir los derechos especificados en los artículos 8 y 7 de la Carta de Derechos Fundamentales de la Unión Europea. Cuando los datos de tráfico deban ser retenidos en casos específicos, debe haber una necesidad demostrable, el periodo de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la Ley.

Declaración de la Conferencia Europea de Autoridades de Control de Protección de Datos sobre el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea

La Conferencia de Primavera de Autoridades de Control Europeas de Protección de Datos Personales constata con satisfacción que el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea refuerza las previsiones sobre protección de datos que han sido establecidas en los últimos años de tal manera que, finalmente, la protección de datos personales ha sido reconocida como un derecho fundamental.

Se ha establecido un verdadero "modelo europeo" de protección de datos. Este modelo está determinando el rumbo de los debates de la comunidad internacional y debería influir positivamente en la difusión de un entendimiento de la protección de datos como un derecho humano fundamental y un componente básico de la ciudadanía electrónica.

Este modelo de protección de datos personales debería servir como directriz para todas las instituciones de la Unión Europea cuando se revise la legislación existente y se desarrollen nuevas reglas así como para guiar sus relaciones con terceros países. La Conferencia quisiera llamar la atención de la Comisión y el Parlamento sobre este importante requerimiento.

9. ENCUENTRO DE REPRESENTANTES DE LAS AUTORIDADES DE CONTROL EUROPEAS RELATIVO AL TRATAMIENTO Y TRAMITACION DE RECLAMACIONES

En el transcurso del pasado año 2001, la Agencia de Protección de Datos Española ha asistido a las dos reuniones anuales convocadas por el Grupo de Tratamiento y Tramitación de Reclamaciones que han tenido lugar en Oslo –marzo de 2001- y Lisboa –noviembre de 2001-. En cada ocasión la reunión se celebra en un país distinto.

El Grupo de reclamaciones se creó a instancias de la Conferencia de Primavera de Autoridades de Protección de Datos, concretamente en la Conferencia de Primavera celebrada en Helsinki en abril de 1999. El Grupo de Reclamaciones informa periódica y anualmente en dicha Conferencia a los Comisionados Europeos acerca de sus actividades, encuentros y avances.

A dichos encuentros se invita a representantes de los Comisionados de Protección de Datos de la Unión Europea, así

como a representantes de las Autoridades de Control de Noruega, Islandia y Suiza, además de representación de la Comisión de la Unión Europea.

El Grupo de Reclamaciones se reunió por primera vez en febrero de 2000 en Manchester. La segunda reunión se celebró en La Haya en octubre de 2000.

El objetivo primordial de tales encuentros es el de intercambiar información, experiencias y métodos en la tramitación de las quejas y denuncias que se reciben en las distintas Autoridades de Control. A tal efecto, se creó una página web denominada "CIRCA" –página web creada para el intercambio de información sobre casos relativos a reclamaciones internacionales- No obstante, junto con este "tema-estrella" que encabeza y ocupa gran parte del tiempo de tales encuentros, otros temas han ocupado la actividad del Grupo en las reuniones mantenidas hasta el momento:

* Análisis y explicación detallada del contenido de las distintas páginas web de las distintas Autoridades de Control.

* Internet y la amenaza que puede representar a la privacidad de los individuos, especialmente a los menores de edad.

* Tratamiento de datos en Internet.

* Protección de datos en el ámbito laboral, en especial en lo relativo a la vigilancia y control de las comunicaciones electrónicas de los trabajadores.

La próxima reunión del Grupo de Reclamaciones tendrá lugar en Dublín el próximo mes de marzo de 2002. En dicha reunión se hará un seguimiento a los temas ya tratados en anteriores reuniones, y mencionados anteriormente, y se presume la incorporación de nuevos asuntos del máximo interés para las distintas Autoridades de Control.

10. CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS (PARÍS, 24 A 26 DE SEPTIEMBRE DE 2001)

Una vez al año, las Autoridades de Control de Protección de Datos de todo el mundo se reúnen para pasar revista a los desarrollos tecnológicos y jurídicos que han influido más poderosamente en la evolución de la protección de datos en los doce meses anteriores así como para identificar y analizar las tendencias de futuro en esta materia. Para ello, las Conferencias Internacionales de Autoridades de Protección de Datos proporcionan el entorno adecuado para la reflexión y el intercambio de ideas y experiencias más relevantes de cada uno de los participantes.

En el año 2001, la Conferencia Internacional se celebró en París. Los temas más relevantes sobre los que se debatió fueron los siguientes:

* El tercer milenio o la odisea tecnológica
* Biometría y reconocimiento facial
* Técnicas de localización
* Protección de datos y de la privacidad: la pedagogía a debate
* Cibercrimen y cibervigilancia: por una ciberciudadanía
* Vida privada – Vida laboral
* Salud en el corazón de los ficheros
* Democracia electrónica
* Tecnologías para la protección de la privacidad
* Cambios en las compañías, personalización de los servicios
* Compañías y protección de datos personales: ¿Qué iniciativas y que organización para asegurar la confianza?
* Un mundo, una privacidad

La delegación española participó activamente en todos los trabajos de la Conferencia y realizó diversas sugerencias sobre las Resoluciones de la misma que se incluyeron, por acuerdo unánime, en el texto final de las mismas.

La Conferencia aprobó por unanimidad dos Resoluciones que tenían como objetivo fundamental dotar a la Conferencia de unas reglas claras y precisas para tramitar la admisión de nuevas autoridades de control como miembros u observadores de la misma así como proporcionar un mecanismo de aprobación de documentos para el futuro.

La primera de ellas fue la "Resolución sobre el procedimiento de acreditación de autoridades de protección de datos personales en la Conferencia Internacional de Autoridades de Protección de Datos". Mediante la segunda Resolución, se procedió al nombramiento de los Comisionados de Protección de Datos de Nueva Zelanda, Reino Unido y Francia como miembros del Comité de Acreditación creado en la Resolución antes mencionada25.

11. SEGUNDO ENCUENTRO IBÉRICO DE PROTECCIÓN DE DATOS

En el año 2000 se celebró en la ciudad portuguesa de Évora el Primer Encuentro Ibérico de Autoridades de Control de Protección de Datos en el que participaron delegaciones de las autoridades española y portuguesa, del que se informó en la anterior memoria. En dicho Encuentro se acordó, ya que ambas partes estimaron el mismo sumamente útil, proseguir la celebración anual de los mismos siendo la Agencia de Protección de Datos la encargada de organizar el Segundo Encuentro Ibérico, que tuvo lugar en la ciudad de Cáceres los días 29 y 30 de noviembre de 2001.

Ambas delegaciones, encabezadas por el D. Luis Lingnau da Silveira, Presidente de la Comissão Nacional de Protecção de Dados y por D. Juan Manuel Fernández López, Director de la Agencia de Protección de Datos, debatieron durante los dos días que duró el Encuentro sobre la utilización del correo electrónico e Internet en el lugar de trabajo y sus implicaciones para la protección de datos, el comercio electrónico y la protección de datos personales, los problemas derivados de la transferencia de datos entre ambos países como consecuencia de fusiones o de relaciones entre empresas del mismo grupo y sobre los ficheros de solvencia patrimonial y crédito.

Al término de las sesiones, se procedió a redactar unas conclusiones del Encuentro que fueron aprobadas por las dos delegaciones y distribuidas a los medios de comunicación que asistieron a la rueda de prensa que puso fin a los trabajos del Encuentro.

Por su interés, a continuación se incluyen las conclusiones del Encuentro.

SEGUNDO ENCUENTRO IBÉRICO DE AUTORIDADES DE PROTECCIÓN DE DATOS
Cáceres, 29 y 30 de noviembre de 2001

Las Autoridades portuguesa y española de Protección de Datos, reunidas los días 29 y 30 de noviembre en la ciudad de Cáceres, pasaron revista a diversos aspectos relevantes en el ámbito del derecho fundamental a la protección de datos personales en relación con los nuevos desarrollos de la Sociedad de la Información y con distintos aspectos de las relaciones económicas entre ambos países que tienen una importante repercusión en la privacidad de los ciudadanos portugueses y españoles.

Ambas autoridades (Comisión Nacional de Protección de Datos de Portugal y Agencia de Protección de Datos de España) son conscientes de la gran importancia que en un mundo cada vez más globalizado han cobrado los intercambios de datos personales en el ámbito internacional y la ineludible necesidad de incrementar la cooperación entre las autoridades a las que las leyes encomiendan el velar por los derechos de los ciudadanos en relación con la protección de sus datos personales.

En el ámbito europeo e internacional, las dos Autoridades constataron la existencia de puntos de vista comunes y consideraron urgente la adopción de medidas para una efectiva armonización práctica que, incluso en el espacio europeo, se encuentra lejos de ser alcanzada. Esta necesidad de armonización se ha visto, si cabe, incrementada, tras la solemne proclamación de la Carta de Derechos Fundamentales de la Unión Europea en la que se consagra, explícitamente, la protección de datos personales como un derecho fundamental de los ciudadanos europeos.

Durante las sesiones se analizaron las repercusiones que para la protección de datos personales se derivan de la utilización del correo electrónico y el acceso a Internet por parte de los trabajadores en el lugar de trabajo, del auge creciente del comercio electrónico y de las transferencias de datos personales entre ambos países como consecuencia de las fusiones y absorciones entre empresas portuguesas y españolas y de la pertenencia a los mismos grupos empresariales de sociedades de ambos países. Finalmente, se trataron los problemas que plantean los ficheros de solvencia patrimonial y crédito en relación con la inclusión de los datos personales de aquellos ciudadanos que no han cumplido con sus obligaciones de pago en el momento adecuado.

Por lo que respecta a la utilización del correo electrónico y el acceso a Internet por parte de los trabajadores, se constató que el marco legal, tanto constitucional como laboral y de protección de datos, es similar en ambos países por lo que las respuestas a los problemas derivados de la colisión del derecho a la intimidad de los trabajadores y del derecho a la dirección, supervisión y control de las actividades de la empresa por parte del empresario han de ser, necesariamente, también similares. En concreto, se constató que, respetando en todo caso la dignidad e intimidad del trabajador y el derecho de los representantes de los trabajadores a informales de aquellos temas que sean de su competencia, el empresario puede dictar las normas que regulen la utilización de estas herramientas e, incluso, prohibir su uso privado. En todo caso, se deberá proporcionar información clara y transparente a los trabajadores de las medidas de supervisión y control que se vayan a adoptar y de las finalidades de dichas medidas. También habrá de respetarse lo que la legislación laboral establezca respecto al derecho de los representantes de los trabajadores a ser oídos cuando se adopten nuevas medidas de vigilancia y control. Sería recomendable que los empresarios regularan la utilización de estos medios por parte de los trabajadores para promover su mejor formación y el acceso a aquellas informaciones y herramientas que redunden en su desarrollo personal, social y profesional.

Respecto al comercio electrónico, teniendo en cuenta las actividades de ambas autoridades en el último año, se tomó nota de los principales problemas detectados en el sector: falta de identificación clara del responsable de los tratamientos de datos en los servidores web a través de los que se realizan las transacciones electrónicas; la no indicación de cambio de servidor al seguir un hiperenlace que, incluso, puede llevar a un servidor situado fuera de la Unión Europea; las grandes deficiencias de la información suministrada al ciudadano y, en particular, respecto a la utilización de cookies.

Por otro lado, también se constató que ha pasado mucho tiempo entre la aprobación de la Directiva de Protección de Datos Personales en el año 1995 (Directiva 95/46/CE) y la Directiva de Comercio Electrónico (Directiva 2000/31/CE) por lo que la remisión que ésta hace a las normas de protección de datos de la primera puede conducir a una falta de adecuación de las mismas a las nuevas realidades. En concreto, a aquellos riesgos derivados de la gran facilidad en la realización de perfiles detallados de las personas para poder realizar una oferta personalizada y diferenciada.

En lo que respecta a las transferencias de datos entre España y Portugal con motivo de las fusiones y absorciones empresariales y las derivadas de la pertenencia al mismo grupo empresarial de compañías de ambos países, se puso de manifiesto que dado que tanto Portugal como España son miembros de la Unión Europea están vinculados por las disposiciones sobre libre circulación de personas, mercancías y capitales presentes en los Tratados de las Comunidades Europeas y, como consecuencia inmediata de ello, sobre la libre circulación de datos personales dentro del mercado interior. Esta libre circulación se basa en la existencia de un nivel equivalente de protección de datos en todos los Estados miembros derivado tanto de sus propias tradiciones constitucionales como de las leyes específicas que regulan esta materia y, especialmente, por aquellas normas de Derecho nacional que transponen la Directiva 95/46/CE. No obstante, sí que es posible que las autoridades de control cooperen entre sí para que, en el momento de recibir una notificación preceptiva de que se va a producir una transferencia, puedan adoptar las medidas necesarias para garantizar una mejor defensa de los derechos de los ciudadanos de ambos países.

Para poder precisar esta posibilidad, también se pasó revista a los distintos supuestos de fusión y absorción de empresas y a las consecuencias que para la existencia de comunicación o cesión de datos personales tienen los distintos modelos. Los factores determinantes para decidir sobre este hecho serían la creación o no de nuevas personas jurídicas, el aumento o no del número de usuarios, la alteración de la actividad que resulta de la fusión y la existencia de un cambio en la finalidad o finalidades para las que se tratan los datos.

Finalmente, en el apartado de ficheros de morosos y en el caso español, se analizaron las sentencias que sobre las resoluciones de la Agencia de Protección de Datos en este sector se han producido en el año 2001. La problemática que se abordó en el análisis fue la obligación de notificación al interesado de su inclusión en uno de estos ficheros y el cumplimiento del principio de calidad de datos tanto cuando los datos provienen de fuentes accesibles al público como cuando la información es suministrada por el acreedor, haciendo especial hincapié en los plazos en los que las actualizaciones deben hacerse efectivas.

Posteriormente, se hizo una mención particular respecto a la imposibilidad de mantener en dichos ficheros datos adversos una vez que la deuda ha sido pagada, hecho este derivado de las modificaciones introducidas en esta materia por la nueva Ley Orgánica de Protección de Datos Personales y la Sentencia número 292/2000 del Tribunal Constitucional.

En el caso de Portugal, la constitución de ficheros sobre solvencia patrimonial y crédito está sujeta a una autorización previa de la Comissão Nacional de Protecção de Dados para cuya concesión se estudia especialmente la información que el responsable proporciona a los ciudadanos y los periodos de permanencia de la información en dichas bases de datos. La legalidad de la inclusión de datos en estos ficheros puede derivarse del consentimiento del ciudadano (que es poco habitual en este sector), de la existencia de cláusulas contractuales o de que esté previsto por una disposición legal que lo permita.

Respecto de los casos más relevantes en Portugal, se mencionaron las decisiones de la Comisión portuguesa declarando insuficiente la información que se proporcionaba a los afectados a través de carteles poco visibles en las líneas de cajas de los hipermercados y declarando ilícito el mantenimiento de la información respecto de cheques sin fondos, por parte de las entidades financieras, más allá de los dos años que marca la ley reguladora en la materia. También se puso de manifiesto que no es posible mantener en estos ficheros datos relativos a deudas que ya hayan sido saldadas y que en el caso de deudas que están siendo discutidas judicialmente, deberán de tomarse las medidas necesarias para incluir el punto de vista del interesado en los datos referentes a la deuda.

A la finalización de las dos jornadas de trabajo, ambas autoridades de control han decidido de común acuerdo continuar en el futuro con estos encuentros, ya que han constatado la utilidad práctica del intercambio de ideas y experiencias que se ha producido que, junto con la puesta en marcha de varias iniciativas aprobadas durante la reunión, redundarán en una mejor cooperación e intercambio de información entre las mismas.

12. OTRAS ACTIVIDADES DE ÁMBITO INTERNACIONAL

12.1. Países del Centro y Este de Europa

La ampliación de la Unión Europea a los países del Centro y Este de Europa es uno de los retos más importantes de la construcción europea. La Agencia de Protección de Datos es consciente de este hecho así como de la necesidad de cooperar con dichos países para que el entorno jurídico y la práctica real en materia de protección de datos se ajusten a lo que se ha dado en llamar "acervo comunitario" de tal forma que la integración de estos países y su adaptación a las exigencias de la Unión Europea en este campo se lleve a cabo en las mejores condiciones posibles.

Fruto de este interés es la colaboración continuada con varios países del Centro y Este de Europa, revistiendo una especial importancia el que se está llevando a cabo con la República Checa.

En el año 2001, la Comisión Europea adjudicó a la Agencia de Protección de Datos el Proyecto de Hermanamiento entre la misma y la Oficina Checa de Protección de Datos, creada en el año 2000, dentro del programa PHARE, que busca el que organismos de los países candidatos se beneficien de la experiencia práctica directa de otros organismos similares de un Estado miembro.

El aspecto más relevante del Proyecto de Hermanamiento lo constituye la presencia de un miembro de la Agencia de Protección de Datos, trabajando durante un año en la Oficina Checa de Protección de Datos, en calidad de Consejero

Pre-adhesión, con la misión de proyectar la experiencia de la Agencia española en el proceso de puesta en marcha de la Autoridad de Control checa, analizar la legislación y práctica checas, aportando su punto de vista, y la coordinación de todas las actividades previstas en el proyecto.

El proyecto incluye además la realización de seminarios, talleres y conferencias en la República Checa, tanto generales como sectoriales, con la presencia de destacados expertos españoles y comunitarios en la materia así como la realización de varias visitas de trabajo de miembros de la Oficina checa a la Agencia española para conocer *in situ* el trabajo real que la misma lleva a cabo en los ámbitos de inscripción de ficheros, inspección, tramitación de reclamaciones, tutela de lo derechos, difusión e información.

En relación con Polonia, en la anterior Memoria de la Agencia de Protección de Datos se informó de las sendas visitas de trabajo realizadas en por sendas delegaciones polacas y españolas a ambas autoridades de control, la Agencia de Protección de Datos y la Inspección General de Protección de Datos polaca en el año 2000.

Durante el año 2001 se han seguido manteniendo contactos regulares con la Inspección General polaca sobre diversos temas de interés común y, además, como ya se ha informado en el apartado correspondiente al Consejo de Europa, el Director de la Agencia de Protección de Datos participó como ponente en la Conferencia sobre el presente y el futuro del Convenio 108 que la Inspección General, conjuntamente con el Consejo de Europa, organizaron en Varsovia en noviembre de 2001.

En el marco de otro proyecto, la Agencia de Protección de Datos fue invitada a impartir un seminario de tres días de duración en el Ministerio del Interior de Bulgaria.

Durante el mismo se pasó revista a la legislación comunitaria de protección de datos, tanto en el Primer como en el Tercer Pilar, presentando los aspectos esenciales de la misma y la especial regulación aplicable a los tratamientos de datos personales realizados en el marco de la actividad policial además de los Convenios europeos encaminados a mejorar la cooperación en este terreno.

El seminario se completó con una exposición de la situación en España desde el punto de vista jurídico y práctico, presentando las actuaciones que la Agencia de Protección de Datos ha venido realizando en este campo a lo largo de los años.

Asimismo, con anterioridad a la celebración de dicho seminario, una delegación del Ministerio del Interior búlgaro, encabezada por el Sr. Elenkov, actual Director General de Coordinación e Información, realizó una visita de trabajo a la Agencia de Protección de Datos a solicitud de las autoridades españolas del Ministerio del Interior.

El Director de la Agencia de Protección de Datos recibió a la delegación y se mantuvo una reunión en la que los miembros de la delegación búlgara plantearon aquellas cuestiones, fundamentalmente relacionadas con las soluciones o previsiones legales existentes en España para aquellas situaciones que les resultaban más complicadas pensando en la introducción de legislación de protección de datos en su país y, especialmente, aquellas normas aplicables a la investigación policial.

12.2. Iberoamérica

Respecto a otros ámbitos geográficos, ya en anteriores memorias se ha puesto de manifiesto el interés con que la Agencia de Protección de Datos ha seguido el desarrollo de iniciativas en este campo en los países de Iberoamérica, con los que España mantiene una muy especial relación.

El año 2001 ha sido muy fructífero pues en el se produjo la visita del Director de la Agencia de Protección de Datos a dos países iberoamericanos, en los que se mantuvo contactos al más alto nivel.

En primer lugar y respondiendo a una invitación del Gobierno argentino, una delegación de la Agencia de Protección de Datos, presidida por su Director viajó a dicho país en el que tuvo ocasión de reunirse con el Ministro de Justicia y con destacados representantes de dicho Ministerio, del Tesoro y del Ministerio de Economía. En estos encuentros, los representantes argentinos mostraron un gran interés por conocer la experiencia española y tuvieron ocasión de realizar numerosas preguntas para aclarar todos aquellos aspectos que resultaban de su interés. También anunciaron al Director la preparación de un Decreto de desarrollo de la Ley de Habeas Data que estaba en preparación y cuyo borrador remitirían a la Agencia de Protección de Datos para recibir comentarios. Dicho Decreto fue aprobado y publicado posteriormente, el día 3 de diciembre, en el Diario Oficial de la República Argentina, en lo que constituye un hito importantísimo, ya que, además de desarrollar otros preceptos de la Ley, regula la creación de la autoridad de control argentina, la Dirección Nacional de Protección de Datos, lo que significa un gran paso en la garantía de los derechos de los ciudadanos de aquel país. Posteriormente, en las primeras semanas del año 2002, fue nombrado primer Director de dicha Autoridad el Dr. D. Juan Antonio Travieso, Profesor Titular de Derechos Humanos y Titular de Derecho Internacional Público en la Universidad de Buenos Aires.

Además, como complemento a estas actividades a puerta cerrada, el Director de la Agencia de Protección de Datos pronunció una conferencia pública sobre "Protección de datos personales. Experiencia española y comunitaria".

Asimismo, respondiendo a otra invitación del Instituto Paraguayo de Derecho Constitucional y teniendo en cuenta que recientemente había entrado en vigor una Ley sectorial sobre protección de datos personales en el sector de la información crediticia, la delegación de la Agencia de Protección de Datos visitó también Paraguay, dónde mantuvo varias

reuniones con el Presidente de la Corte Suprema, el Presidente del Congreso Nacional, el Ministro para la Reforma y diversos expertos y personalidades de la vida académica y empresarial.

Por otra parte, tanto el Director como el Adjunto al Director de la Agencia de Protección de Datos participaron en un Seminario Internacional organizado por el Instituto Paraguayo de Derecho Constitucional, el Centro Interdisciplinario de Derecho Social y Economía Política (CIDSEP) de la Universidad Católica de Paraguay y la Fundación "Konrad Adenauer" bajo el lema "Protección de la Información de Carácter Privado" en el que impartieron sendas conferencias sobre la experiencia de la Agencia de Protección de Datos española y los principios y derechos de protección de datos en España y la Unión Europea.

12.3. Estados Unidos de América

Unos meses después de la entrada en vigor del mecanismo de adecuación basado en los Principios de Puerto Seguro publicados por el Departamento de Comercio de los Estados Unidos, una vez que una Decisión de la Comisión que les otorgaba dicho *status*, una delegación de dicho Departamento, al frente de la cual estaba el Sr. Charles Ludolph, Deputy Assistant Secretary for Europe, visitó la Agencia de Protección de Datos para conocer los criterios y métodos empleados por la Agencia en el tratamiento de las transferencias internacionales de datos personales en general y de aquellas acogidas al Puerto Seguro en particular.

Durante dicha visita se produjo una reunión de trabajo en la que se comunicó al Sr. Ludolph la publicación de la Instrucción 1/2000, de la Agencia de Protección de Datos en la que se pretendía informar a todos los interesados, de una manera sistemática, del complejo marco de las transferencias internacionales y de los criterios seguidos por la Agencia en esa materia.

En el transcurso de dicha visita, además de acordar mantener informado al Departamento de Comercio, a través de la Embajada de los Estados Unidos en España, de cualquier desarrollo que se produjera en este campo, en el cual el Gobierno de los Estados Unidos estaba muy interesado, el Sr. Ludolph invitó al Director de la Agencia de Protección de Datos a visitar los Estados Unidos para poder comprobar de una forma directa el funcionamiento y las garantías existentes en la gestión del sistema de Puerto Seguro y para poder mantener una serie de contactos con aquellas personas y sectores, tanto públicos como privados, con mayores inquietudes en materia de protección de datos.

La visita estaba previsto realizarla a mediados del mes de septiembre e incluía toda una serie de encuentros con responsables de la Administración americana, el Congreso, representantes de las más importantes firmas del sector financiero y de los organismos de autocontrol privados encargados de la aplicación de los principios de Puerto Seguro.

Finalmente, dicho viaje no pudo llevarse a cabo debido a los trágicos sucesos del 11 de septiembre por todos conocidos, por lo que ha sido pospuesto hasta encontrar una fecha adecuada para ambas partes.

12.4. Cooperación con la Autoridad de Control sueca

A pesar de que las autoridades de control europeas mantienen estrechos y frecuentes contactos, tanto formales como informales, dadas las diferentes tradiciones jurídicas y las diferencias que aun subsisten en la práctica de las mismas, resulta de gran interés poder mantener contactos bilaterales con otras autoridades europeas con vistas a profundizar el conocimiento mutuo y, de esa manera, promover una cooperación más efectiva.

En este sentido, en el mes de mayo del año 2001 se produjo una visita oficial de trabajo de tres días de duración de la Sra. Birgitta Åbjörnsson, Asesora Legal Internacional de la Autoridad de Control sueca (Datainspektionen).

El objetivo de la misma era conocer las similitudes y diferencias tanto jurídicas como prácticas en las actividades de ambas autoridades de control. Durante los tres días que duró la visita, la Sra. Åbjörnsson mantuvo reuniones de trabajo con todas las unidades de la Agencia de Protección de Datos. En ellas, tanto la Sra. Åbjörnsson como los representantes de la Agencia presentaron las líneas fundamentales de trabajo en el área de que se trataba y a continuación profundizaban en los detalles prácticos para llegar a un mutuo entendimiento de los procedimientos y las diferencias existentes entre ambas autoridades.

1 Todos los documentos aprobados por el Grupo de Trabajo se pueden encontrar en http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.
2 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
3 Dicho representante actuará en nombre de la autoridad responsable de las cuestiones relacionadas con la protección de datos dentro de las instituciones europeas, de conformidad con lo establecido en el Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de estos datos.
4 El Grupo de Trabajo del artículo 29 ha aprobado mediante Decisión 1/2001 de 13 de diciembre del pasado año 2001 la posibilidad de que representantes de las Autoridades de Control de los 13 países candidatos a la UE participen, previa invitación, en calidad de observadores en las reuniones del Grupo.
5 El Comité del artículo 31 de la Directiva 95/46/CE se compone de representantes de los Estados miembros y es presidido por un representante de la Comisión. Su principal función es la de emitir dictamen sobre los proyectos de medidas que le presenta la Comisión.

6 Se puede consultar en http://conventions.coe.int/treaty/EN/cadreprincipal.htm
7 Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
8 Véanse letras a) y c) del apartado 1 del artículo 4 de la Directiva 95/46/CE.
9 En este punto debe ser mencionado nuevamente el Reglamento 45/2001/CE, de 18 de diciembre de 2000, del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos
10 Una versión *on-line* de esta Decisión puede consultarse en http://europa.eu.int/eur-lex/pri/es/oj/dat/2001/l_181/l_18120010704es00190031.pdf
11 Una versión *on-line* de esta Decisión puede consultarse en http://europa.eu.int/eur-lex/es/dat/2002/l_006/l_00620020110es00520062.pdf
12 El texto del Protocolo Adicional puede encontrarse en http://conventions.coe.int/Treaty/EN/Treaties/Html/181.htm
13 Tanto el Convenio Europol como el resto de la normativa reguladora de Europol puede encontrarse en http://www.europol.eu.int/content.htm?legal/conv/es.htm.
14 Véase el artículo 14 del Convenio Europol
15 Para una descripción detallada de estos subgrupos, consultar la Memoria correspondiente al ejercicio de 2000. En la actualidad existen los subgrupos de Procedimientos, Órdenes de Creación de Ficheros de Análisis, Publicidad, Inspección y Nuevos desarrollos (TI).
16 Las Órdenes de Creación y los datos asociados a las mismas son información clasificada, por lo que no es posible dar más detalles sobre este asunto en este documento.
17 Véase el artículo 18.2 del Convenio Europol y el artículo 5.1 de la Decisión del Consejo 2000/C 106/01, de 27 de marzo de 2000, por la que se autoriza al Director de Europol a entablar negociaciones sobre acuerdos con terceros Estados y organismos no relacionados con la Unión Europea.
18 Véase el artículo 18.2 del Convenio Europol y artículo 2.1 del Acto del Consejo 1999/C 88/01, de 12 de marzo, por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros
19 Para una descripción de los aspectos fundamentales del Convenio SIA en materia de protección de datos, véase este apartado de la Memoria de la Agencia de Protección de Datos correspondiente al año 2000. El texto del Convenio SIA puede encontrarse en http://europa.eu.int/eur-lex/es/lif/dat/1995/es_495A1127_02.html.
20 Véase el apartado 1 del articulo 18 del Convenio SIA.
21 Véase http://europa.eu.int/eur-lex/pri/es/oj/dat/2000/l_316/l_31620001215es00010010.pdf para consultar una versión *on-line* del Reglamento Eurodac
22 Publicado, junto con el Instrumento de Ratificación, en el B.O.E. núm 183, de 1 de agosto de 1997. Una versión *on-line* del mismo se puede consultar en http://europa.eu.int/eur-lex/es/lif/dat/1997/es_497A0819_01.html
23 El alcance de este documento se circunscribe a los procesos electores en los que se eligen representantes públicos. Los términos "Órganos gubernamentales" engloban a las tres ramas del poder: legislativo, ejecutivo y judicial.
24 Recientes investigaciones realizadas en EEUU prevén que hasta dentro de aproximadamente diez años no se habrá alcanzado este objetivo; Ver informe del Instituto Tecnológico de California / Instituto Tecnológico de Massachusetts denominado *"Voting Technology Project, Voting – What Is –What Could Be",* de julio de 2001 disponible en: http://www.vote.caltech.edu/Report/index.html.
25 Los textos de ambas resoluciones se pueden consultar en http://www.paris-conference-2001.org/eng/contribution/Resolution/closed_session.html

MEMORIA DE 2001 - OTRAS ACTIVIDADES

1. **COLABORACION CON OTRAS ENTIDADES.**

En el ámbito institucional la Agencia de Protección de Datos mantiene una relación constante con el Defensor del Pueblo y con la Agencia de Protección de Datos de la Comunidad de Madrid. En el primer caso, como consecuencia de la obligación legal de comunicar al Defensor del Pueblo las resoluciones dictadas respecto de responsables de ficheros de titularidad pública y, en el segundo, debido a la necesidad de mantener una estrecha colaboración entre dos Entidades que tienen una finalidad común, como es la de velar por el cumplimiento de la normativa de protección de datos personales.

En el año 2001 se ha mantenido la tradición por parte del Director de la Agencia de presentar personalmente la Memoria anual al Defensor del Pueblo, informándole de los principales aspectos de la misma e intercambiando opiniones sobre ambas instituciones.

Asimismo han continuado las actividades de coordinación con la Agencia de Protección de Datos de la Comunidad de Madrid mediante el intercambio de información y la participación conjunta en diversos seminarios y foros públicos. En este sentido merece una mención específica la presentación realizada por el órgano autonómico de Protección de Datos del Proyecto "Data Prot" para la formación en materia de protección de datos que, ulteriormente, fue objeto de comunicación en la Conferencia Internacional celebrada en París.

Respecto de las Universidades se han mantenido las actuaciones dirigidas al cumplimiento de los objetivos contemplados en la memoria del año anterior: resolución de sus problemas como responsables de ficheros, participación en "masters" especializados y realización de prácticas de sus alumnos en la sede de la Agencia. En este último aspecto se han ampliado los convenios de colaboración mediante la suscripción del correspondiente documento con la Universidad Carlos III de Madrid.

La Agencia de Protección de Datos ha continuado desarrollando relaciones con Corporaciones de Derecho Público tales como las Cámaras Oficiales de Comercio, Industria y Navegación y los Colegios Profesionales. Así, se han llevado a cabo las previsiones contenidas en los Protocolos suscritos con el Consejo Superior de Cámaras y con la Unión Profesional de los que ya se informaba en la Memoria del año 2000.

No obstante, se han ampliado las reuniones mantenidas con algunos Colegios que presentan problemas específicos respecto de la protección de datos personales, como son, particularmente, los vinculados a profesiones que implican el tratamiento de datos de salud.

En el año 2001 se ha incrementado la colaboración con otras Administraciones Públicas para resolver dudas y facilitar el adecuado cumplimiento de la LOPD. A este respecto destacan las relaciones mantenidas con el Ministerio del Interior, el Instituto Nacional de Estadística, la Consejería de Administración y Servicios del Gobierno Vasco, así como con diversas Corporaciones Locales.

Especial mención merece la colaboración llevada a cabo con la Fiscalía General del Estado respecto de los ficheros de que ésta es titular; así como la mantenida con el Tribunal de Defensa de la Competencia sobre cuestiones en las que ambas instituciones ostentan competencia.

La actividad de colaboración realizada por la Agencia se ha extendido, igualmente, a instituciones internacionales. De ellas se da cuenta en el apartado específico de esta Memoria.

Cabe, finalmente, señalar que en fecha 26 de julio se presentó públicamente la Memoria anual de la Agencia con asistencia de representantes de sectores relacionados con la protección de datos personales y de los medios de comunicación.

2. **PARTICIPACION DEL DIRECTOR DE LA AGENCIA EN CONFERENCIAS, SEMINARIOS, JORNADAS Y REUNIONES INSTITUCIONALES.**

A lo largo del año 2001 han sido muy numerosos los requerimientos planteados al Director de la Agencia para participar, con asistencia de diversos sectores afectados por la aplicación de la LOPD, en conferencias y seminarios en los que poder plantear directamente los distintos aspectos relacionados con aquélla.

Este tipo de participaciones permite al Director exponer los criterios de aplicación de la LOPD contenidos en sus resoluciones así como resolver las dudas que se plantean en cada sector concreto.

De este modo se lleva a cabo una función preventiva en relación con la LOPD, facilitando su cumplimiento a los operadores económicos que han de adecuar su actividad a las exigencias legales.

Asimismo el Director ha mantenido constantes reuniones con responsables de ficheros posibilitando abordar en profundidad las peculiaridades de cada empresa.

El año 2001 destaca por el número y complejidad de reuniones mantenidas con empresas que operan en el sector de

las telecomunicaciones, lo que ha permitido tratar no sólo las cuestiones relacionadas con la LOPD, sino también las que hacen referencia a la normativa específica de protección de datos en dicho sector, derivada de la Directiva 97/66/CE.

Han continuado celebrándose, junto a las anteriores, reuniones con representantes de otros sectores tradicionalmente relacionados con la protección de datos como los de carácter financiero, solvencia patrimonial y crédito, publicidad, distribución comercial, sanidad, así como con diversos despachos de abogados.

También han sido objeto de análisis los planteamientos de las asociaciones de consumidores y usuarios de servicios, cuyo enfoque permite completar el que ofrecen las empresas responsables de ficheros.

La actividad informativa del Director de la Agencia se ha completado con la publicación de artículos divulgativos de la materia.

2. CONFERENCIAS OFICIALES 2001

Fecha	Ciudad	Título de la Conferencia	Organizada por
11/01/01	BARCELONA	LA NUEVA LEY DE PROTECCIÓN DE DATOS Y SUS REPERCUSIONES EN EL ÁMBITO DE LA ABOGACÍA	COLEGIO DE ABOGADOS DE BARCELONA
12/01/01	BARCELONA	LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL POR LAS CORPORACIONES LOCALES	AYUNTAMIENTO Y DIPUTACIÓN DE BARCELONA
30/01/01	MADRID	CICLO DE CONFERENCIAS MAGISTRALES PROTECCIÓN DE DATOS EN INTERNET	MINISTERIO DE CIENCIA Y TECNOLOGÍA Y CEFI
14/02/01	MADRID	NUEVA LEY DE PROTECCIÓN DE DATOS	UNIVERSIDAD COMPLUTENSE
20/02/01	MADRID	EL DERECHO DE LA PROTECCIÓN DE DATOS EN LA U.E.	CENTRO DE ESTUDIOS EUROPEOS
26/02/01	MADRID	EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS	REVISTA OTROSÍ COLEGIO DE ABOGADOS
05/03/01	MADRID	TERCER CURSO DE INICIACIÓN AL DERECHO DE LA PUBLICIDAD: PROTECCIÓN DE DATOS PERSONALES	ASOCIACIÓN DE AUTOCONTROL DE LA PUBLICIDAD
06/03/01	MADRID	DATSALU, 2001 : EL NUEVO MARCO DE LA PROTECCIÓN DE DATOS, UNA ESPECIAL REFERENCIA A LOS DATOS DE SALUD	INFORMÁTICOS EUROPEOS EXPERTOS
09/03/01	MADRID	EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS	REVISTA DERECHO Y NUEVAS TECNOLOGÍAS
14/03/01	SEVILLA	III JORNADAS TÉCNICAS DE ESTADÍSTICA PÚBLICA EN ANDALUCÍA "PROTECCIÓN DE DATOS Y ESTADÍSTICA"	INSTITUTO DE ESTADÍSTICA DE ANDALUCÍA
15/03/01	MADRID	I CONGRESO INTERNACIONAL DE TELEMEDICINA "LA ESPECIAL PROTECCIÓN LEGAL DE LOS DATOS SANITARIOS"	ASOCIACIÓN EUROPEA DE TELEMEDICINA Y ASOCIACIÓN ESPAÑOLA DE TELEMEDICINA
27/03/01	MADRID	JORNADAS SOBRE DELINCUENCIA INFORMÁTICA Y NUEVAS TECNOLOGÍA DE LA INFORMACIÓN "ASPECTOS JURÍDICOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL"	MINISTERIO DEL INTERIOR SECRETARIA DE ESTADO DE SEGURIDAD
02/04/01	MADRID	JORNADAS PROTECCIÓN DE DATOS: "EL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS Y LAS NOVEDADES DE LA NUEVA LEY"	UNIVERSIDAD PONTIFICIA DE COMILLAS
06/04/01	MADRID	XII SEMINARIO PERMANENTE DE ADMINISTRACIÓN Y ECONOMÍA PÚBLICA: "EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS EN ESPAÑA Y EN LA UNIÓN EUROPEA"	INSTITUTO UNIVERSITARIO ORTEGA Y GASSET
18/04/01	MADRID	FORO DEBATE SCORING	UNIVERSIDAD DE COMILLAS
19/04/01	MADRID	SEMINARIO AUDITORIA DE PROTECCIÓN DE DATOS Y MEDIDAS DE SEGURIDAD "EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS TRAS LA STC 292/2000"	GRUPO RECOLETOS
24/04/01	MADRID	SECURMÁTICA 2001/04/24"EL DERECHO A LA PROTECCIÓN DE DATOS EN EL MARCO DE LA STC 292/2000.	REVISTA SEGURIDAD EN INFORMÁTICA Y COMUNICACIONES
25/04/01	BILBAO	VIII JORNADAS SOBRE DERECHO Y GENOMA HUMANO "LA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y SU POSIBLE PROYECCIÓN A LOS DATOS GENÉTICOS Y RELATIVOS A LA SALUD"	UNIVERSIDAD DEL PAÍS VASCO-FUNDACIÓN BBV

DESDE OCTUBRE DE 2001 CONVENIO HERMANAMIENTO CON REP. CHECA

3. JORNADAS SOBRE PROTECCIÓN DE DATOS PERSONALES POR LAS ADMINISTRACIONES PÚBLICAS (LOGROÑO, 5 Y 6 DE JULIO DE 2001)

Con objeto de dar a conocer la normativa sobre Protección de Datos Personales y concienciar a las autoridades y funcionarios de las Administraciones Públicas sobre la importancia del más estricto cumplimiento de la misma, dentro del ejercicio de sus competencias, la Agencia organizó, en colaboración con el Gobierno de La Rioja (Consejería de Desarrollo Autonómico y Administraciones Públicas), unas Jornadas sobre "Protección de Datos Personales por las Administraciones Públicas", que tuvieron lugar en Logroño los días 5 y 6 de Julio de 2001.

En las Jornadas se abordaron los siguientes temas, expuestos por los señores que a continuación se detallan:

* "Obligaciones de las Administraciones Públicas en el tratamiento de Datos Personales. Consecuencias de su incumplimiento".

Ilmo. Sr. D. Juan Manuel Fernández López. Director de la Agencia de Protección de Datos.

* "Funciones de la Agencia de Protección de Datos y de las Agencias Autonómicas"

Ilma. Sra. Dª Rosa García Ontoso. Directora de la Agencia de Protección de Datos de la Comunidad de Madrid.

* "Tratamiento y cesión de datos por los Ayuntamientos".

Ilmo. Sr. D. Jesús Rubí Navarrete. Adjunto al Director de la Agencia de Protección de Datos.

* "Medidas de seguridad técnicas y organizativas que han de aportar los responsables de ficheros y los encargados del tratamiento"

Ilmo. Sr. D. Gregorio González Valero. Subdirector General Adjunto de la Subdirección de Sistemas de la Información del Ministerio de Ciencia y Tecnología.

* "Ficheros de solvencia patrimonial de titularidad pública y su compatibilidad con otros ficheros de titularidad privada".

Ilmo. Sr. D. Rafael Prado Iglesias. Banco de España – CIRBE.
Ilmo. Sr. D. Miguel Angel Davara. Catedrático de Derecho Informático de la Universidad Pontificia de Comillas (ICADE).

* "Régimen de los ficheros de las Administraciones Tributarias".

Ilmo. Sr. D. Santiago García Izquierdo. Subdirector General de la Inspección de Datos de la Agencia de Protección de Datos.

* "Datos especialmente protegidos en ficheros gestionados por las Administraciones Públicas. Especial referencia a los ficheros policiales".

Excmo. Sr. D. José Antonio Martín Pallín.
Magistrado del Tribunal Supremo.
* "Revisión en vía jurisdiccional de las resoluciones dictadas por la Agencia de Protección de Datos y las Agencia Autonómicas".

Excmo. Sr. D. Tomás García Gonzalo. Magistrado de lo Contencioso-Administrativo de la Audiencia Nacional.

4. PREMIOS "PROTECCIÓN DE DATOS PERSONALES"

Por Resoluciones ambas, de 5 de febrero de 2001 se convocaron los premios "Protección de Datos Personales" y de Periodismo "Protección de Datos Personales".

* El Premio "Protección de Datos Personales" Convocatoria 2001, con una dotación de un millón de pesetas y un accésit con una asignación de doscientas cincuenta mil pesetas, tiene la finalidad de profundizar en el estudio del desarrollo del derecho fundamental a la protección de datos.

Según las Bases de la Convocatoria este premio se otorga a la mejor obra científica, original e inédita, de autor español o extranjero, que verse sobre la materia de la protección de datos personales, desde un plano jurídico, ya sea con un enfoque estrictamente teórico o a partir de experiencias concretas basadas en nuestro ordenamiento o en el derecho comparado.

El Jurado establecido en las Bases de la convocatoria otorgó por unanimidad el Premio al trabajo titulado "El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones" del que

son autores D. Lorenzo Marroig Pol y Dª María de los Reyes Corripio Gil-Delgado.

Como se indica en la presentación de la obra, de la que se ha realizado una edición de 1000 ejemplares para su entrega y difusión institucional, la decisión del Jurado es reveladora de la importancia que está adquiriendo el desarrollo de las tecnologías de la información en las comunicaciones, así como de su incidencia en la protección de los datos de abonados y usuarios.

La obra se caracteriza por realizar un diagnóstico completo e interdisciplinar del sector de las telecomunicaciones y de su régimen jurídico no sólo presente, sino también de futuro, al ser constantes las referencias a los trabajos en curso sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre le tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.

Se concedió un accésit a la obra titulada "La protección de los datos en la Unión Europea: Divergencias normativas y anhelos unificadores" de la que es autor D. Abel Tellez Aguilera. En ella se recoge un exhaustivo estudio de la normativa sobre Protección de Datos en diferentes Estados de la Unión y de fuera de ella, poniendo de manifiesto que, pese a los intentos armonizadores de la Directiva 95/46/CE en el ámbito europeo, su objetivo sólo ha sido alcanzado parcialmente, subsistiendo regulaciones diversas en los Estados Miembros que sería conveniente evitar.

* El Premio de Periodismo "Protección de Datos Personales" al que podían optar los trabajos publicados en cualquier medio de comunicación (televisión, radio, prensa) que tuvieran como tema central la protección de datos personales, fue declarado desierto, por unanimidad del Jurado, al entender que los contenidos de los trabajos presentados no tenían como tema el exigido por las Bases de la Convocatoria.

El día 18 de diciembre en un acto celebrado en Madrid, el Director de la Agencia hizo entrega de los premios indicados, acto en el que estuvieron presentes el Consejo Consultivo de la Agencia de Protección de Datos, medios de comunicación e invitados.

MEMORIA DE 2001 - ANEXO I - RESOLUCIÓN DE 27 DE JULIO DE 2001, DE LA AGENCIA DE PROTECCIÓN DE DATOS, POR LA QUE SE CREAN Y MODIFICAN FICHEROS DE DATOS DE CARÁCTER PERSONAL DE LA AGENCIA.

El artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) establece que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente. Asimismo, la Disposición Adicional primera de la LOPD ordena a las Administraciones Públicas responsables de ficheros aprobar la disposición de creación de los mismos o adaptar la ya existente a las previsiones de la propia Ley.

En la Agencia de Protección de Datos se hace necesaria la aprobación de la pertinente disposición de regulación de ficheros para la adecuación de los mismos a la LOPD, en los términos que establece el artículo 20.2 de la LOPD.

A fin de facilitar el conocimiento público de los ficheros de la Agencia en una sola Disposición, la presente Resolución deroga las de esta Agencia de Protección de Datos de 18 de julio de 1994 y 7 de febrero de 1995, incorporando en su Anexo los ficheros ya regulados por aquéllas, con las modificaciones que la Ley o el transcurso del tiempo recomien - dan. Además, se incluyen en dicho Anexo dos nuevos ficheros ("Agenda de Comunicaciones" y "Gestión de consultas"), que no aparecían en las anteriores Resoluciones.

En su virtud, y en el ejercicio de las atribuciones que me confiere el artículo 12.2. del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos y a fin de dar cumplimiento al mandato legal del artículo 20 de la LOPD, sobre creación y modificación de ficheros que contengan datos de carácter personal gestionados por la Agencia de Protección de Datos, y asegurar a los administrados el ejercicio de sus legítimos dere - chos, dispongo:

Primero.- Los ficheros de la Agencia de Protección de Datos serán los contenidos en el Anexo de esta Resolución, adaptando los ficheros contenidos en las Resoluciones de 18 de julio de 1994 (BOE nº 180, de 29) y de 7 de febrero de 1995 (BOE nº 39, del 15) a lo dispuesto en el artículo 20.2 de la LOPD e indicando el nivel de medidas de seguridad básico, medio o alto correspondiente a cada uno de estos ficheros, en aplicación del Real Decreto 994/1999, de 25 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Segundo.- Se crean los ficheros "Agenda de comunicaciones relaciones institucionales" y "Gestión de consultas sobre protección de datos", incluidos en el Anexo de esta Resolución, en cumplimiento del artículo 20 de la Ley Orgánica 15/1999.

Tercero.- Los ficheros que se indican en el Anexo se regirán por las disposiciones generales e instrucciones que se detallen para cada uno de ellos, y estarán sometidos, en todo caso, a las normas legales y reglamentarias de superior rango que les sean aplicables.

Cuarto.- La aprobación de la presente Resolución no supone la supresión de ningún fichero de datos de carácter personal, por lo que no es necesaria la aplicación de lo dispuesto en el artículo 20.3 de la LOPD.

Quinto.- Quedan derogadas las Resoluciones de esta Agencia de Protección de Datos de 18 de julio de 1994, por la que se crean los ficheros de datos de carácter personal de la Agencia y 7 de febrero de 1997, por la que se crean y modifican los ficheros de datos de carácter personal de la Agencia.

Sexto.- La presente Resolución entrará en vigor el día siguiente de su publicación en el "Boletín Oficial del Estado".

Madrid, 27 de julio de 2001.

EL DIRECTOR DE LA AGENCIA.

Juan Manuel Fernández López

ANEXO

Fichero: Registro General de Protección de Datos

a) *Finalidad del fichero y usos previstos para el mismo* .

La finalidad del fichero es velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de los datos. El fichero contiene los datos relacionados con la persona que actúa como declarante de la notificación con la finalidad de tramitar la correspondiente solicitud en los términos previstos en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Los usos que se darán del fichero son los derivados de la tramitación de los expedientes de inscripción de creaciones, modificaciones y supresiones de ficheros con datos personales; expedientes de transferencias internacionales de datos; expedientes de inscripción de códigos tipo; expedición de certificados; publicación del catálogo de ficheros; obtención de estadísticas y elaboración de la Memoria anual de la Agencia.

El Registro General de Protección de Datos no contiene datos de carácter personal a excepción de los datos del titular del fichero, cuando éste sea una persona física y de la persona que actúa como declarante de la notificación. Igualmente, puede contener datos de carácter personal de destinatarios de cesiones de datos o transferencias internacionales de datos y, en su caso, del encargado del tratamiento, siempre que se trate de personas físicas.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos*.

Responsables de ficheros, encargados de tratamiento y destinatarios de cesiones o transferencias internacionales de datos, siempre que éstos sean personas físicas;

Personas físicas que actúan como declarantes en la notificación.

c) *Procedimiento de recogida de los datos de carácter personal.*

A través de la notificación de inscripción mediante el modelo de notificación del tratamiento de datos de carácter personal, presentada en soporte papel, informático o telemático.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Número de identificación fiscal.
Nombre y apellidos.
Dirección postal y electrónica.
Puesto desempeñado por el declarante.
Relación, en su caso, con el responsable del fichero (representante, encargado del tratamiento, etc.).

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

El Registro será público en relación con los datos a que se refiere el artículo 14 de la LOPD.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel básico

Fichero: Gestión de recursos humanos de la Agencia de Protección de Datos

a) *Finalidad del fichero y usos previstos para el mismo* .

La finalidad del fichero es la gestión del personal adscrito a la Agencia de Protección de Datos.

Los usos que se darán del fichero son los derivados de la gestión de recursos humanos, control de incompatibilidades, situación laboral, obtención de estadísticas e impresos necesarios en la gestión de personal.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos*.

Personal funcionario y laboral destinado en la Agencia de Protección de Datos.

c) *Procedimiento de recogida de los datos de carácter personal.*

Transmisión por medios informáticos de los datos relativos al personal de la unidad, procedente del Registro Central de Personal del Ministerio de Administraciones Públicas y formularios cumplimentados por el personal funcionario o laboral.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Aplicación horizontal suministrada por el Ministerio de Administraciones Públicas, con los siguientes tipos de datos:

Datos especialmente protegidos: Datos sobre ejecución de sanciones en materia de función pública.

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, número de registro de personal, número de Seguridad Social/Mutualidad, dirección postal y teléfono.

Datos de características personales: Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos familiares.

Datos de circunstancias sociales: Fechas de alta y baja, licencias, permisos, autorizaciones y situación militar.

Datos académicos y profesionales: Titulaciones, formación y experiencia profesional.

Datos de detalle de empleo y carrera administrativa. Incompatibilidades.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

Al Registro Central de Personal en cumplimiento de lo establecido en el artículo 13 de la Ley 30/1984 de Medidas para la Reforma de la Función Pública.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel medio.

Fichero: Nómina estándar de la Agencia de Protección de Datos

a) Finalidad del fichero y usos previstos para el mismo .

La finalidad del fichero es la gestión de la nómina del personal adscrito a la Agencia de Protección de Datos.

Los usos que se darán del fichero son los derivados de la emisión de la nómina del personal de la Agencia, así como los destinados a la obtención de todos los productos derivados de la misma, tales como información periódica para los afectados: informes y ficheros destinados a la Agencia Estatal de Administración Tributaria, Tesorería General de la Seguridad Social y bancos pagadores; seguimiento contable del capítulo 1 presupuestario; gestión económica de acción social y obtención de estudios estadísticos o monográficos destinados a la gestión económica del personal.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos* .

Personal funcionario y laboral destinado en la Agencia de Protección de Datos.

c) *Procedimiento de recogida de los datos de carácter personal.*

Transmisión por medios informáticos de los datos relativos al personal, procedente del Registro Central de Personal del Ministerio de Administraciones Públicas y formularios cumplimentados por el personal funcionario o laboral.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Aplicación horizontal suministrada por el Ministerio de Administraciones Públicas, con los siguientes tipos de datos:

Datos especialmente protegidos: Afiliación sindical, bajas por enfermedad del personal laboral y minusvalías.

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, número de registro de personal, número de Seguridad Social/Mutualidad, dirección postal y teléfono.

Datos de características personales: Sexo, estado civil, edad, fecha y lugar de nacimiento y datos familiares.

Datos académicos y profesionales: Formación, titulaciones y experiencia profesional.

Datos de detalle de empleo y carrera administrativa: Cuerpo/escala, categoría/grado, puestos de trabajo, datos no económicos de nómina, historial del trabajador.

Datos económico financieros. Datos económicos de nómina, créditos, préstamos, avales y deducciones impositivas. Datos de cuenta bancaria de percepción de haberes.

Datos de transacciones: Compensaciones/indemnizaciones por dietas.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

A la Agencia Estatal de Administración Tributaria, en virtud de la Ley 40/1998, de 9 de diciembre, del Impuesto sobre la Renta de las Personas Físicas.

A la Tesorería General de la Seguridad Social, en virtud del Real Decreto Legislativo 1/1994, de 20 de junio, Texto Refundido de la Ley General de la Seguridad Social, a efectos recaudatorios.

A MUFACE y a la Mutualidad General Judicial.

A la Dirección General de Costes de Personal y Pensiones Públicas, en virtud del Real Decreto Legislativo 670/1987, de 30 de abril, por el que se aprueba el Texto Refundido de la Ley de Clases Pasivas del Estado.

A los bancos y cajas de ahorros, los datos necesarios para el abono de los haberes líquidos.

A las mutualidades de funcionarios y Colegios de Huérfanos, a los que voluntariamente coticen algunos funcionarios, cuando éstos lo soliciten.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel alto

Fichero: Gestión económica de la Agencia de Protección de Datos

a) Finalidad del fichero y usos previstos para el mismo .

La finalidad del fichero es la gestión económica de la Agencia de Protección de Datos.

Los usos que se dan del fichero son los derivados de la gestión y tramitación de los expedientes de contratación y gasto; documentos contables de la Agencia de Protección de Datos; gestión económica de las dietas del personal de la Agencia y gestión económica de las sanciones impuestas por infracciones a la Ley Orgánica 15/1999.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos* .

Proveedores del ente público. Personas físicas afectadas por las sanciones impuestas por la Agencia de Protección de Datos. Personal funcionario y laboral destinado en la Agencia de Protección de Datos.

c) *Procedimiento de recogida de los datos de carácter personal.*

A través del propio interesado o su representante legal y de fuentes accesibles al público, de las previstas como tales en el art. 3.j) de la Ley Orgánica 15/1999.

De los expedientes sancionadores de la Inspección de datos, a los solos efectos de proceder al cobro de las sanciones.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Aplicación horizontal suministrada por la Intervención General de la Administración del Estado, con los siguientes tipos de datos:

Datos especialmente protegidos: Sanciones a la Ley Orgánica 15/1999, con la única finalidad de proceder a su cobro.

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección postal y electrónica.

Datos económico financieros. Datos bancarios.

Datos de transacciones. Bienes y servicios suministrados.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

A la Agencia Estatal de Administración Tributaria, en virtud de la Ley General Tributaria.

Al Tribunal de Cuentas, y a la Intervención General de la Administración del Estado, según dispone la Ley General Presupuestaria (Real Decreto Legislativo 1091/1988).

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel medio

Fichero: Gestión interna de la Agencia de Protección de Datos

a) Finalidad del fichero y usos previstos para el mismo .

La finalidad del fichero es la gestión y administración interna de la Agencia de Protección de Datos.

Los usos que se dan del fichero son los derivados de la gestión de personal, acción social, promoción y selección de personal mediante oposiciones y concursos, gestión de usuarios, estadísticas, administración de la red, control de inventario y gestión de biblioteca así como los derivados de las restantes actividades relacionadas con el funcionamiento y gestión interna de la Agencia.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos* .

Personal funcionario y laboral destinado en la Agencia de Protección de Datos y sus beneficiarios.

Personas que solicitan participar en procesos de selección de personal de la Agencia de Protección de Datos.

c) *Procedimiento de recogida de los datos de carácter personal.*

A través del propio interesado o su representante mediante declaraciones o formularios.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, número de registro de personal, número de Seguridad Social/Mutualidad, dirección postal y teléfono.

Datos de características personales: Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos familiares.

Datos académicos y profesionales: Formación, titulaciones y experiencia profesional.

Datos de detalle de empleo y carrera administrativa: Cuerpo/escala, categoría/grado, puestos de trabajo, historial del trabajador.

Datos económico-financieros. Ingresos, rentas.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

A la entidad a quien se atribuya la gestión en materia de riesgos laborales, según dispone la Ley 31/1995 de Prevención de Riesgos Laborales.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel básico

Fichero: Registro de entrada y salida de documentos de la Agencia de Protección de Datos

a) Finalidad del fichero y usos previstos para el mismo .

La finalidad del fichero es la gestión del registro de entrada y salida de documentos de la Agencia de Protección de Datos, en los términos previstos en el art. 45 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Los usos que se dan del fichero son los derivados de la gestión integral de las operaciones de registro de documentos de entrada y salida.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos* .

Personas físicas o representantes de personas jurídicas que se dirigen a la Agencia de Protección de Datos o que reciben comunicaciones de este ente público.

c) *Procedimiento de recogida de los datos de carácter personal.*

Declaración en soporte papel, magnético o telemático del propio interesado o su representante legal.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección postal y electrónica, teléfono, fax y e-mail.
Puesto de trabajo.
Datos de representación, en su caso.
Datos relacionados con el documento presentado.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

No se prevén cesiones.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel básico

Fichero: Expedientes de la Inspección de Datos

a) Finalidad del fichero y usos previstos para el mismo .

La finalidad del fichero es la gestión y tramitación de expedientes de la Inspección de Datos, tramitados en virtud de la potestad sancionadora atribuida a la Agencia de Protección de Datos por el artículo 37 g) de la LOPD.

Los usos que se dan del fichero son los derivados de la tramitación, control y seguimiento de los expedientes sancionadores y de reclamación y tutela de derechos.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos* .

Personas físicas o representantes de personas jurídicas presuntos responsables en el expediente.

Personas físicas que tengan la condición legal de afectados y hayan formulado una denuncia relacionada con el expediente.

c) *Procedimiento de recogida de los datos de carácter personal.*

Declaraciones o formularios, recibidos del propio interesado o su representante legal, de las actas de inspección, del Registro General de Protección de Datos y Registros Públicos.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Datos especialmente protegidos: Sanciones a la Ley Orgánica 15/1999 (amparados en el art. 37.g)

Datos de carácter identificativo: Nombre y apellidos, DNI/NIF, dirección postal, electrónica y teléfono.

Otros datos personales aportados por los afectados.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

No se prevén cesiones.

Podrán efectuarse transferencias a Autoridades de Control de otros Estados, en virtud de lo dispuesto en Convenios y Tratados Internacionales o en las normas de Derecho Comunitario Europeo.

f) *Órgano de la Administración responsable del fichero.*

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible.*

Nivel medio

Fichero: Agenda de comunicaciones y relaciones institucionales

a) *Finalidad del fichero y usos previstos para el mismo.*

La finalidad del fichero es mantener una agenda de los representantes de medios de comunicación e instituciones públicas y privadas, nacionales e internacionales con las que la Agencia de Protección de Datos mantiene relaciones institucionales.

Los usos que se darán del fichero son los de envío de publicaciones y comunicaciones, convocatoria de actos y relaciones institucionales y de protocolo de la Agencia de Protección de Datos.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos*.

Representantes de medios de comunicación, entidades públicas y privadas y autoridades de control internacionales.

c) *Procedimiento de recogida de los datos de carácter personal* .

A través del propio interesado, de la institución o medio que representa y de las fuentes accesibles al público previstas como tales en el art. 3.j) de la Ley Orgánica 15/1999.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Nombre y apellidos.
Dirección postal y/o electrónica.
Teléfono.
Denominación de la entidad o medio que representa.
Cargo o puesto desempeñado en la misma.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

No se prevén cesiones ni transferencias de los datos de carácter personal.

f) *Órgano de la Administración responsable del fichero* .

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pudiesen ejercitarse los derechos de oposición, acceso, rectificación y cancelación*.

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible* .

Nivel básico

Fichero: Gestión de Consultas sobre Protección de Datos

a) Finalidad del fichero y usos previstos para el mismo.

Gestión de las consultas relacionadas con la protección de datos personales que las personas físicas o representantes de personas jurídicas que planteen ante la Agencia de Protección de Datos.

b) *Personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos*.

Personas físicas que realicen consultas particulares sobre protección de datos. Personas que dirijan consultas a la Agencia en representación de instituciones, empresas, asociaciones, etc.

c) *Procedimiento de recogida de los datos de carácter personal* .

Proceden del propio interesado o su representante legal, recogidos mediante escrito entregado físicamente en la Agencia, envío por correo ordinario o mediante formulario en la página Web de la Agencia de Protección de Datos.

d) *Estructura básica del fichero y descripción de los tipos de datos de carácter personal incluidos en el mismo:*

Nombre y apellidos.
Dirección postal y/o electrónica.
Teléfono.

e) *Cesiones de datos de carácter personal y, en su caso, transferencias de datos que se prevean a países terceros.*

No se prevén cesiones ni transferencias de los datos de carácter personal que contiene el fichero.

f) *Órgano de la Administración responsable del fichero* .

Agencia de Protección de Datos.

g) *Servicios o unidades ante los que pudiesen ejercitarse los derechos de oposición, acceso, rectificación y cancelación*.

Agencia de Protección de Datos, calle Sagasta, número 22, 28004 Madrid.

h) *Medidas de seguridad con indicación del nivel exigible* .

Nivel básico

AGENCIA DE PROTECCIÓN DE DATOS
CALLE SAGASTA, 22 - 28004 MADRID
TELÉFONO 91 3996200

MEMORIA DE 2001 - ANEXO II - INFORMES PRECEPTIVOS

PROYECTO DE DISPOSICIÓN	SOLICITADO POR	FECHA
Proyecto de Orden por la que se establecen los procedimientos aplicables para las declaraciones de inversiones exteriores y su liquidación, así como los procedimientos para la presentación de memorias anuales y de expedientes de autorización.	Sub. Gral. de Coordinación Normativa y Relaciones Institucionales	23/01/01
Informe referente al Proyecto de Orden por la que se modifica la Orden de 25 de febrero del 2000 por la que se crea y regula el Indice Nacional de Defunciones	Secretario General Técnico de Sanidad y Consumo	07/02/01
Informe referente al Proyecto de Orden Ministerial por la que se actualiza y amplia la relación de ficheros automatizados del Ministerio.	Secretario General Técnico del Mº de Fomento	07/02/01
Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.	Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.	07/02/01
Informe relativo al Borrador de "Resolución de la Dirección General de Seguros y Fondo de Pensiones y la Dirección General de Tráfico, sobre cesión de datos que figuran en los ficheros automatizados del Consorcio de Compensación de Seguros y la Dirección General de Tráfico, para hacer efectivo el control de la obligación de asegurarse".	Director General de Tráfico	07/02/01
Informe referido al Borrador de Anteproyecto de Ley de adecuación de la legislación de la Comunidad de Madrid en materia de Protección de Datos a los Principios y Normas contenido en la Ley Orgánica 15/1999.	Secretaría General Técnica. Consejería de Presidencia y Hacienda Comunidad de Madrid	05/03/01
Informe referente al proyecto de Real Decreto por el que se establecen los controles higienico-sanitarios para la prevención y control de la legionelosis.	Secretario General Técnico Mº de Sanidad	07/03/01
Informe referente al Proyecto de Orden Ministerial por la que se actualiza la relación de ficheros del Mº de Fomento	Secretario General Técnico del Mº de Fomento	07/03/01
Informe referente a los cuestionarios censales de los censos de población y vivienda, así como del pliego de prescripciones técnicas que regirá el concurso de servicios para la implementación y gestión de un sistema telemático que permita la cumplimentación via Internet.	Director General de Estadísticas de Población e Información I.N.E.	12/03/01
Informe referente a la Propuesta de texto de Instrucción por la que se define el formato y contenido del documento individual de seguimiento radiológico (carné radiológico)	Secretario General del Consejo de Seguridad Nuclear	13/03/01
Informe referente al Borrador de Real Decreto por el que se desarrolla el art. 81 de la Ley 66/97 de Medidas Fiscales en materia de prestación de servicios de seguridad por el Fábrica Nacional de la Moneda y Timbre.	Subsecretario del Mº de Economía	15/03/01
Informe referente al Proyecto de Orden del Ministerio del Interior por la que se crean y actualizan los ficheros automatizados con datos de carácter personal.	Secretario General Técnico del Mº de Justicia (Lo solicita el Mº del Interior)	15/03/01
Informe referente al Borrador de Convenio entre el Reino de España y la República de Kazajstán sobre cooperación para combatir determinados delitos.	Subdirector General de Asuntos Jurídicos Consulares	02/04/01
Informe referente al Proyecto de Orden del Ministerio de Sanidad y Consumo, por la que se regula el Registro Nacional de las Encefalopatías Espongiformes transmisibles humanas y que modifica la de 21 de octubre de 1996.	Secretario General Técnico del Mº de Sanidad	02/04/01
Informe referente a la encuesta a realizar por el Instituto Gallego de Estadística sobre las condiciones de vida de las familias	Director del Instituto Gallego de Estadística	03/04/01
Informe referente al Proyecto de Orden por el que se crea un fichero de datos de carácter personal, relativo al Proyecto Itínere	Secretario General Técnico del Mº de Sanidad y Consumo	03/04/01
Informe referente al Proyecto de Orden de la Consejería de Medio Ambiente por la que se convocan subvenciones a Corporaciones Locales para las Agrupaciones Municipales de Voluntarios de Protección Civil en el ámbito territorial de la Comunidad de Madrid.	Director General de Protección Ciudadana de la Consejería de Medio Ambiente de la Comunidad de Madrid	03/04/01
Informe referente al Anteproyecto de Ley Financiera	Directora General del Tesoro y Política Financiera	09/04/01

MEMORIA DE 2001 - ANEXO III - CÓDIGO TIPO ANF

PREÁMBULO

La Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, tiene por objeto garantizar y proteger, en lo que concierne a tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

No obstante, el espectacular desarrollo de las nuevas tecnologías de comunicación: Internet, WebTV... etc.; la necesidad de contratación externa de servicios especializados de hospedaje web y conectividad: hosting; la masiva utilización de avanzados instrumentos de alta disponibilidad, que simplifican el transporte de equipos y la conexión entre programas y ordenadores: poket pc, handels, ordenadores portátiles, etc. Y aún más importante, la aparición de sofisticadas técnicas de contaminación e intrusión que permiten acceder de forma remota a los sistemas informáticos para sustraer información sensible de las personas: números de cuentas bancarias, números de tarjetas de créditos, perfiles de consumo... etc., todo lo cual repercute en un alto grado de desconfianza en el empleo de estas tecnologías y por ende, un grave perjuicio para numerosas empresas y profesionales que ven frustradas sus expectativas de desarrollo y sus esfuerzos de adaptación a la nueva economía. Requisito básico de subsistencia para afrontar un mercado cada vez más globalizado.

La ASOCIACIÓN NACIONAL DE FABRIANTES, ANF, es una entidad sin ánimo de lucro, constituida en fecha 30 de octubre de 1995 e inscrita en el Registro de Asociaciones del Ministerio del Interior con el núm. nacional 160.009, que agrupa, fundamentalmente, a empresas y profesionales de los sectores de alimentación, bebidas, droguería y perfumería. Su sede central se halla en la ciudad de Barcelona, Gran Via de les Corts Catalanes, 996, 4º 2ª.

En Asamblea General Extraordinaria celebrada en fecha 20 de junio de 2001, se reconoció por los miembros de la Asociación la necesidad de regular el tratamiento de los datos de carácter personal mediante normas de compromiso voluntario.

En esta Asamblea se facultó a la Junta Directiva y en representación de la misma, al Presidente de la Asociación, para la elaboración de un código ético y para llevar a cabo cuantas gestiones fueran necesarias ante la Agencia de Protección de Datos, hasta la inscripción del mismo.

Es por ello, que elabora el presente código, que podrán suscribir todas aquellas empresas o profesionales asociados o

adheridos a la ASOCIACIÓN NACIONAL DE FABRICANTES, ANF.

El presente código será de aplicación a los datos de carácter personal contenidos en ficheros sobre clientes.

El presente código arbitra un sistema, cuyo seguimiento asegura a los adheridos al mismo el pleno cumplimiento de sus obligaciones en materia de protección de datos de carácter personal. Así, entre otras, las ventajas de adherirse al código son las siguientes:

a) Aumento de la confianza de todos los clientes al facilitar sus datos personales a las empresas y que estos datos sean objeto de tratamiento.

b) Posibilidad de utilización del sello de "Garantía TID de protección de datos" -refiriéndose las siglas TID a un tratamiento informatizado o digital de los datos- que posiciona a la empresa como una entidad seria y preocupada por la protección de la intimidad de las personas.

c) Este sello de garantía es un distintivo de calidad y normalización tecnológica. El compromiso permite establecer una imagen de homologación básica de entidades que son conscientes de que, además del puro compromiso ético de actuación individual, tienen que tomar una posición activa sobre los datos que tienen la obligación de custodiar.

Asimismo, el código garantiza plenamente la protección de los datos de carácter personal y el ejercicio por sus titulares de los derechos sobre los mismos:

a) Se detallan los derechos de los titulares sobre sus datos de carácter personal.

b) Se establecen los deberes de los adheridos al Código para lograr el respeto de esos derechos, entre ellos, el deber de informar sobre el contenido del fichero, el destino de los datos, los derechos que ostenta frente al responsable del fichero, etc.

c) Se restringen las fuentes de recogida de datos de carácter personal.

d) Se garantiza el derecho de oposición.

e) Se regula el procedimiento para el ejercicio por sus titulares de los derechos de acceso, rectificación y cancelación sobre sus datos de carácter personal, adjuntándose al Código unos formularios para facilitarles el ejercicio de estos derechos.

f) Se crea el "Comité de Protección de Datos de la ANF" como órgano que vele por el cumplimiento del Código y que persiga las violaciones de los derechos de los titulares de los datos de carácter personal.

g) Se regula el procedimiento de presentación de quejas ante el Comité por el titular de los datos de carácter personal afectado por una entidad adherida al Código.

h) Se establece un sistema de sanciones para castigar las infracciones cometidas.

Todas las empresas y profesionales que voluntariamente se adhieran al código y a los protocolos de carácter técnico que establezca en cada momento el responsable del mismo podrán utilizar el "Sello Garantía TID de protección de datos", como símbolo identificador de la adhesión al presente código.

CAPÍTULO PRIMERO
PRINCIPIOS GENERALES

Articulo 1: Definiciones

A los efectos del presente Código se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas, identificadas o identificables.

b) Fichero: conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero: persona física o jurídica que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto de tratamiento a que se refiere el apartado c).

f) Cliente: persona física que adquiere productos o servicios de una empresa o profesional adheridos al código, y cuyos datos personales han sido objeto de tratamiento en esa relación.

g) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

h) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

i) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impe-

dida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos, en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen carácter de fuentes de acceso público, los Diarios y Boletines Oficiales y los medios de comunicación.

Artículo 2: Niveles de Seguridad

Las empresas y profesionales adheridos a este Código se comprometen a analizar detenidamente los contenidos de sus ficheros y adaptarlos a lo dispuesto en el Real Decreto 994/1999 de 11 de junio por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

En concreto, las medidas de seguridad adoptadas por las empresas y profesionales adheridos al presente código en sus ficheros sobre clientes que contengan datos de carácter personal serán, como mínimo, las que el Real Decreto 994/1999 de 11 de junio califica de nivel básico, juntamente con las de nivel medio.

Artículo 3: Seguridad en la red

Las empresas y profesionales adheridos a este Código que capten datos personales "on-line" deberán contar con un sistema de conexión segura SSL de 128 b. que imposibilite la captación por parte de terceros de la información que se está transmitiendo.

CAPÍTULO SEGUNDO
DERECHOS DE LOS TITULARES

Artículo 4: Fuentes de recogida de datos.

Las fuentes de recogida de datos personales de los clientes, que formen parte de los ficheros protegidos por el presente código, podrán ser las siguientes:

* Cuestionario rellenado por el cliente.

* Cuestionado rellenado por el responsable del fichero, a través de contacto personal o telefónico con el cliente.

* Otros ficheros promocionales que posea el responsable del fichero objeto del presente código.

* Cuestionario ubicado a tal efecto en la web del responsable del fichero, quien al objeto de garantizar la seguridad del sistema, deberá contar con un sistema de conexión segura SSL DE 128 b.

* Fuentes accesibles al público.

Articulo 5: Deber de Información

Los responsables de los ficheros deberán incluir el sello de garantía en lugar visible del cuestionario o del sistema que utilice para recabar la información de los titulares, ya sea sobre soporte informático o impreso.

Cuando se trate de un cuestionario ubicado en Internet, el sello de garantía integrado en el mismo, tendrá un acceso directo a la página que contenga el texto íntegro del Código y sus anexos.

Además los titulares de datos de carácter personal afectados por el presente código, deberán ser informados de modo expreso, como mínimo, de lo siguiente:

a) De que sus datos de carácter personal van a ser incorporados a un fichero sobre clientes.

b) De los datos de carácter personal contenidos en el cuestionario cuya cumplimentación es obligatoria y de los voluntarios.

c) Del uso que se va a dar a sus datos de carácter personal.

d) De la cesión, en su caso, de sus datos personales.

e) De la identidad y dirección del responsable del fichero o tratamiento.

f) De la posibilidad de ejercitar los derechos de acceso, oposición, rectificación y cancelación, y del modo de ejercerlos.

g) De que el responsable del fichero o tratamiento ha suscrito el presente Código y de la manera de obtenerlo.

h) De la identidad y dirección del responsable del presente código.

Articulo 6: Derecho de oposición.

Se garantiza el derecho de oposición.

El interesado podrá oponerse al registro de sus datos personales en soportes físicos que los haga susceptibles de tratamiento en las siguientes circunstancias:

a) Al tratamiento de sus datos con otros fines que no sean los puramente necesarios para la ejecución de los contratos celebrados o trabajos encomendados.

b) A la cesión de la información a terceros, excepto que la misma sea precisa para la ejecución de los contratos celebrados o de los trabajos encomendados.

Artículo 7: Derecho de acceso.

El titular de los datos tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas de los mismos.

Para la efectividad de este derecho se informará al interesado sobre su posible ejercicio y de los modos de ejercitarlo.

Esta información se facilitará al interesado en los propios cuestionarios que cumplimente, ya sea impreso o a través de internet, o en caso de que la información no haya sido obtenida directamente del interesado remitiéndole esta información por correo. En todos los casos se le facilitarán las direcciones, tanto del responsable del fichero o tratamiento, como del responsable del código, a las que puede dirigirse.

El procedimiento para el ejercicio de estos derechos consistirá en dirigir una comunicación a las direcciones facilitadas, a elección del afectado, es decir, al responsable del fichero o al responsable del Código, que hará de intermediario ante el responsable del fichero. La contestación se efectuará por escrito en un plazo no superior a 10 días.

Si el interesado lo desea se le facilitará por el responsable del fichero o por el responsable del Código, los formularios existentes para el ejercicio de su derecho, siendo su uso voluntario, ya que este derecho se pueden ejercitar en el modo indicado en el párrafo anterior.

En todo caso, el responsable del código asesorará gratuitamente a los titulares de los datos de carácter personal y procurará que el responsable del fichero permita al cliente el acceso a sus datos en tiempo real.

La solicitud del interesado deberá tener un contenido mínimo, que permita la identificación del interesado, así como el poder dirigirse al mismo:

* Nombre, apellidos del interesado y fotocopia de su D.N.I. o cuaquier otro medio que acredite la identidad del interesado.

* Petición en la que se concreta la solicitud.

* Domicilio a efectos de notificaciones, fecha y firma del solicitante.

El derecho de acceso sólo podrá ser ejercitado a intervalos de tiempo no inferiores a 12 meses, salvo que el cliente titular de los datos acredite un interés legítimo, en cuyo caso podrá ejercitarlo antes.

Artículo 8: Derecho de rectificación y cancelación.

Serán rectificados o cancelados los datos de carácter personal cuando resulten inexactos o incompletos o su tratamiento no se ajuste al presente Código o a la Ley de Protección de Datos.

Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar a quien lo hubiera comunicado la rectificación o cancelación de los datos.

Para la efectividad de este derecho se informará al interesado sobre su posible ejercicio y de los modos de ejercitarlo.

Esta información se facilitará al interesado en los propios cuestionarios que cumplimente, ya sea impreso o a través de internet, o en caso de que la información no haya sido obtenida directamente del interesado remitiéndole esta información por correo. En todos los casos se le facilitarán las direcciones, tanto del responsable del fichero o tratamiento, como del responsable del código, a las que puede dirigirse.

El procedimiento para el ejercicio de este derecho consistirá en dirigir una comunicación a las direcciones facilitadas, a elección del afectado, es decir, al responsable del fichero o al responsable del Código, que hará de intermediario ante el responsable del fichero. La contestación se efectuará por escrito en un plazo no superior a 10 días.

Si el interesado lo desea se le facilitará por el responsable del fichero o por el responsable del Código, los formularios existentes para el ejercicio de su derecho, siendo su uso voluntario, ya que este derecho se puede ejercitar en el modo indicado en el párrafo anterior.

En todo caso, el responsable del código asesorará gratuitamente a los titulares de los datos de carácter personal y procurará que el responsable del fichero rectifique o cancele los datos en tiempo real.

La solicitud del interesado deberá tener un contenido mínimo, que permita la identificación del interesado, así como el poder dirigirse al mismo:

* Nombre, apellidos del interesado y fotocopia de su D.N.I. o cuaquier otro medio que acredite la identidad del interesado.

* Petición en la que se concreta la solicitud.

* Domicilio a efectos de notificaciones, fecha y firma del solicitante.

Articulo 9: Finalidad

El interesado podrá, en cualquier momento, determinar la finalidad o finalidades a las que consiente sean destinados sus datos, o excluir alguna finalidad inicialmente consentida.

En ningún caso, se podrá utilizar la información para finalidades distintas de las que haya consentido el interesado.

CAPÍTULO TERCERO
El CÓDIGO ÉTICO ANTE LAS TECNICAS DE INTERNET

Articulo 10: Cookies - Plugins - Active X

Las empresas y profesionales adheridos a este Código se comprometen a no utilizar en sus web cookies - Plugins - Active X que sustraigan información de los equipos que las visitan.

Articulo 11: Explotación de Listas de Datos

Las empresas y profesionales adheridos a este Código se comprometen a no explotar comercialmente sus ficheros. Queda por tanto prohibido en el ámbito de este código ético el alquilar, vender o intercambiar ficheros de datos personales.

Articulo 12: Procedimientos de búsqueda de datos

En evitación de las fugas de datos personales, se prohíbe la instalación de ficheros que contengan datos de carácter personal en páginas estáticas html. Asimismo, los "buscadores" que se instalen en los en los ficheros que contengan datos de carácter personal, podrán dar respuesta por aproximación formando listados dinámicamente.

Artículo 13: Páginas informativas

Las empresas y profesionales adheridos a este Código en su web establecerán un link a la web de ANF donde se podrá acceder al texto del Código ético y a los formularios- que se acompañan con ANEXO al mismo- para el ejercicio de los derechos de acceso, oposición, rectificación o cancelación.

Además, las empresas y profesionales introducirán en su web su denominación completa y dirección.

En el cuestionario de recogida de datos insertado en la web, se facilitará la dirección de correo electrónico, así como de todas las cuestiones contenidas en el artículo 5 del presente Código.

CAPÍTULO CUARTO
MODALIDADES DE UTILIZACIÓN DEL SELLO DE GARANTÍA

Articulo 14: Objeto

El Sello de "Garantía de protección de datos" es el símbolo que representa la adhesión de empresas y profesionales al presente código, y su concesión, posesión o pérdida irá inseparablemente unida al cumplimiento de las normas contenidas en el presente código.

Articulo 15: Obtención

Únicamente las empresas y profesionales adheridos al Código Ético pueden utilizar el Sello de Garantía. La adhesión se realizará por escrito, en el documento al uso creado por el responsable del código, que deberá ser suscrito y remitido a su sede.

Articulo 16: Modalidades de utilización

El objetivo esencial del sello de garantía es el de constituir una marca de homologación, distintiva de posesión y empleo de medios que garantizan la seguridad exigida según el nivel de protección de los datos tratados. Por ello, se considera de interés general el alcanzar la mayor difusión posible del Sello de Garantía, al objeto de que el público en general pueda determinar la existencia de entidades con las que puede operar con absoluta confianza.

Las empresas podrán insertar este Sello de Garantía tanto en páginas electrónicas, en impresos o productos.

Este derecho de uso puede perderse en caso de incurrir en alguno de los supuestos que establece este Código Ético en el Apartado Sanciones.

CAPÍTULO QUINTO
CONTROL DEL CUMPLIMIENTO DE LAS NORMAS DEL CÓDIGO Y RESOLUCIÓN DE LOS LITIGIOS

Artículo 17: Control de cumplimiento

El control del cumplimiento de las normas del código ético se realizará por el **Comité de Protección de Datos de la ANF**, en adelante, El comité.

El Comité fija su domicilio en Barcelona, Gran Via de les Corts Catalanes, 996, 4º 2ª.

El Comité estará compuesto por 3 miembros, uno de los cuales será el Presidente de la Asociación y los dos restantes elegidos por sufragio libre, directo y secreto de entre todos los adheridos a la ANF.

El Comité fijará sus propias normas de funcionamiento interno.

El Comité se reunirá a instancia de su Presidente, que será el de la Asociación, o de cualquiera de sus miembros, siempre que se tenga conocimiento de cualquier violación del presente código ético

Para verificar el alcance de las violaciones o incumplimiento del Código, el Comité contará con la colaboración de un órgano consultivo formado por el Departamento Técnico Informático de ANF, quien emitirá informe a esos efectos.

El Comité realizará un programa anual de auditorías sistemáticas y al azar, entre las empresas que se adhieran voluntariamente al código ético y utilicen el Sello de Garantía, con el fin de comprobar el cumplimiento de las normas que impone el presente código.

En caso de advertir irregularidades, el Comité solicitará informe del órgano consultivo, quien deberá emitirlo en un periodo no superior a 15 días hábiles.

A resultas del informe y dándole traslado del mismo, el Comité oirá a la empresa afectada que podrá valerse de un experto para su defensa.

Realizado este trámite, el Comité adoptará la decisión que estime procedente por mayoría de sus miembros constituidos en junta, imponiendo, en su caso, sanciones acordes con la gravedad de la infracción cometida.

Artículo 18: Presentación de Reclamaciones.

Cuando el titular de los datos personales considere que una empresa que utiliza el **Sello "Garantía TID de Protección de Datos"** ha actuado contra este código ético, podrá tramitar su queja por carta ante el Comité, o compareciendo en sus oficinas.

El Comité contactará con la empresa responsable del fichero o tratamiento para que manifieste lo que considere oportuno. Si de la reclamación efectuada se desprende que la persona denunciante ha sufrido algún tipo de perjuicio o que el asunto le afecta directamente, le dará traslado inmediato de las alegaciones recibidas, asesorándole de los medios que este código ético le ofrece para dirimir el asunto.

Asimismo, se le informará sobre si la empresa o profesional adherido al presente código, han suscrito un sometimiento al **TRIBUNAL DE ARBITRAJE DEL CONSEJO EMPRESARIAL DE LA DISTRIBUCIÓN (TACED)** para la solución de los conflictos que se generen entre ellos y sus clientes en materia de protección de datos de carácter personal. El TACED es una institución independiente especializada en la administración de arbitraje, de la que es parte fundadora la Asociación Nacional de Fabricantes. Esta comunicación se hace a los efectos de que, si es de su interés, el titular de los datos personales, someta también el asunto al conocimiento y solución del TACED, con arreglo a su Reglamento y a la ley de Arbitraje, remitiéndole a la sede del Tribunal de Arbitraje donde le facilitarán la documentación necesaria y cuanta información requiera sobre el procedimiento arbitral.

Igualmente, se asesorará al afectado de los sistemas de tutela de derechos con los que cuenta la Agencia de Protección de Datos.

Artículo 19: Sanciones.

Con independencia de las sanciones legales a que puedan dar lugar las infracciones cometidas, el Comité apreciará en función de la gravedad del caso y de los daños causados, las sanciones a aplicar, que podrán ser de:

1. **Advertencia.** El cumplimiento defectuoso por parte de las empresas o profesionales adheridos al presente código de su deber de información a los clientes en materia de datos de carácter personal, dará lugar a una advertencia por parte de Comité, que requerirá al infractor para que subsane ese defecto en un periodo de tiempo no superior a 30 días.

2. **Amonestación.** Si transcurrido el plazo de 30 días, el infractor persiste en el incumplimiento de su deber de información, recibirá una amonestación del Comité, otorgándole un plazo improrrogable de 10 días para subsanar el defecto.

La violación por las empresas o profesionales adheridos al presente código de los derechos de acceso, oposición, cancelación y rectificación de los interesados dará lugar, asimismo, a una amonestación por parte del Comité, que concederá un plazo improrrogable de 10 días para que se proceda a la subsanación.

Tres advertencias dentro del periodo de un año –contado de fecha a fecha desde la última advertencia computable- darán lugar a amonestación.

3. **Retirada provisional del Sello de Garantía y expulsión provisional del código ético.** La falta de subsanación de las infracciones que den lugar a amonestación, según lo establecido en el punto anterior, darán lugar a la retirada provisional del sello de garantía y expulsión provisional del código ético.

Asimismo, la concurrencia de tres amonestaciones dentro del periodo de un año –contado de fecha a fecha desde la última amonestación computable- dará lugar a la retirada provisional del sello de garantía y expulsión provisional del código ético.

El Comité fijara la duración de la sanción en función de la gravedad del caso y del perjuicio causado, pero en ningún caso la retirada provisional del sello de garantía podrá ser por un plazo inferior a 3 meses.

4. **Retirada definitiva del Sello de Garantía y expulsión definitiva del código ético.** La comisión de tres infracciones que den lugar a la retirada provisional del sello de garantía y consiguiente expulsión provisional del código dentro del periodo de un año –contado de fecha a fecha desde la última retirada provisional del sello de garantía computable- dará lugar a la retirada definitiva del sello de garantía y expulsión definitiva del presente código.

Igualmente, el Comité podrá decidir la retirada definitiva del sello de garantía y consiguiente expulsión definitiva del código en función de la gravedad de la infracción cometida y del perjuicio causado al interesado.

Artículo 20: Notificación.

El Comité notificará a la empresa y a la persona interesada el aviso o sanción acordados.

En el caso de existencia de violaciones a los principios de la ley Orgánica de Protección de Datos de carácter personal, el Comité presentará denuncia ante la Agencia de Protección de Datos.

Artículo 21: Asesoramiento y formación.

El responsable del código facilitará a los adheridos al mismo y a los clientes en general asesoramiento sobre cualquier cuestión relacionada con la protección de los datos de carácter personal. Este servicio será de carácter gratuito.

Asimismo, ANF organizará seminarios y campañas de formación dirigidos a concienciar al mundo empresarial de la necesidad de proteger los datos personales, de sus obligaciones al respecto y de la forma de llevarlo a cabo.

Artículo 22: Adhesiones al Código.

Las empresas o profesionales que se adhieran al presente Código, deberán suscribir un documento que el responsable del código ha elaborado a tal efecto. Este documento será remitido a la ANF, Gran Via de les Corts Catalanes, 996, 4º 2ª, 08018 Barcelona.

La ANF en un plazo no superior a diez días a contar desde aquel en que ha recibido el documento de adhesión, lo comunicará a la Agencia de Protección de Datos, así como todas las altas y bajas que se vayan produciendo.

Asimismo, con carácter anual, la ANF remitirá a la Agencia de Protección de Datos un listado actualizado de los adheridos al Código.

DISPOSICIÓN FINAL

Artículo 23: Revisión y actualización de este Código.

El contenido de este Código se revisará y actualizará siempre que los avances tecnológicos y de comportamiento del sector lo requieran y, como mínimo, cada dos años se planteará la oportunidad de su revisión. La revisión que se

apruebe, deberá presentarse para su inscripción en el **Registro General de la Agencia de Protección de Datos.**

A. EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:.....

Dirección de la Oficina de Acceso:C/.....

nº.....C.P.....Localidad:.....Provincia:.....

(Nota: Si Vd. desconoce la dirección del responsable del fichero puede dirigirse por correo a la ASOCIACIÓN NACIONAL DE FABRICANTES, ANF, con domicilio en Avda. Gran Via de les Corts Catalanes, 996, 4º 2ª, 08018 Barcelona, o al teléfono 93 266 16 14 en horario de 9 a 14 y de 16 a 18 de lunes a viernes. (LA ANF NO DISPONE DE LOS DATOS CONTENIDOS EN EL FICHERO, SINO TAN SÓLO LA DIRECCIÓN DEL RESPONSABLE DEL FICHERO).

DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 7 del Código Ético de protección de datos personales informatizados en oficinas y despachos profesionales.

SOLICITA.-

1.- Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante el Comité de Protección de Datos de la ANF para iniciar el procedimiento de tutela de derechos, establecido en el Código Ético.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En .....a.....de.....de 200..

B. EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamiento incluidos en un fichero

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:.....

Dirección de la Oficina de Acceso: C/..... nº..... C.P..... Localidad:..... Provincia:.....

(Nota: Si Vd. desconoce la dirección del responsable del fichero puede dirigirse por correo a la ASOCIACIÓN NACIONAL DE FABRICANTES, ANF, con domicilio en Avda. Gran Via de les Corts Catalanes, 996, 4º 2ª, 08018 Barcelona, o al teléfono 93 266 16 14 en horario de 9 a 14 y de 16 a 18 de lunes a viernes. (LA ANF NO DISPONE DE LOS DATOS CONTENIDOS EN EL FICHERO, SINO TAN SÓLO DE LA DIRECCIÓN DEL RESPONSABLE DEL FICHERO).

DATOS DEL SOLICITANTE

D/ Dª ..... mayor de edad, con domicilio en la calle .....nº..... Localidad ....., Provincia .....C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 8 del Código Ético de protección de datos personales informatizados en oficinas y despa-

chos profesionales.

SOLICITA.-

1. Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en sus ficheros.

2.Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3.Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4.Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 19 del Código Ético de protección de datos personales informatizados en oficinas y despachos profesionales.

En..... a..... de..... de 200.....

C. EJERCICIO DEL DERECHO DE CANCELACIÓN PARCIAL

Petición de supresión de datos personales objeto de tratamiento incluidos en un fichero

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:.....

Dirección de la Oficina de Acceso : C/..... nº.....

C.P. ..... Localidad .....

Provincia:.....

(Nota: Si Vd. desconoce la dirección del responsable del fichero puede dirigirse por correo a la ASOCIACIÓN NACIONAL DE FABRICANTES, ANF, con domicilio en Avda. Gran Via de les Corts Catalanes, 996, 4º 2ª, 08018 Barcelona, o al teléfono 93 266 16 14 en horario de 9 a 14 y de 16 a 18 de lunes a viernes. (LA ANF NO DISPONE DE LOS DATOS CONTENIDOS EN EL FICHERO, SINO TAN SÓLO DE LA DIRECCIÓN DEL RESPONSABLE DEL FICHERO).

DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia .....C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 8 del Código Ético de protección de datos personales informatizados en oficinas y despachos profesionales.

SOLICITA.-

1.Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de los datos relativos a mi persona que se encuentren en sus ficheros y que se enumeran en el anexo, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento, como se acredita en los documentos aportados.

2.Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

3.Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 19 del Código Ético de protección de datos personales informatizados en oficinas y despachos profesionales.

En..... a..... de..... de 200....

D. EJERCICIO DEL DERECHO DE CANCELACIÓN

Petición de supresión de datos personales objeto de tratamiento incluido en un fichero

DATOS DEL RESPONSABLE DEL FICHERO

Nombre:.....

Dirección de la Oficina de Acceso : C/..... nº.....

C.P. .....Localidad .....

Provincia:.....

(Nota: Si Vd. desconoce la dirección del responsable del fichero puede dirigirse por correo a la ASOCIACIÓN NACIONAL DE FABRICANTES, ANF, con domicilio en Avda. Gran Via de les Corts Catalanes, 996, 4º 2ª, 08018 Barcelona, o al teléfono 93 266 16 14 en horario de 9 a 14 y de 16 a 18 de lunes a viernes. (LA ANF NO DISPONE DE LOS DATOS CONTENIDOS EN EL FICHERO, SINO TAN SÓLO DE LA DIRECCIÓN DEL RESPONSABLE DEL FICHERO).

DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia .....C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 8 del Código Ético de protección de datos personales informatizados en empresas y despachos profesionales.

SOLICITA.-

1. Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.

2. Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

3. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 19 del Código Ético de protección de datos personales informatizados en oficinas y despachos profesionales.

En..... a..... de..... de 200.....

MEMORIA DE 2001 - ANEXO IV - CÓDIGO TIPO DE ACES

1 Presentación

La "AGRUPACIÓ CATALANA D'ESTABLIMENTS SANITARIS" (en adelante ACES), es una asociación privada sin ánimo de lucro integrada por centros y establecimientos sanitarios privados de la Comunidad Autónoma de Cataluña.

La ACES se fundó en el año 1977, bajo la denominación inicial de "Agrupación de Clínicas y Sanatorios Privados de Barcelona", mediante la asociación, como miembros fundadores, de "Clínica Corachán, S.A.", "Policlínica de Barcelona, S.A.", "Hospital Evangèlic", "Institut Barraquer", "Centro Médico Delfos, S.A.", "Clínica Ntra. Sra. De Lourdes", "Clínica Ntra. Sra. Del Pilar".

El depósito de los Estatutos de la asociación se publicó en el Boletín Oficial de la Provincia núm. 118, de 18 de mayo de 1977.

El 7 de octubre de 1992 se presentó a inscripción la modificación del nombre y Estatutos de la Agrupación, pasando a utilizar la actual denominación.

En la actualidad la ACES está integrada por 95 centros o establecimientos sanitarios privados de Cataluña, representando, aproximadamente, el 99% del número de camas y empleados de los centros o establecimientos sanitarios privados no concertados de la Comunidad Autónoma de Cataluña, y mantiene una fuerte tendencia expansiva, como demuestra la reciente incorporación en los últimos meses de 15 nuevos socios.

Se adjunta de Anexo-1 (Pág. 53) una relación actualizada de los miembros de la ACES junto con sus direcciones postales. Las variaciones que se produzcan en adelante se irán introduciendo así que tengan efecto.

Según el art. 1 de sus Estatutos, la ACES es una asociación empresarial constituida al amparo de la Ley 19/1977, de 1 de abril, que tiene como finalidad el asesoramiento, defensa y representación de sus miembros, procurando en todo momento la optimización de métodos de trabajo y objetivos en general atendiendo fundamentalmente a la promoción de sus intereses sociales, laborales, profesionales y culturales.

El art. 7 de los Estatutos regula las finalidades especificas de la ACES dentro del marco de representación, defensa y promoción de los centros sanitarios asociados, enumerando las siguientes:

a) Ostentar delante de toda clase de entidades y organismos públicos la representación de los intereses de sus asociados.

b) Representar igualmente el interés colectivo de sus asociados o un sector de ellos, en toda clase de negociaciones y cuestiones delante de la Administración Pública, centrales sindicales y entidades públicas y privadas.

c) Fomentar la colaboración entre sus socios, promocionando y creando servicios comunes en beneficio de éstos.

d) Promocionar la constitución de fundaciones o entidades no lucrativas para el desarrollo de actividades formativas, docente o complementarias a las asignadas a ACES.

e) Programar y gestionar las acciones adecuadas para conseguir mejoras sociales, técnicas y económicas para sus afiliados.

f) Informar a los organismos públicos de todos las cuestiones relacionadas con sus asociados y emitir toda clase de dictámenes prestando su asesoramiento.

g) Efectuar estudios y proyectos de cualquier tipo relacionados con la actividad de sus asociados, acogiendo y ordenando los datos referentes a aquellos fenómenos que sean de interés para sus asociados, intentando con esto la mejora del nivel del sector.

h) Informar a sus asociados y asesorados de cuantas cuestiones y datos puedan ser de interés para éstos.

i) Elevar ante los organismos que corresponda las iniciativas y aspiraciones de los integrantes de ACES.

j) Dirimir las cuestiones planteadas entre los asociados siempre que le sean sometidas por los mismos o estén dentro de la esfera de la competencia de acuerdo con los Estatutos.

k) Dar soporte y fomentar todas aquellas iniciativas que se le presenten y guarden coherencia con sus objetivos.

l) Informar a sus afiliados de todas aquellas gestiones que se realicen en los aspectos económicos, laborales, legales y técnicos que puedan ser de su interés.

m) En general, cualquier otro que corresponda a su actividad y que pueda redundar a favor o defensa de la ACES y sus miembros.

2 **Condiciones de organización**

2.1 Denominación y finalidad

Como se ha dicho la ACES es una asociación empresarial constituida al amparo de la Ley 19/1977, de 1 de abril, que tiene como finalidad el asesoramiento, defensa y representación de sus miembros, procurando en todo momento la optimización de métodos de trabajo y objetivos en general atendiendo fundamentalmente a la promoción de sus intereses sociales, laborales, profesionales y culturales.

2.2 Ámbito funcional

Conforme al art. 2 de los Estatutos, pueden formar parte de ACES como socios de número las personas físicas o jurídicas que siendo de titularidad privada desarrollen su actividad principal dentro del sector sanitario.

También podrán formar parte de la ACES con carácter de socios de honor aquellas personas o entidades que presten o hayan prestado a la Agrupación o a la Sanidad ayudas o colaboraciones destacadas, siempre previo acuerdo de la Asamblea General de ACES a propuesta de la Junta Directiva.

2.3 Delimitación territorial

El ámbito territorial de la ACES es el de Cataluña.

La ACES podrá federarse, asociarse o establecer colaboración con otros organismos o asociaciones del mismo o diferente ámbito.

2.4 Duración

La ACES está constituida por tiempo indefinido y sólo podrá ser disuelta por los motivos que se establecen en el art. 37 de los Estatutos.

2.5 Personalidad jurídica

La Agrupación tiene personalidad jurídica propia diferente de la de sus asociados y capacidad de obrar para el cumplimiento de sus fines.

2.6 Domicilio

La ACES tiene su domicilio social en la calle Vía Augusta 125, 6º, 7ª, 08006 de Barcelona.

La Junta Directiva por mayoría absoluta de sus miembros podrá acordar el cambio de domicilio y también establecer las delegaciones y representaciones que considere convenientes tanto dentro del territorio catalán como fuera de su ámbito territorial.

2.7 Socios de número

Habrá tres categorías de socios con independencia de los socios de honor previstos por el art. 2:

a) Socios activos
b) Asociados
c) Socios agrupados

Podrán ser "socios activos" las personas físicas o las jurídicas que no sean de titularidad pública que desarrollen su actividad principal dentro del sector de asistencia sanitaria. Se entenderá que la actividad es principal cuando represente como mínimo el 50% de los ingresos de la actividad de acuerdo con las cuentas de los tres últimos ejercicios.

Podrán ser "asociados" las personas físicas o jurídicas que no sean de titularidad pública que, desarrollando también su actividad principal dentro del campo de la asistencia sanitaria lo hagan con vinculación a un socio activo al desarrollar dentro de su ámbito una actividad complementaria o accesoria.

Podrán ser "socios agrupados" las asociaciones existentes dentro del ámbito de Cataluña que agrupen en su seno personas o entidades que no sean de titularidad pública con finalidades similares o análogas a las que representa la ACES.

La admisión de socios en cualquiera de las categorías se hará por la Junta Directiva de la Asociación previa solicitud de la persona interesada y una vez comprobados los datos que se requieren para analizar la procedencia de la solicitud y las características del solicitante.

El acuerdo de admisión efectuado por la Junta directiva será eficaz desde el momento que se adopte, pero se tendrá

que ratificar en la próxima Asamblea General que se celebre. Si se revocase quedará sin efecto la admisión procediendo a devolver al solicitante las cuotas satisfechas hasta aquel momento.

Los socios, excepto los de honor, tendrán derecho a participar en las asambleas y en las comisiones que se puedan crear, y a beneficiarse de todas las actividades de la ACES.

El derecho de voto no obstante sólo corresponderá a los socios activos y a los asociados. Únicamente los socios activos podrán pertenecer a la Junta Directiva.

El voto de los socios activos y asociados será ponderado correspondiendo un voto en todo caso, por el solo hecho de ser socio activo o asociado. En función del número de trabajadores vinculados al socio o asociado con relación laboral el número de votos totales será de la siguiente forma:

Empresas hasta 10 trabajadores:	1 voto		
" entre 11 a 25 "	:	2 votos	
" entre 26 a 50	"	:	3 votos
" entre 51 a 100	"	:	4 votos
" entre 101 a 200	:	5 votos	
" entre 201 o más	:	6 votos	

Los votos ponderados se revisarán cada anualidad por la Junta Directiva durante el último trimestre del año sobre la base de los datos oficiales de los ejercicios anteriores. La falta de entrega de los datos permitirá a la Junta Directiva la suspensión temporal de los votos basados en el número de trabajadores.

La representación de los socios en la Asamblea se llevará a cabo mediante la persona física en quien el titular o en su caso el legal representante del socio delegue por escrito, o mediante el propio legal representante.

Todos los socios podrán formar parte de las comisiones o representaciones que para el desarrollo de las actividades de la ACES pueda crear la Junta Directiva y podrán presentar antes ésta o de la Asamblea todas aquellas iniciativas que puedan creer conveniente para el buen fin y objeto de la Agrupación o para la defensa de sus intereses o de sus asociados. Sólo los socios activos podrán formar parte de la Junta Directiva.

2.8 Deberes de los socios

Son obligaciones de los socios:

a) Cumplir las prescripciones de los Estatutos así como los acuerdos que se adopten por la Asamblea General o Junta Directiva.

b) Asistir a las Asambleas Generales, ejercer los cargos para los que fueron elegidos y aquellas otras tareas y funciones que les encarguen, ya sea en comisiones, delegaciones, asesoramientos y todo lo que represente el mejor cumplimiento de los fines sociales.

c) Contribuir al sostenimiento de la ACES haciendo efectivas las cuotas que periódicamente se establezcan en la cantidad y términos, además de las aportaciones que se fijen.

d) Mantener la solidaridad de los acuerdos y la colaboración necesaria para el buen logro de la misión que la ACES tiene encargada.

e) Mantener dentro del ámbito de su empresa una política de calidad y de control normativo y ético con los principios de la asociación.

2.9 Pérdida de la condición de socio

La condición de socio se perderá:

a) A petición del mismo si lo hace por escrito.

b) Por incumplimiento de las obligaciones establecidas en el artículo anterior después de haber sido advertido de esta eventualidad y, si transcurridos seis meses desde el aviso no se reparase el incumplimiento y siempre previo expediente tal como se prevé seguidamente.

c) Por falta grave contra los principios y normas de la ACES apreciada por la Junta Directiva previo pliego de cargos que se comunicará al infractor para que pueda presentar en un plazo de 10 días naturales sus descargos antes que la Junta Directiva adopte su resolución. En todo caso el acuerdo de la Junta Directiva será recurrible ante la Asamblea General dentro de un término de 30 días naturales sin perjuicio de las acciones judiciales que todo caso correspondan al sancionado.

2.10 Órganos de gobierno

La representación, la gestión y la administración de la Agrupación corresponden a los siguientes órganos de gobierno:

a) La Asamblea General.

b) La Junta Directiva.

2.11 De la Asamblea General

La Asamblea General, válidamente constituida, es el órgano supremo de gobierno de la Agrupación y los acuerdos que ésta adopte de acuerdo con los Estatutos obligan a todos los afiliados.

2.12 Composición

La Asamblea General estará constituida por la totalidad de los socios activos y asociados a la ACES. Los socios agrupados podrán asistir con voz pero sin voto. El número de votos para cada socio es el que resulta del articulo 8 y también el régimen de representación y delegación.

La Asamblea General quedará constituida en primera convocatoria de pleno derecho si asisten la mitad más uno de los socios con derecho de voto que representen la mayoría de votos de la entidad. En otro caso, se constituirá en segunda convocatoria una vez hayan pasado treinta minutos de la hora prefijada, cualquiera que sea el número de asistentes y los votos que se encuentren presentes y representados.

Los acuerdos se tomarán siempre por mayoría de votos presentes o representados excepto cuando se requiera de acuerdo con la Ley o con los Estatutos una mayoría cualificada.

Cualquier socio podrá hacerse representar por otro socio siempre que la delegación sea por escrito, especial para la Asamblea y se encuentre firmada por el socio que haga la delegación o su legal representante.

2.13 Funciones

Son funciones de la Asamblea General:

a) La elección y revocación de la Junta Directiva y de sus miembros.

b) La aprobación de las cuentas del último ejercicio y de la Memoria así como el presupuesto anual de ingresos y gastos.

c) Modificar los Estatutos y el contenido de cualquier norma o acuerdo adoptado con anterioridad por la Asamblea o una Junta Directiva.

d) Establecer la política general y directrices a seguir por la Agrupación.

e) Ratificar las incorporaciones de socios presentadas por la Junta Directiva.

f) Disolver la asocición y determinar la forma de liquidación que se haya de utilizar.

Estas funciones de la Asamblea General no son limitadas en ningún caso, pudiéndolas modificar la propia Asamblea cuando lo considere conveniente.

2.14 Votaciones para la designación de la Junta Directiva

La Asamblea General elegirá, por votación libre y secreta entre sus socios activos a los que hayan de integrar la Junta Directiva. Las candidaturas se presentarán cerradas y habrán de cubrir todo los cargos para los cuales se haya hecho la convocatoria electoral por parte de la Junta Directiva. Los candidatos habrán de ser personas que sean socios activos o que representa a un socio activo que sea persona jurídica siempre que sea designado por el órgano de administración o legal representante de la mencionada persona jurídica y que además ocupe en el si de ella un cargo de representación o ejecutivo a nivel de miembro del Consejo de Administración, gerente, director general o director médico.

El secretario de la Junta Directiva será designado por la propia Junta recayendo el nombramiento en un letrado en ejercicio de cualquier Colegio de Cataluña. El secretario tendrá voz pero no voto en las Juntas Directivas y Asambleas y ocupará el cargo por el tiempo que sea designado sin perjuicio de su reelección.

Las candidaturas se habrán de presentar antes de 72 horas de la hora fijada por la Asamblea y los candidatos serán proclamados por la Junta Directiva si reúnen los requisitos legales y estatutarios.

La elección se hará por mayoría simple de votos presentes o representados de los asistentes a la Asamblea Extraordinaria que con la finalidad de designar a la Junta Directiva se convoque.

2.15 Composición

La Junta Directiva estará constituida por:

* Presidente

* Vicepresidente

* Tesorero

* Secretario

* Siete a nueve vocales

De estos últimos habrá un vocal en representación de los centros de cada una de las provincias de Girona, Lérida y Tarragona, respectivamente; también un vocal para los socios que desarrollen la actividad de internamiento general, otro para los de internamiento socio-sanitario, un tercero para servicios diagnósticos y uno pera los que tienen actividad sin internamiento, excluidos los anteriores. El número de vocales mínimo será pues de 7.

2.16 Periodicidad reuniones y acuerdos

La Junta Directiva se considerará válidamente constituida encontrándose presentes o representados la mitad más uno de sus miembros. La representación sólo se podrá otorgar entre miembros de la Junta Directiva y se hará por escrito especial para cada Junta.

La Junta Directiva se reunirá como mínimo, una vez cada trimestre, sin perjuicio de que lo haga tantas veces como fuere convocada por el Presidente o a petición de tres de sus integrantes.

Los acuerdos se adoptarán por mayoría de votos presentes y representados.

Cada miembro tendrá derecho a un voto.

En caso de empate, se entenderá como voto decisorio el del Presidente.

2.17 Funciones

A la Junta Directiva le corresponde la representación, dirección y administración de la ACES y, en especial, las siguientes funciones:

a) La representación judicial y extrajudicial de la ACES con la facultad de delegar y apoderar y que, por regla general, salvo de delegación expresa, corresponda al Presidente.

b) El cumplimiento y vigilancia de los fines y tareas sociales.

c) Fijar las cuotas periódicas y demás aportaciones de los socios.

d) La formulación de cuentas, confección de presupuestos, memorias y todos los actos relativos a la gestión económica y social de la Asociación.

e) La preparación de las Asambleas, así como la ejecución de los acuerdos adoptados en la reunión.

f) La elaboración y creación de informes, estudios, actividades, servicios o actos necesarios para la obtención de los objetivos fijados por la Asamblea General.

g) La designación del Director General. Sus objetivos serán establecidos por la Junta Directiva.

h) Acordar la exclusión de algún socio por falta de abono de les cuotas sociales.

La resolución acordada por la Junta habrá de ser ratificada ante la Asamblea General que entonces acordará de forma inapelable.

i) Admitir a nuevos socios, activos, asociados o socios agrupados, acuerdo que habrá de ser ratificado por la Asamblea General.

j) La creación de comisiones para cubrir objetivos específicos en forma temporal o permanente.

k) Y todas aquellas atribuciones que se establezcan en los Estatutos o le confiera la Asamblea General.

2.18 Presidente. Atribuciones

El Presidente representa a la ACES ante terceros y dirige de forma habitual tanto la Junta Directiva como la Asambleas Ordinarias y Extraordinarias.

Son funciones específicas del Presidente:

a) Representar a la ACES ante cualquier Administración, Tribunal, Organismo o Sindicato. Tal función representativa se entenderá automáticamente delegada al Vicepresidente en los casos de ausencia del Presidente. Así mismo, podrá ser delegada, cuando lo considere oportuno, en cualquier miembro de la Junta Directiva o en Procuradores de los Tribunales o Abogados cuando la situación lo requiera.

b) Convocar y presidir las Juntas Directivas y Asambleas firmando el Orden del Día y vigilar el cumplimiento de los acuerdos que se tomen.

c) Autorizar con su firma los actos, nombramientos, comunicaciones y demás documentos de la ACES. Podrá delegar en cualquier miembro de la Junta Directiva su representación cuando lo estime pertinente.

d) Apoderar a las personas que sea necesario previa autorización de la Junta Directiva.

2.19 Comisión Permanente.

El Presidente, Vicepresidente, Tesorero, Secretario, formarán la Comisión Permanente de la entidad que se reunirá una vez al mes como mínimo y siempre que lo pida cualquiera de sus miembros. El director general o gerente asistirá con voz y sin voto a las reuniones preparando su celebración. Los acuerdo se tomarán por mayoría de votos presentes o representados. Para que la reunión sea válida habrá de ser previamente convocada con una antelación mínima de 24 horas encontrándose presentes o representados al menos 3 de sus miembros. La representación por escrito especial para cada reunión se tendrá que hacer a favor de algún otro miembro de la comisión.

La Comisión tendrá las facultades que le delegue la Junta Directiva excepto las estatutaria o legalmente indelegables

2.20 El Director General o Director Gerente

El director general o director gerente será elegido por la Junta Directiva.

Le corresponde la dirección general de la ACES, la coordinación de todas sus actividades de acuerdo con las directrices establecidas por la Junta Directiva, y el impulso de la entidad encauzando y proponiendo actuaciones dentro del ámbito competencial de la ACES.

Reportará delante del Presidente, del Tesorero y de la Junta Directiva.

Asistirá con voz y sin voto a las reuniones de la Junta Directiva y de la Asamblea así como a las reuniones de todas las comisiones que se puedan crear.

El Director tendrá las siguientes facultades:

a) Administrar los bienes de la entidad; ejercitar y cumplir toda clase de derechos y obligaciones de la misma; constituir, modificar, ceder y extinguir contratos de todo tipo relativos al objeto de la Asociación y constituir, reconocer, aceptar, pagar y cobrar deudas y créditos.
b) Tomar parte en concursos y subastas, formulando propuestas y aceptando adjudicaciones.
c) Librar, aceptar, avalar, endosar, negociar, descontar, cobrar, pagar, intervenir y protestar letras de cambio, cheques, talones, pagarés y otros efectos; abrir, seguir y cancelar depósitos, libretas de ahorro, cuentas corrientes y de crédito, a la vista o a término; concertar activa o pasivamente créditos comerciales; celebrar, modificar, ceder y extinguir, como arrendataria, contratos de arrendamiento financiero o "leasing" sobre bienes muebles o inmuebles; y, en general, operar en Cajas de Ahorro, bancos, incluido el de España, y otros oficiales, y entidades similares, haciendo cuanto, en general, permitan la legislación y la práctica bancaria.
d) Comparecer en Juzgados y Tribunales, Fiscalías, Delegaciones, Jurados, Comisiones, servicios, Centros, Notarías, Registros y toda clase de oficinas públicas y privadas, Autoridades y Organismos del Estado, Comunidades Autónomas, Provincias y Municipios, en asuntos civiles, penales, administrativos, contencioso y económico-administrativo, gubernativo, laborales, fiscales y eclesiásticos, de todos los grados, jurisdicciones e instancias, promover, instar, seguir, contestar y acabar como actor, solicitante, coadyuvante, requerido, demandado, oponente, o en cualquier otro concepto, toda clase de expedientes, actos, juicios, pretensiones, tramitaciones, quejas, recursos, incluido el de casación, con la facultad de formalizar ratificaciones personales, desistimientos y allanamientos.
e) Otorgar poder a Procuradores, Letrados y Graduados sociales, incluso para recursos extraordinarios de amparo, casación y/o revisión, con o sin facultad de sustitución y revocarlos.
f) Instar actas notariales de presencia y para constancia de hechos y comparecer delante de Notario como requirente o requerido efectuando las pertinentes manifestaciones.

2.21 Modificación de Estatutos

La modificación de los Estatutos se acordará en la Asamblea General Extraordinaria, convocándose con quince días de antelación como mínimo y habiendo de acompañar la convocatoria con el texto de la propuesta.

Para que los acuerdos alcanzados tengan validez se han de adoptar por socios presentes o representados que signifiquen la mayoría de los votos de la entidad.

2.22 Disolución

La "ASSOCIACIÓ CATALANA D'ESTABLIMENTS SANITARIS" se disolverá:

a) Por acuerdo de la Asamblea General adoptado por la mayoría cualificada de votos que se establece en el artículo anterior y también por mayoría de socios. En este caso y el mismo acto se nombrará una Comisión liquidadora de cinco miembros para que se establezca el inventario y se haga la evaluación de los bienes que constituyen el patrimonio de la ACES.

b) Por otros casos previstos en la Ley.

El resultado de esta disolución se asignará de la manera que determine la Asamblea General.

De no acordarse otra cosa por la Asamblea General, actuarán de liquidadores los miembros de la Junta Directiva.

2.23 Disposición final

Todos los supuestos para los cuales no exista nada previsto de forma expresa en los Estatutos pueden, a propuesta de la Junta Directiva, ser establecidos por la Junta Directiva en el Reglamento Interior, que:

a) No podrá contener ninguna estipulación que esté en contradicción con los Estatutos.

b) Sus modificaciones habrán de ser acordadas por la Asamblea General previa propuesta razonada de la Junta Directiva.

3 La ACES y el régimen de protección de datos de carácter personal.

La promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), en desarrollo de lo previsto en el art. 18.4 de la Constitución, conforme al cual "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"; así como lo dispuesto en el art. 9.1 de aquélla:

"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."

Así como el contenido del Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, dictado en desarrollo del citado art. 9.1 de la LORTAD; junto con lo dispuesto en la Disposición transitoria única de aquél respecto a los plazos de implantación de las medidas de seguridad por él reguladas; determinó que los centros y establecimientos sanitarios pertenecientes a la ACES fuesen adaptando, cada uno de ellos por su cuenta, sus sistemas informáticos y bases de datos a las prescripciones de la LORTAD y de su Reglamento.

Con la entrada en vigor el pasado 14 de enero de 2000, de la actualmente vigente Ley Orgánica 15/1999, de 13 de diciembre, Ley de Protección de Datos de Carácter Personal (LOPD o Ley de Protección de Datos), que dispuso la derogación de la LORTAD. El legislador ha ampliado el campo de protección en el ámbito de los datos personales y su tratamiento, pues la nueva Ley de Protección de Datos es de aplicación tanto a los datos personales contenidos en ficheros automatizados -ámbito exclusivo de aplicación de la LORTAD y del Real Decreto 994/1999-, como a los registrados en cualquier clase de soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

La nueva Ley de Protección de Datos reproduce en su art. 9 el contenido del mismo precepto, antes citado, de la LORTAD. Por consiguiente, la obligación genérica que dicho precepto atribuye al responsable del fichero en orden a adoptar las medidas necesarias para garantizar su seguridad se extiende ahora también a los ficheros no automatizados, si bien el Reglamento de Medidas de Seguridad dictado en desarrollo del art. 9 de la LORTAD, sigue limitando su ámbito de aplicación a los ficheros automatizados.

No obstante, debe recordarse que la LOPD, en su disposición adicional primera, con relación a los ficheros y tratamientos preexistentes, establece plazos distintos para proceder a la adecuación a sus prescripciones y para el cumplimiento de la obligación de comunicar su existencia a la Agencia de Protección de Datos, según sean automatizados o no.

Los ficheros y tratamiento automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la Ley antes del 14 de enero de 2003. Mientras que los ficheros no automatizados tienen como fecha límite el 24 de octubre de 2007. Todo ello sin perjuicio del derecho de acceso, rectificación y cancelación por parte de los afectados, que podrán ejercerlos sin esperar ningún plazo,

Por su parte, el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, Real Decreto 994/1999, en su disposición transitoria única, modificada por el Real Decreto 195/2000, esta-

blece los siguientes plazos para la implantación de las medidas de seguridad que regula en los sistemas de información automatizados que se encontraban en funcionamiento a su entrada en vigor:

a) Medidas de seguridad de nivel básico: 26 de marzo de 2000.
b) Medidas de seguridad de nivel medio: 26 de junio de 2000.
c) Medidas de seguridad de nivel alto: 26 de junio de 2002.

La derogación de la LORTAD por la LOPD, con la consecuente y expuesta ampliación del ámbito de protección de los datos de carácter personal a todo tipo de soporte, y la proximidad de los plazos impuestos por el Reglamento de Medidas de Seguridad para su implementación, motivaron un gran número de consultas de los asociados de la ACES sobre las dudas o cuestiones suscitadas en el curso dicho proceso.

3.1 El Código Tipo del art. 32 LOPD.

Las múltiples consultas de los asociados y la previsión del Código Tipo sectorial contenida en el art. 32 de la LOPD, conforme al cual:

"1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos tipo podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél."

Motivaron que desde la ACES se hiciera la reflexión sobre si la mejor manera de colaborar con los asociados en el cumplimiento de su obligación de adaptación al nuevo régimen legal de protección de datos de carácter personal fuese confeccionar un Código Tipo aplicable a todos los centros asociados.

Las ventajas de todo orden que se apreciaron en esta solución condujeron a que finalmente, en la Asamblea General Ordinaria celebrada el pasado 11 de abril de 2000, se acordase por unanimidad de todos los presentes la redacción de un Código Tipo de los previstos en el art. 32 LOPD aplicable a todos los miembros de la ACES.

De las múltiples ventajas que llevaron a adoptar esta decisión podemos destacar las siguientes:

a) Se resuelven de este modo para todos los asociados las múltiples cuestiones y dudas surgidas en el proceso de implementación de la LOPD y del Reglamento de Medidas de Seguridad.

b) Se presta un servicio global a los asociados, proporcionándoles un texto completo, igual para todos, que se someterá a su aprobación definitiva.

c) Se logra, mediante su reparto equitativo entre todos los asociados, una considerable rebaja de los costes que supondría seguir el proceso de adaptación a la legislación aplicable de forma individualizada por cada uno de los centros o establecimientos sanitarios integrados en la ACES.

d) Se consigue implantar un régimen homogéneo de protección de datos de carácter personal en el seno de la ACES, lo que supone ventajas tanto para la propia organización como para los usuarios.

Para la organización por cuanto permite incluir dentro de la imagen de marca de la asociación, como característica de calidad homogénea del colectivo, el esfuerzo corporativo y la sensibilización del grupo en orden a garantizar el respeto a los derechos y libertades de los ciudadanos en el tratamiento de los datos personales de sus usuarios o pacientes, de conformidad con la legislación aplicable.

Para los usuarios, porque la uniformidad del régimen de protección de datos de carácter personal en el seno de la agrupación supone una ventaja añadida para los mismos, proporcionando una seguridad jurídica de otro modo difícilmente alcanzable, evitando la proliferación de diversos procedimientos o regímenes y facilitando el ejercicio de sus derechos y la defensa de sus intereses a los afectados, que sabrán a qué atenerse con relación a la protección de sus derechos vinculados al uso y tratamiento que se dé a sus datos personales en cualquiera de los centros o establecimientos asociados a la ACES.

4 Procedimiento de elaboración y aprobación

Como se ha expuesto, en la Asamblea General Ordinaria de la ACES celebrada el pasado 11 de abril de 2000, se acordó por unanimidad de todos los presentes la redacción de un Código Tipo de los previstos en el art. 32 LOPD aplicable a todos los miembros de la ACES.

Se acompaña de Anexo-2 (Pág. 55) certificación extendida por el Secretario de la ACES en la que se da cuenta de este acuerdo de 11.4.2000.

Concluidos los trabajos de redacción del Código Tipo, se somete la propuesta a la aprobación inicial de la Junta Directiva de la ACES.

El texto aprobado inicialmente por la Junta Directiva de ACES, en su redacción inicialmente propuesta o con las enmiendas introducidas a instancia de la propia Junta Directiva, se remite a la Organización de Consumidores y Usuarios de Catalunya (en adelante OCUC), para que en el plazo de un mes emitia un informe consultivo no vinculante sobre su redactado. En el informe la OCUC propone las modificaciones y enmiendas que considere convenientes. Asimismo, y mediante acuerdo expreso, la OCUC acepta, en su caso, su intervención, con designación de un representante al efecto, en el órgano regulado en el capítulo 9 para la determinación por procedimiento arbitral de las indemnizaciones por los daños y perjuicios que, eventualmente, sufran los afectados.

A la vista del mismo se introducen, en su caso, las modificaciones que se estimen pertinentes y se aprueba definitivamente el Código Tipo por la Junta Directiva de la ACES.

A continuación se remite el texto definitivamente aprobado a cada uno de los miembros de ACES, para que en un plazo de 15 días hábiles efectúen su ratificación y declaración individual y expresa de adhesión y sometimiento al mismo. En el mismo trámite, los asociados también manifestan de forma expresa su inequívoca voluntad de someterse al procedimiento arbitral regulado en el capítulo 9 y a la solución que se adopte conforme al mismo, para solucionar las cuestiones que se susciten respecto a las reclamaciones de daños y perjuicios sufridos por sus pacientes y usuarios como consecuencia de la infracción del régimen establecido en la legislación aplicable y en el presente Código Tipo con relación a los datos de carácter personal que éstos hayan proporcionado o de los que disponga cualquier miembro asociado.

Verificado el trámite anterior, se remite el Código Tipo al Registro General de Protección de Datos, introduciendo finalmente, en su caso, las correcciones que este órgano requiera para efectuar su inscripción.

5 Ámbito de aplicación, eficacia y extensión o desarrollo del Código Tipo

5.1 Ámbito de aplicación

Las disposiciones del presente Código Tipo serán de aplicación a todos los centros y establecimientos sanitarios privados miembros de la ACES, quienes cuidarán de su cumplimiento y de llevarlas a efecto en el seno de sus organizaciones.

Los centros y establecimientos sanitarios que en un futuro entren a formar parte de la ACES deberán efectuar por escrito una declaración expresa de aceptación y sometimiento al mismo.

Sólo quedarán excluidos de la aplicación y sujeción al presente Código Tipo, excepcionalmente, aquellos miembros de la ACES que por su pertenencia a otras corporaciones análogas o por cualquier otra circunstancia, ya cuenten con un Código Tipo equivalente o están en trámite de disponer de uno y hagan declaración expresa de su voluntad de ser excluidos de su ámbito de aplicación.

Cuando en el desarrollo del procedimiento de aprobación del presente Código antes expuesto, se requiera a los miembros de la ACES para su ratificación y adhesión expresa al mismo, aquellos centros y establecimientos que, conforme a lo dispuesto en el párrafo anterior, ya se encuentren sometidos a otro Código Tipo equivalente o en curso de disponer de uno, deberán declararlo expresamente, con indicación precisa del instrumento que les sea de aplicación, así como su voluntad de excluirse de la aplicación del presente.

Los centros sanitarios pertenecientes a ACES que acogiéndose a esta posibilidad se excluyan del ámbito de aplicación del presente Código Tipo se enumerarán en una lista o relación que constituirá el Anexo-3 (Pág. 57) del presente Código y que se mantendrá actualizado con las variaciones que se produzcan. En este documento se hará mención expresa del instrumento equivalente al que estén sujetos estos centros.

5.2 Eficacia

El presente Código Tipo entrará en vigor y será plenamente eficaz desde la fecha de su inscripción en el Registro General de Protección de Datos.

Los centros y establecimientos sanitarios pertenecientes a ACES y sujetos al presente Código, estarán obligados al cumplimiento de sus prescripciones, llevando a puro y pleno efecto su contenido. Para lo cual adoptarán los acuerdos, medidas y acciones que se requieran para adecuar su organización y funcionamiento al mismo en el término de un año desde que la ACES les notifique el texto definitivo objeto de inscripción.

Entre las medidas ha adoptar se incluirán las encaminadas a asegurar la debida instrucción del personal autorizado para acceder a los datos de carácter personal de las disposiciones del presente Código y del régimen de derechos y obligaciones, procedimientos y cautelas que comporta de conformidad con la ley.

5.2.1 Eficacia anticipada de las disposiciones relativas al derecho de acceso, rectificación y cancelación de los afectados

Sin perjuicio de lo anterior, las disposiciones del Código Tipo sobre los derechos y garantías de los afectados relativas al ejercicio de su derecho de acceso, rectificación, oposición y cancelación de sus datos personales, serán de plena aplicación desde que los miembros asociados hayan efectuado la declaración expresa de adhesión y sometimiento al mismo tras su aprobación definitiva por la Junta Directiva.

Hasta que no se produzca la anterior circunstancia, los centros asociados aplicarán, con relación al ejercicio de los derechos de los afectados mencionados, sus disposiciones particulares vigentes al respecto o, en su defecto, el régimen general establecido en la LOPD y, en la medida que resulte aplicable al caso de que se trate, en la Instrucción 1/1998, de 19.1.1998, de la Agencia de Protección de Datos, sobre el ejercicio de los derechos de acceso, rectificación y cancelación de ficheros automatizados.

5.2.2 Incorporación al Reglamento Interior de la ACES. Imperatividad

De conformidad con lo dispuesto en la disposición final de los Estatutos de la ACES, la Junta Directiva incluirá en el Orden del Día de la primera Asamblea General a celebrar tras la entrada en vigor del presente Código Tipo una propuesta para integrarlo, como normas y principios de la Agrupación, en el Reglamento Interior de la entidad.

Tras la aprobación por la Asamblea General, en su caso, de la propuesta comentada, el Código Tipo pasará a formar parte del Reglamento Interior de la ACES, de manera que el incumplimiento de sus prescripciones por algún miembro asociado numerario, se considerará infracción de sus obligaciones sociales -art. 10.a) de los Estatutos y apartado 2.8.a) del presente Código Tipo- y podrá dar lugar al procedimiento para la pérdida de la condición de socio previsto en el art. 11.b) y c) de los Estatutos y en el apartado 2.9.b) y c) del presente Código Tipo.

5.2.3 Desarrollo. Formalización y aplicación del Documento de Seguridad respecto a los ficheros automatizados

Sin perjuicio de que el presente Código Tipo no adquiera plena eficacia hasta su inscripción en el Registro General de Protección de Datos, y dada la inmediatez del vencimiento del plazo legal para adoptar las medidas de seguridad correspondientes al nivel alto (reguladas en el Real Decreto 994/1999), desde que los centros y establecimientos asociados que dispongan de ficheros automatizados se hayan adherido y sometido expresamente al presente Código Tipo -tras la aprobación definitiva del Código por la Junta Directiva-, estarán obligados a desarrollar las prescripciones del mismo relativas al Documento de Seguridad, formalizando uno para su centro de acuerdo con las directrices establecidas y adaptándolo a las circunstancias específicas del centro al que se vaya aplicar.

El término final para el cumplimiento de esta obligación será el establecido en el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (RD 994/1999) para implementar las medidas de seguridad del nivel alto: 26 de junio de 2002.

Si en el trámite de inscripción del presente Código Tipo en el Registro General de Protección de Datos, se introdujesen modificaciones en el mismo que afectasen a sus disposiciones relativas al Documento de Seguridad, los centros asociados, en su caso, adaptarán sus Documentos de Seguridad previos a estas enmiendas y modificaciones en el plazo de treinta días hábiles desde que la ACES notifique sus miembros el redactado definitivo que haya sido objeto de inscripción.

6 Publicidad

6.1 Corporativa

La ACES desarrollará un símbolo, marca o logotipo, que exprese la existencia del presente Código Tipo de protección de datos de carácter personal en la Agrupación y su aplicación y vigencia en los centros asociados.

Se adoptarán los acuerdos precisos para su configuración y para su incorporación a los documentos, circulares y boletines de la Agrupación.

6.2 En los centros sanitarios asociados

Los centros y establecimientos sanitarios miembros numerarios de la Agrupación, que no se hayan excluido, conforme a la excepción prevista en el apartado 5.1 de este Código, del ámbito de aplicación del presente Código Tipo, reproducirán, también, en los documentos o en la carta de presentación que acompañe a los mismos que tengan por destinatarios a los pacientes o usuarios, la marca, símbolo o logotipo al que se refiere el número anterior. Y colocarán un cartel a la vista del público en el departamento de información o recepción de pacientes, así como en los vestíbulos y salas de espera, en el que se informará de la existencia del presente Código Tipo de protección de datos de carácter personal a disposición del público y de su número o referencia de inscripción en el Registro General de Protección de Datos.

Se facilitará un ejemplar de consulta a cualquier usuario que así lo requiera. A este efecto en la oficina de información o de recepción de los centros sujetos al Código dispondrán al menos de dos ejemplares editados del mismo. Sin perjuicio de la posibilidad de habilitar un terminal informático para su consulta electrónica.

Asimismo, se hará entrega de una copia del Código Tipo a cualquier usuario que lo solicite y pague el coste de su reproducción, que se establece en 500,- ptas. Este precio se actualizará anual y automáticamente conforme al Indice de Precios al Consumo a partir del mes siguiente al de su publicación.

No obstante, la Agencia de Protección de Datos facilitará una copia a cualquier persona que lo solicite sin coste alguno.

7 Principios de la protección de datos

En el tratamiento y uso de los datos personales se observarán, de conformidad con lo dispuesto en el Título II de la LOPD, los siguientes principios:

a) Recogida lícita y leal de los datos. Observando siempre las prescripciones legales vigentes y las del presente Código Tipo, respetando la obligación de información y de consentimiento, salvo las excepciones legales, y sin utilizar en ningún caso métodos ilícitos, fraudulentos o subterfugios para obtener la información.

b) Proporcionalidad cualitativa, en función de su destino, de los datos. Éstos deberán ser adecuados y pertinentes en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, y no podrán usarse para finalidades incompatibles con éstas. No se considerará incompatible el tratamiento posterior de aquéllos con fines históricos, estadísticos o científicos.

c) Proporcionalidad cuantitativa de los datos. Éstos no deben ser excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

d) Veracidad de los datos. Deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Si resultaren inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que corresponden a los afectados en orden a su rectificación y cancelación, así como del régimen especial del deber de conservación de las historias clínicas.

e) Conservación limitada de los datos en función de su destino. Los datos personales serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Sin perjuicio del régimen especial del deber de conservación de las historias clínicas.

f) Seguridad física y lógica de los datos. El responsable del fichero y, en su caso, el encargado del tratamiento, deberán garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

8 Obligaciones de los usuarios

Los responsables de los ficheros; es decir, las personas físicas o jurídicas que decidan sobre la finalidad, contenido y uso del tratamiento, y el personal a su cargo autorizado para el uso de los datos de carácter personal, están sujetos al cumplimiento de los siguientes deberes y obligaciones, que desde otro punto de vista constituyen derechos de los afectados.

8.1 Deber de información en la recogida de datos

La LOPD establece que los interesados a los que se les soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

No obstante, la Ley permite omitir la información correspondiente a las letras b), c) y d), si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan y de las circunstancias que se recaban.

En este sentido, al concurrir la circunstancia eximente prevista en la Ley, tanto en la recogida de datos personales relativos a la salud de los pacientes de los centros o establecimientos sanitarios asociados, como en la recogida de datos personales relativos a la gestión del personal laboral o facultativo de aquéllos, se obviará la información mencionada en las letras b) y c).

Este deber de información se cumplimentará entregando al afectado un **Documento de Información** (Pág. 58) en el que figuren los datos recabados y a continuación:

a) Indicación del fichero o tratamiento de datos al que se destinen los recabados.

b) Expresión de la finalidad de la recogida de los datos.

c) Indicación de los destinatarios de la información.

d) Información de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, con indicación de la existencia de este Código Tipo a disposición de los interesados y de los formularios que contiene para el ejercicio de esos derechos, así como de la legislación aplicable, en la actualidad: LOPD 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Instrucción de la Agencia de Protección de Datos de 19.1.1998, número 1/1998, sobre el ejercicio de dichos derechos en los ficheros automatizados.

e) Comunicación de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Del documento de información se entregarán dos copias al interesado, requiriéndole para que firme una que conservará el responsable del fichero, o los usuarios autorizados que recaben personalmente los datos, en el archivo correspondiente al interesado como prueba de la información prestada.

8.2 Obligación de recabar el consentimiento del afectado para el tratamiento de los datos de carácter personal

Con relación a este deber hay que distinguir los supuestos en que el tratamiento tiene por objeto meros datos personales, de cuando lo constituye datos personales relativos a la salud, pues estos últimos están sujetos a un régimen especial.

8.2.1 Datos de carácter personal sujetos al régimen general

Para el tratamiento de datos de carácter personal que no estén especialmente protegidos se exige el consentimiento inequívoco del afectado salvo que la Ley disponga otra cosa.

Por consiguiente, cuando con ocasión de la recogida de estos datos personales se formalice el **Documento de Información** (Pág. 58) al que se ha hecho referencia en el epígrafe 8.1, se completará con una cláusula f) del siguiente tenor literal:

"f) El afectado, titular de los datos personales arriba consignados, al suscribir este Documento de Información autoriza expresamente al responsable del fichero para el tratamiento de esos datos personales para las finalidades expresadas.

8.2.2 Tratamiento de datos de carácter personal relativos a la salud

Los datos personales relativos a la salud están especialmente protegidos y cuentan también con un régimen específico para su tratamiento en atención a su destino.

Conforme al apartado 6 del art. 7 de la LOPD, y por lo que aquí interesa, los datos de carácter personal relativos a la salud podrán ser objeto de tratamiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

Y añade, también podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Asimismo, con relación a los datos personales relativos a la salud el art. 8 LOPD autoriza a las instituciones, a los centros sanitarios, públicos o privados, y a los profesionales correspondientes al tratamiento de los de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad donde, atendiendo a circunstancias especiales relativas a la salud de las personas y de la población en general, se contienen muchas excepciones al régimen general de protección de datos de carácter personal.

Por consiguiente, en el **Documento de Información** (Pág. 58) introducido en el epígrafe 8.1 y desarrollado en el 8.2.1, cuando se refiera a la recogida de datos personales relativos a la salud, se añadirá una cláusula g) del siguiente tenor literal:

"g) El art. 7.6 de la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 15/1999, de 13 de diciembre, autoriza a los profesionales sanitarios sujetos a secreto profesional y a otras personas sujetas a equivalente obligación de secreto, al tratamiento de los datos de carácter personal relativos a la salud cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.

Todo ello sin perjuicio de los supuestos y autorizaciones excepcionales contenidas en la legislación sanitaria estatal y autonómica para casos en que concurra un peligro para la salud de la población o se trate de controlar enfermedades transmisibles o de situaciones de escasez de medicamentos, o demás casos de urgencia previstos en la legislación citada, en los que las autoridades sanitarias podrán ordenar recabar y tratar datos personales de salud sin necesidad de información ni consentimiento de los afectados. Supuesto que no concurre en el presente caso."

8.3 Deber de adoptar medidas de seguridad

El responsable del fichero deberá adoptar las medidas de índoles 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.

8.3.1 Ficheros automatizados

Los responsables de los ficheros automatizados que contengan datos personales deberán redactar un **Documento de Seguridad** para su centro o establecimiento sanitario, conforme a las directrices establecidas en el presente Código Tipo y aplicar las medidas de seguridad de nivel básico, medio o alto según la naturaleza de los datos almacenados en los distintos ficheros existentes.

Los ficheros que contengan datos relativos a la salud deberán satisfacer los requisitos de seguridad correspondientes al nivel alto, que implica cumplir también con las medidas de seguridad de los niveles inferiores: medio y básico.

8.4 Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Este deber de secreto, respecto al personal facultativo, se ve reforzado por lo dispuesto expresamente al respecto en la Ley General de Sanidad.

8.4.1 Compromiso de secreto del personal autorizado

El personal autorizado para acceder a los datos personales objeto de protección, suscribirá un **Compromiso Escrito** (Pág. 61) en el que se expondrá el deber de secreto y de custodia que le sujeta conforme al redactado del punto anterior; las sanciones administrativas y penales, laborales y profesionales (según lo que se dirá a continuación), a que puede dar lugar su incumplimiento; y en el que asumirá personalmente el compromiso de cumplimiento de dichas obligaciones y la eventual responsabilidad patrimonial en la que incurriría en caso de que el centro sanitario al que pertenezca sea sancionado económicamente o deba responder por los daños y perjuicios causados por infracción de dicho deber por conducta imputable personalmente al mismo, en cuyo caso al centro o establecimiento sanitario le asistirán las acciones legales pertinentes para repetir lo pagado por este concepto al personal directa y personalmente responsable de la conducta que haya supuesto la infracción de la obligación de guardar secreto.

Asimismo se adoptarán los acuerdos y negociaciones en su caso pertinentes para incluir esta obligación de guardar secreto y custodia de los datos personales entre las obligaciones profesionales o laborales del personal autorizado para su uso y acceso, pudiendo dar lugar su incumplimiento a las sanciones laborales y profesionales más relevantes, incluso el despido, en función de la gravedad de la conducta infractora y de las circunstancias que concurran, lo que se determinará y establecerá mediante los procedimientos y ante las instancias competentes.

8.5 Obligación de recabar el consentimiento del interesado para la cesión de los datos de carácter personal

La comunicación de los datos de carácter personal a un tercero sólo podrá realizarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y con el previo consentimiento del interesado.

Cuando el responsable del fichero tenga necesidad de comunicar los datos de carácter personal objeto de tratamiento a un tercero, remitirá, por medio que deje constancia del envío y de la fecha de recepción, un comunicado al interesado en el que se expondrán los siguientes extremos:

* Datos identificativos del responsable del fichero cedente: denominación, actividad, dirección postal, teléfono, y en su caso, fax y dirección de correo electrónico.

* Datos de carácter personal del interesado que obran en poder del responsable del fichero y cuya comunicación a un tercero se pretende autorizar.

* Circunstancias en que el responsable del fichero obtuvo los datos que se pretende comunicar, con mención de la información o el consentimiento prestados con ocasión de la recogida de los mismos.

* Finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar.

* La sujeción del cesionario, por el sólo hecho de la comunicación de los datos personales, a las disposiciones de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, de 13 de diciembre.

* La advertencia, gráficamente destacada, de que si no manifiesta lo contrario en el término de 15 días naturales contados a partir del día siguiente al de la recepción del comunicado, se entenderá que presta su consentimiento a la comunicación de sus datos personales expuesta. No obstante, el afectado podrá revocar el consentimiento prestado en cualquier momento. En este caso, la revocación no podrá tener efectos retroactivos.

* Igualmente destacado, el carácter revocable del consentimiento prestado.

8.5.1 Excepciones en la cesión de datos personales relativos a la salud

Urgencias y legislación sanitaria

No se requerirá el consentimiento del interesado cuando la comunicación tenga por objeto datos de carácter personal relativos a la salud y sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sanitaria estatal o autonómica.

Comunicaciones a las compañías aseguradoras de salud

Cuando el interesado utilice los servicios sanitarios bajo la cobertura de un seguro sanitario, el establecimiento sanitario acreedor comunicará a la entidad aseguradora los datos sanitarios estrictamente necesarios para que ésta pueda conocer el acto sanitario prestado y hacer frente a su responsabilidad.

En el **Documento de Información** (Pág. 58) introducido en el apartado 8.1 y desarrollado en los apartado 8.2.1 y 8.2.2, a cumplimentar y entregar al interesado en el momento de recabar sus datos de carácter personal, cuando sean relativos a la salud, se añadirá, destacada gráficamente, una cláusula h) con el siguiente contenido:

"h) Salvo que el interesado manifieste expresamente lo contrario en este documento marcando la opción abajo dispuesta, cuando el interesado utilice los servicios sanitarios bajo la cobertura de un seguro sanitario, el establecimiento sanitario acreedor comunicará a la entidad aseguradora los datos sanitarios estrictamente necesarios para que ésta pueda conocer el acto sanitario prestado y hacer frente a su responsabilidad."

La cláusula constará de un apartado inferior con marco cuadrado vacío para que el interesado pueda marcar la opción negativa con el siguiente enunciado:

* "No se autoriza la comunicación de datos personales a compañías aseguradoras"
Marcar el cuadro con una X si se deniega la autorización, en cuyo caso, la consulta se evacuará y facturará como correspondiente a un paciente particular.

Si el interesado desautoriza la comunicación de los datos de referencia, el centro sanitario se abstendrá de realizarla, y ante cualquier eventual requerimiento de compañías aseguradoras al respecto, se limitará a informar de lo dispuesto por aquél. La consulta se evacuará y facturará como correspondiente a un paciente particular.

8.6 Deber de comunicación de la cesión de los datos

En el momento que se efectúe la primera cesión de datos que requiera el consentimiento del interesado conforme al apartado 8.5, el responsable del fichero deberá informar de ello al afectado. Para ello le remitirá un comunicado por medio que deje constancia de ello, en el que consignará la siguiente información:

* Datos identificativos del responsable del fichero cedente: denominación, actividad, dirección postal, teléfono, y en su caso, fax y dirección de correo electrónico.

* Naturaleza de los datos de carácter personal que han sido objeto de cesión con referencia a la solicitud de autorización de cesión que hayan motivado conforme al apartado 8.5.

* Advertencia de que en adelante las análogas comunicaciones de datos que se produzcan amparadas en la misma autorización no darán lugar a información expresa como la presente.

* Recordatorio de que, no obstante lo anterior, la autorización de comunicación es revocable.

* Datos identificativos del responsable del fichero cesionario: denominación, actividad, dirección postal, teléfono, y en su caso, fax y dirección de correo electrónico.

* Finalidad del fichero para el que han sido cedidos los datos.

8.7 Deber de información al cesionario

Si los datos rectificados o cancelados han sido objeto de cesión previa, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

8.8 Deber de indemnización

Las acciones que corresponden a los afectados para hacer efectivo frente al responsable del fichero el derecho de indemnización por los daños y perjuicios, tanto materiales como morales, que sufran como consecuencia del incumplimiento de las disposiciones legales vigentes de protección de datos de carácter personal, así como del incumplimiento de las disposiciones del presente Código Tipo, podrán ejercitarlas frente a los órganos de la jurisdicción ordinaria o según el procedimiento de determinación arbitral de la indemnización que se regula en el capítulo siguiente.

8.9 Deber de cooperación con la Agencia de Protección de Datos

El responsable del fichero, de conformidad con lo dispuesto en la LOPD y en las disposiciones que la desarrollen, tiene la obligación de cooperar con la Agencia de Protección de Datos, lo que incluye:

* Cumplir puntualmente las instrucciones que dicte el Director de la Agencia.

* Proporcionar la información y documentos que éste o aquélla requieran.

* Remitir a la Agencia las notificaciones previstas en la Ley y en las disposiciones que la desarrollen.

* No obstruir su labor inspectora.

* Permitir el acceso de los inspectores de la Agencia a los locales en que se hallen los ficheros y equipos informáticos previa exhibición por los funcionarios de la autorización expedida al efecto por el Director de la Agencia, salvo que, excepcionalmente, dichos locales tengan la consideración de domicilio particular, en cuyo caso deberán respetarse las reglas que garantizan su inviolabilidad.

* Notificar a la Agencia de Protección de Datos la creación o modificación de un fichero de datos de carácter personal de acuerdo con la reglamentación que se establezca, y comunicando como mínimo la identidad del responsable del fichero, la finalidad del mismo, el tipo de datos que contiene, las medidas de seguridad que cumple, con indicación del nivel exigible, y las cesiones de datos que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

* Y, en general, cumplir con todos sus deberes y obligaciones respecto a la Agencia de Protección de Datos establecidos en la legislación vigente.

9 Derechos y garantías de los afectados

Los principales derechos de los afectados en materia de protección de datos de carácter personal, con independencia de los que constituyen la contrapartida de los deberes y obligaciones del responsable del fichero hasta ahora expuestos, son los de acceso, rectificación y cancelación. Estos derechos han sido regulados por la Agencia de Protección de Datos mediante la Instrucción núm. 1/1998, de 19 de enero, sobre el ejercicio de los mismos en ficheros automatizados.

Siguiendo la línea de homogeneización y simplificación de procedimientos y de respeto a las disposiciones de la legislación aplicable del presente Código Tipo, se recoge a continuación la ordenación en la materia de la mencionada Instrucción núm. 1/1998, extendiendo su ámbito de aplicación, en aquello que resulte aplicable, también a los ficheros no automatizados.

Por lo que respecta a las garantías de los derechos de los afectados, y en relación con el derecho que les asiste de indemnización de los daños y perjuicios sufridos como consecuencia de la infracción de sus derechos en esta materia. Se ha establecido un procedimiento arbitral para su determinación por medio de un órgano mixto formado por un representante de la Agrupación y uno de la Organización de Consumidores y Usuarios de Cataluña (OCUC).

El procedimiento está caracterizado por su simplicidad, brevedad, voluntariedad y principio de vencimiento, pero implica renuncia a las correspondientes acciones civiles del afectado ante la jurisdicción ordinaria si concluye en término. En otro caso no perjudica el derecho a acudir a la jurisdicción ordinaria del afectado, quien, además, si lo prefiere, puede optar por reclamar la defensa de sus derechos ante los Tribunales de Justicia.

Todo ello con independencia de la función de tutela y auxilio a los interesados, y de la función disciplinaria para perseguir y sancionar las infracciones al régimen legal aplicable en la materia, que corresponden en todo caso a la Agencia de Protección de Datos

9.1 Requisitos generales de los derechos de acceso, rectificación, oposición y cancelación de datos

9.1.1 Derechos personalísimos

Estos derechos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad ante el responsable.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o

minoría de edad que le imposibilite el ejercicio personal de sus derechos, en cuyo caso el representante legal deberá acreditar su condición.

9.1.2 De ejercicio independiente

Los derechos de acceso, rectificación y cancelación, son independientes, no constituyendo el ejercicio de ninguno de ellos requisito previo para el ejercicio de otro.

9.1.3 Solicitud

Los derechos se ejercitarán mediante solicitud dirigida al responsable del fichero que contendrá:

? Nombre y apellidos del interesado y fotocopia del documento nacional de identidad del interesado, así como, en los casos excepcionalmente admitidos, de la persona que lo represente y del documento que acredite dicha representación.

? Petición en que se concreta la solicitud.

? Domicilio a efectos de notificaciones, fecha y firma del solicitante.

? Documentos acreditativos de la petición que se formula, en su caso.

9.1.4 Respuesta debida

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros.

Si la solicitud no reúne los requisitos expuestos en el apartado anterior, el responsable del fichero deberá requerir la subsanación de los mismos.

En cualquier caso se empleará algún medio que permita acreditar el envío y la recepción de la respuesta.

9.1.5 Información y ayuda para su ejercicio

El responsable del fichero cuidará que el personal autorizado para acceder a los datos personales conozca y pueda prestar información a los interesados sobre sus derechos de acceso, rectificación y cancelación.

A este efecto, con la documentación que se entregará al personal autorizado junto con el **Compromiso Escrito** (Pág. 61) -regulado en el apartado 8.4.1- que tendrá que suscribir en orden al cumplimiento del deber de secreto y custodia de los datos, figurará la reproducción de las disposiciones de este Código sobre los referidos derechos.

Asimismo estarán a disposición del público los modelos de solicitudes para el ejercicio de estos derechos que se adjuntan al presente Código de **Formularios C, D y E**, (Págs. 97, 98 y 100) para, respectivamente, el derecho de acceso, rectificación y cancelación.

9.2 Derecho de acceso

El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dicho datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

9.2.1 Medios de acceso

El ejercicio del derecho de acceso podrá hacerse, a elección del interesado, por uno de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla
b) Escrito, copia o fotocopia remitida por correo.
c) Telecopia.
d) Cualquier otro procedimiento que sea adecuado a la configuración implantación material del fichero, ofrecido por el responsable del mismo.

9.2.2 Resolución

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación correspondiente.

En el caso de que no disponga de datos personales de los afectados deberá igualmente comunicárselo en el mismo plazo.

Si la resolución fuese estimatoria, el acceso se hará efectivo en el plazo de los 10 días siguientes a la notificación de

aquélla.

9.2.3 Denegación

El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

9.2.4 Información

La información que se proporcione, cualquiera que sea el soporte en que fuera facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

9.3 Derechos de rectificación y cancelación

Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

9.3.1 Efectividad

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

9.3.2 Solicitud de rectificación

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

9.3.3 Solicitud de cancelación

En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

9.3.4 Improcedencia de la cancelación

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

En este sentido, no procederá la cancelación de datos de la Historia Clínica del interesado en virtud del deber de conservación de la misma establecido en la legislación sanitaria.

9.3.5 Contestación

Si solicitada la rectificación o la cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación correspondiente.

Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

9.3.6 Efectos de la cancelación

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales. Cuando acabe el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento, deberá procederse al borrado físico de los datos.

En los casos 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.

Lo mismo se observará cuando la cancelación no proceda por tratarse de datos propios de la Historia Clínica del afectado protegidos por el deber de conservación de las mismas establecido en la legislación sanitaria.

Se exceptúa, no obstante, el supuesto en el 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 que aquéllos figuren.

9.4 Procedimiento arbitral para la determinación de la indemnización de daños y perjuicios

Los afectados que sufran cualquier daño, lesión o perjuicio, tanto material como moral, en sus derechos e intereses legítimos, como consecuencia de la infracción del régimen establecido en la legislación aplicable y en el presente Código Tipo con relación a los datos de carácter personal que haya proporcionado o de los que disponga cualquier miembro asociado, podrán ejercitar las acciones legales correspondientes ante la jurisdicción ordinaria.

Si lo desean, también podrán acudir al procedimiento arbitral aquí establecido para la determinación de la indemnización que les corresponda como consecuencia de los daños y perjuicios sufridos.

Los miembros de ACES, mediante la ratificación y declaración individual y expresa de adhesión y sometimiento al presente Código Tipo, prevista en el capítulo 4, manifestarán también de forma expresa su inequívoca voluntad de someterse al presente procedimiento arbitral y a la decisión que se adopte en su seno, para solucionar las cuestiones que se susciten respecto a las reclamaciones de daños y perjuicios sufridos por sus pacientes y usuarios como consecuencia de la infracción del régimen establecido en la legislación aplicable y en el presente Código Tipo con relación a los datos de carácter personal que éstos hayan proporcionado o de los que disponga cualquier miembro asociado.

9.4.1 Órgano competente

El órgano competente para instruir y resolver el procedimiento arbitral de determinación de la indemnización correspondiente por daños y perjuicios estará compuesto por el Gerente de la ACES o, en su caso, un representante legal designado por éste al efecto, que ejercerá de Presidente del órgano arbitral, un representante de la Organización de Consumidores y Usuarios de Cataluña (OCUC) designado por este ente también expresamente al efecto y una persona de reconocida valía y prestigio, social y profesional, en el ámbito de la sanidad o de la defensa, promoción y protección de los derechos de los ciudadanos o de los consumidores y usuarios, en el territorio de la Comunidad Autónoma de Catalunya, designado al efecto por la Junta Directiva de ACES.

Los acuerdos se adoptarán por mayoría de votos, dirimiendo el empate el voto del Presidente. Si no hubiere acuerdo mayoritario, el laudo será dictado por el Presidente.

9.4.2 Cuantía

La cuantía de la indemnización procedente será de hasta 10.000.000,- ptas.

9.4.3 Procedimiento

El procedimiento estará presidido por las notas de simplicidad, brevedad, voluntariedad y principio de vencimiento, pero implica renuncia a las correspondientes acciones civiles del afectado ante la jurisdicción ordinaria si concluye en término. En otro caso no perjudica el derecho a acudir a la jurisdicción ordinaria del afectado.

<u>9.4.3.1 Iniciación</u>

El interesado que considere que ha sufrido ilegítimamente un perjuicio, daño o lesión, material o moral, como consecuencia de la infracción del régimen legal, o del establecido en este Código Tipo, para la recogida o el tratamiento de los datos personales por parte de algún miembro numerario de la ACES, y desee acogerse al procedimiento arbitral aquí establecido para la determinación de la indemnización correspondiente; presentará ante el responsable del fichero asociado a la ACES una solicitud en ese sentido, en la que constará:

* Declaración expresa e inequívoca de sometimiento voluntario a este procedimiento y a la resolución que en él se dicte, con renuncia, también expresa, en caso de que el mismo termine con una resolución dentro de plazo, a las acciones civiles que le corresponderían ante la jurisdicción civil para la determinación y reclamación de la indemnización correspondiente.

* Datos identificativos del interesado: nombre, apellidos, Documento Nacional de Identidad, domicilio a efectos de notificaciones, teléfono.

* Datos identificativos del responsable del fichero, miembro numerario de la ACES sujeto al presente Código Tipo, cuya actividad haya originado la lesión indemnizable: denominación, dirección, actividad.

* Datos personales con relación a los cuales se ha producido la infracción causante del daño, con indicación de su naturaleza y de la información recibida en el momento de su recogida y, en su caso, del consentimiento prestado para su tratamiento.

* Circunstancias en que se ha producido la infracción. En este apartado el interesado deberá describir la conducta constitutiva de la infracción y las principales circunstancias que considere concurrentes.

* Descripción del daño, lesión o perjuicio sufrido.

* Petición en que se concrete la solicitud, con cuantificación, en su caso, de la indemnización que se reclama.

* Caso de que proceda, documentos acreditativos de la infracción y de la lesión producidas o medios de prueba que proponga la parte.

* Fecha y firma del solicitante

La solicitud se presentará por cualquier medio que permita acreditar la entrega y su fecha. También podrá presentarse personalmente en las oficinas del responsable del fichero, aportando una copia que éste, o su personal autorizado, sellará consignando la fecha y devolviéndosela al interesado.

9.4.3.2 Constitución del órgano arbitral y subsanación de la solicitud

Presentada la solicitud por el interesado, el responsable del fichero la comunicará en el plazo de 10 días de forma fehaciente al Gerente de ACES, quien dará traslado de la misma, también de forma fehaciente y en el mismo plazo, al representante designado al efecto por la OCUC y a la persona de reconocido prestigio designado por la Junta Directiva, así como, en su caso, a su propio representante designado al efecto, convocando la reunión del órgano arbitral.

Los árbitros, en el plazo de quince días naturales contados desde el día siguiente al de su notificación, deberán aceptar por escrito el cargo ante el órgano de su designación y ante el Gerente de ACES, en caso contrario se entenderá que no aceptan el nombramiento y el órgano de designación para cada caso nombrará un sustituto.

Reunido el órgano arbitral, examinará la solicitud, si reúne los requisitos exigidos así lo manifestará en la resolución que notificará los interesados poniéndoles de manifiesto la aceptación del cargo, en caso contrario, si advierte que está incompleta requerirá al interesado para que subsane la falta en el plazo de diez días.

El procedimiento arbitral comenzará cuando los árbitros, mediante la anterior resolución escrita, hayan notificado a los interesados la aceptación del cargo, sin perjuicio de su interrupción hasta que, en su caso, se subsane la solicitud inicial conforme al requerimiento.

9.4.3.3 Vigencia y supletoriedad de la Ley de Arbitraje 36/1988. Oposición, recusación y procedimiento

En todo lo no expresamente regulado aquí y en aquellas de sus disposiciones que eventualmente se opusiesen a lo legalmente establecido, regirá directa o supletoriamente lo dispuesto en la Ley de Arbitraje, Ley 36/1988, de 5 de diciembre.

Así:

a) Las partes podrán actuar por sí mismas o valerse de abogado en ejercicio.

b) La inactividad de las partes no impedirá que se dicte el laudo ni le privará de eficacia.

c) La oposición al arbitraje por falta de competencia objetiva y la recusación de los árbitros se regirá por la regulación contenida al respecto en la Ley de Arbitraje, Ley 36/1988.

d) Los árbitros decidirán el lugar donde se desarrollará la actuación arbitral, así como el lugar en el que deban realizar cualquier actuación concreta, y lo notificarán a las partes.

e) Las partes podrán designar un domicilio a efectos de notificaciones. En su defecto, se entenderá como domicilio el del propio interesado o el de su representante.

f) Los árbitros fijarán a las partes plazos preclusivos para efectuar alegaciones.

g) Las partes podrán presentar sus escritos de alegaciones en cualquiera de los idiomas oficiales en la Comunidad Autónoma de Cataluña, y los árbitros, en atención a la lengua empleada por las partes en sus escritos, decidirán el idioma en que se dicte el laudo.

h) Los árbitros practicarán a instancia de parte, o por propia iniciativa, las pruebas que estimen pertinentes y admisibles en Derecho. A toda práctica de prueba serán citadas y podrán intervenir las partes o sus representantes.

i) Los árbitros podrán solicitar el auxilio del Juez de Primera Instancia del lugar donde se desarrolle el arbitraje, para practicar las pruebas que no puedan efectuar por sí mismos.

j) Si en el curso del arbitraje se incorpora un nuevo árbitro en sustitución de otro anterior, se volverán a practicar todas las pruebas que se hubieren realizado con anterioridad, salvo que el nuevo árbitro se considere suficientemente informado por la lectura de las actuaciones.

k) Los árbitros podrán acordar, una vez practicadas las pruebas, oír a las partes o a sus representantes.

9.4.3.4 Laudo arbitral

9.4.3.4.1 Naturaleza y plazo

El órgano arbitral, hayan presentado o no los interesados alegaciones, dictará resolución conforme a equidad en el plazo de seis meses, contados desde la fecha en que hubieren aceptado la resolución de la controversia o desde el día en que fuera sustituido el último de los componentes del órgano arbitral.

Transcurrido este plazo sin haberse dictado la resolución, caducará el expediente y quedará expedita para el afectado la vía jurisdiccional.

9.4.3.4.2 Contenido

La resolución escrita que ponga fin al expediente instruido, expresará al menos las circunstancias personales de los árbitros y de las partes, el lugar en que se dicta, la cuestión sometida a arbitraje, una sucinta relación de las pruebas practicadas, las alegaciones de las partes y la decisión arbitral, que tendrá alguno de los siguientes contenidos:

a) Declaración de haberse producido una infracción del régimen aplicable a los datos de carácter personal del interesado, con su descripción y la del daño, perjuicio o lesión ocasionado, y determinación de la indemnización de daños y perjuicios procedente.

b) Declaración de inexistencia de la infracción denunciada y de la improcedencia de la indemnización solicitada.

c) Declaración de improcedencia del expediente, ordenando su archivo, por no reunir la solicitud los requisitos exigidos y no haberse subsanado su falta por el interesado.

El laudo será firmado por los árbitros, que podrán hacer constar su parecer discrepante. Si alguno de los árbitros no lo firmase, se entenderá que se adhiere a la decisión de la mayoría.

La resolución se protocolizará notarialmente y se notificará por medio que deje constancia del envío y de la recepción al domicilio señalado por los interesados a efectos de notificaciones.

Los árbitros se pronunciarán en el laudo sobre las costas del arbitraje, que incluirán los honorarios y gastos debidamente justificados de los árbitros, los gastos que origine la protocolización notarial del laudo y su aclaración, los derivados de notificaciones y los que origine la práctica de las pruebas. Las costas no incluirán el coste del servicio prestado por la ACES como administradora del arbitraje, que se reputará gratuito como atención a los pacientes y usuarios de los asociados.

9.4.3.4.3 Eficacia

El laudo arbitral firme produce efectos idénticos a la cosa juzgada. Contra el mismo sólo cabrá el recurso de revisión, conforme a lo establecido en la legislación procesal para las sentencias judiciales firmes.

ANEXO I

Relación de miembros de la Agrupació Catalana d'Establiments Sanitaris (ACES)

Centre	adreça	cp	ciutat
A.T.C. SL	Plaça Gironella, 6-8	08017	BARCELONA
Aliança Mèdica Leridana S.A. - Clínica Montserrat	C. Bisbe Torras, 13	25002	LLEIDA
Analisis Clínicos Dra. Gomis, SL	Avda. Príncep d'Asturies, 63	08012	BARCELONA
Benito Menni, C.A.S.M.	Antoni Pujades, 38	08830	SANT BOI DE LLOBREGAT
BIOPAT , Hospital de Barcelona, S.L.	Avda. Diagonal, 660	08034	BARCELONA
Brugues Assistencial S.A.	Crta Santa Creu de Calafell, 135	08850	GAVA
C A R S A , Centres Assistencials Reunits S.A.	C. Marina, 315	08025	BARCELONA
Centre Faixat SL	C. Ausiàs Marc, 48, pral, 2º	08010	BARCELONA
Centre Cardiovascular Sant Jordi S.A.	Via Augusta, 269	08017	BARCELONA
Centre d'Oftalmologia Barraquer S.A.	C. Muntaner, 314	08021	BARCELONA
Centre de Diagnòstic per la Imatge Dr. Manchón S.A.	Avda. Tibidabo, 9, Torre	08022	BARCELONA
Centre de Rehabilitació L'EIVAX, S.A.	C. Sant Pau, 30	08911	BADALONA
Centre Mèdic de Recuperació Funcional S.A.	C. Marià Cubí, 10, baixos	08006	BARCELONA
Centre Mèdic Delfos S.A.	Avda. Hospital Militar, 127-161	08023	BARCELONA
Centre Mèdic I.T.C.O. SL	Carrasco i Formiguera, 8	08240	MANRESA
Centre Mèdic Manlleu	C. Baixa Cortada, 2	08560	MANLLEU
Centre Mèdic Molins S.A.	C. Pare Manyanet, 1	08750	MOLINS DE REI
Centre Mèdic Quirúrgic Dr. Permanyer	Avda. Catalunya, 43, baixos	08290	CERDANYOLA
Centre Mèdic Rehastet, S.L.	Camí de la Geganta, 31-37	08302	MATARO
Centre Mèdic Teknon SL	C. Vilana, 12	08022	BARCELONA
Centre Sociosanitari de Balaguer SL	C. Urgell, 1	25600	BALAGUER
Centro de Traumatologia Dres. Serrano S.A.	C. Ignacio Iglesias, 5, entlo	08912	BADALONA
Centro de Traumatologia y Ortopedia S.L.	C. Enric Borràs, 14	08912	BADALONA
Clínica Bofill S.L.	Sant Antoni Ma Claret, 20	17001	GIRONA
Clínica Bonanova, Cirurgia Ocular SL	Passeig Bonanova, 22-24	08022	BARCELONA
Clínica Carmelitana	C. Eduardo Toda, 45	08031	BARCELONA
Clínica Catalunya SL	C. Campoamor, 48	08031	BARCELONA
Clínica Císter, SL	C. Císter, 8-10	08022	BARCELONA
Clínica Corachan S.A.	C. Buigas, 19	08017	BARCELONA
Clínica Coroleu SL	C. Coroleu, 44-50	08030	BARCELONA
Clínica de Girona (CARSA)	C. Heroínes Sta. Bárbara, 6	17004	GIRONA
Clínica de l'Esperança	C. Ginesta, 2	17001	GIRONA
Clínica de Lleida (CARSA)	Avda. Prat de la Riba 79-81	25004	LLEIDA
Clínica de Tortosa (CARSA)	Plaça Joaquim Bau, 6-8	43500	TORTOSA
Clínica de Vic (CARSA)	Rda. Francesc Camprodón, 4	08500	VIC
Clínica Dr. Planas	C. Pedro II de Moncada, 16	08034	BARCELONA
Clínica Figarola - HUCASVE S.L.	C. Provença, 340	08037	BARCELONA
Clínica Fundació FIATC	Avda. Diagonal, 648	08017	BARCELONA
Clínica Infantil Stauros	Plaça Karl Marx, núm. 1	08035	BARCELONA
Clínica Monegal (SMASA)	C. López Peláez, 15-17	43002	TARRAGONA
Clínica Ntra. Sra. de Guadalupe S.A.	C. Francesc Moragues, 4	08950	ESPLUGUES DE LLOBREGAT
Clínica Ntra. Sra. del Pilar	C. Balmes, 271	08006	BARCELONA
Clínica Ntra. Sra. del Remei	C. Escorial, 148	08024	BARCELONA
Clínica Ntra. Sra. Lourdes	C. Torrent de l'Olla, 214	08012	BARCELONA
Clínica Provenza S.A.	C. Provença, 279	08037	BARCELONA

ANEXO II

ANEXO III

Relación de miembros de ACES que todavía no se han adherido ni excluido expresamente del presente Código Tipo, pendientes, por tanto, de su adhesión o de su exclusión expresa al mismo con indicación, en este último caso, del instrumento análogo que les resulta de aplicación.

Centre	adreça	cp	ciutat
Benito Menni, C.A.S.M.	Antoni Pujades, 38	08830	SANT BOI DE LLOBREGAT
BIOPAT , Hospital de Barcelona, S.L.	Avda. Diagonal, 660	08034	BARCELONA
Centre Mèdic de Recuperació Funcional S.A.	C. Marià Cubí, 10, baixos	08006	BARCELONA
Centre Mèdic Teknon SL	C. Vilana, 12	08022	BARCELONA
Clínica Bofill S.L.	Sant Antoni Ma Claret, 20	17001	GIRONA
Clínica Catalunya SL	C. Campoamor, 48	08031	BARCELONA
Clínica Ntra. Sra. de Guadalupe S.A.	C. Francesc Moragues, 4	08950	ESPLUGUES DE LLOBREGAT
Clínica Sant Honorat	Avda. Tibidabo, 20	08022	BARCELONA
Clínica Sant Josep	Passeig M. Cinto Verdaguer, 31	08700	IGUALADA
Clínica Santa Creu, S.L.	C. Santa Llogaia, 27	17600	FIGUERES
Corporació Médica Catalana S.L.	Avda. Tibidabo, 20	08022	BARCELONA
Guia'm	C. Narcís Giralt, 62	08202	SABADELL
Institut Català de la Retina SL	C. Pau Alcover, 69-71	08017	BARCELONA
Institut Català de Serveis Mèdics S.A.	Passeig Marítim, 25	08003	BARCELONA
Institut Diagnòstic Dr. Domènech Clarós S.A.	C. Torras i Pujalt, 1	08022	BARCELONA
Institut Poal de Reumatologia	C. Castanyer, 15	08022	BARCELONA
Lab. Dr. F. Echevarne Análisis S.A.	C. Provença, 312, baixos	08037	BARCELONA
Meditrauma S.L.	C. Biada, 119	08301	MATARO
Mutua Penedes	Avda. Tarragona, 6	08720	VILAFRANCA DEL PENEDES
Ortex SL	Avda. Canaletas, 29 bis	08290	CERDANYOLA
Sagrat Cor, Serveis en Salut Mental, GHSCJ	Avda. Compte Llobregat, 117	08760	MARTORELL

DOCUMENTO DE INFORMACIÓN

Nombre	1er. Apellido	2º Apellido

Otros datos personales recabados:

Datos relativos a la salud recabados:

f) Fichero o tratamiento de datos al que se destinan los datos recabados:

g) Finalidad de la recogida de los datos:

h) Indicación de los destinatarios de la información:

i) Los interesados tienen la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de conformidad con lo dispuesto al respecto en la legislación aplicable. En la actualidad: Ley Orgánica de Protección de

Datos de Carácter Personal (LOPD) 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y la Instrucción de la Agencia de Protección de Datos de 19.1.1998, número 1/1998, sobre el ejercicio de dichos derechos en los ficheros automatizados. Este establecimiento cuenta con un Código Tipo de los previstos en el art. 32 LOPD a disposición de los interesados y así como formularios que contiene para el ejercicio de esos derechos.

j) Identidad y dirección del responsable del tratamiento o, en su caso, de su representante:

k) El afectado, titular de los datos personales arriba consignados, al suscribir este Documento de Información autoriza expresamente al responsable del fichero para el tratamiento de esos datos personales para las finalidades expresadas.

Todo ello sin perjuicio de los supuestos y autorizaciones excepcionales contenidas en la legislación sanitaria estatal y autonómica para casos en que concurra un peligro para la salud de la población o se trate de controlar enfermedades transmisibles o de situaciones de escasez de medicamentos, o demás casos de urgencia previstos en la legislación citada, en los que las autoridades sanitarias podrán ordenar recabar y tratar datos personales de salud sin necesidad de información ni consentimiento de los afectados. Supuesto que no concurre en el presente caso.

l) El art. 7.6 de la Ley Orgánica de Protección de Datos de Carácter Personal, Ley 15/1999, de 13 de diciembre, autoriza a los profesionales sanitarios sujetos a secreto profesional y a otras personas sujetas a equivalente obligación de secreto, al tratamiento de los datos de carácter personal relativos a la salud cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.

m) Salvo que el interesado manifieste expresamente lo contrario en este documento marcando la opción abajo dispuesta, cuando el interesado utilice los servicios sanitarios bajo la cobertura de un seguro sanitario, el establecimiento sanitario acreedor comunicará a la entidad aseguradora los datos sanitarios estrictamente necesarios para que ésta pueda conocer el acto sanitario prestado y hacer frente a su responsabilidad.

|| *No se autoriza la comunicación de datos personales a compañías aseguradoras.*

Marcar el cuadro con una X si se deniega la autorización, en cuyo caso, la consulta se evacuará y facturará como correspondiente a un paciente particular.

Compromiso escrito del personal autorizado al acceso y tratamiento de los datos de carácter personal de guardar secreto sobre los mismos

Conforme a la Ley Orgánica de Protección de Datos de Carácter Personal, Ley Orgánica 15/1999, de 13 de diciembre, el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Este deber de secreto, respecto al personal facultativo, se ve reforzado por lo dispuesto expresamente al respecto en la Ley General de Sanidad.

La infracción de este deber, independientemente de las sanciones administrativas a que puede dar lugar conforme a la

Ley Orgánica de Protección de los Datos de Carácter Personal, que configura la vulneración del deber de secreto respecto a los datos de carácter personal relativos a la salud como falta muy grave, castigada con multa de 50 a 100 millones de pesetas, como infracción grave, sancionada con multa de 10 a 50 millones de pesetas, la vulneración del deber de guardar secreto sobre los datos de carácter personal suficientes en su conjunto para obtener una evaluación de las personalidad del individuo, y como falta leve, sancionada con multa de 100.000 a 10 millones de pesetas, el incumplimiento del deber de secreto salvo que constituya infracción grave; además, el incumplimiento del deber de secreto respecto a los datos de carácter personal puede dar lugar a responsabilidad penal tipificada en el Título X del Libro II del vigente Código Penal, donde se castiga con prisión de 1 a 4 años y multa de 12 a 24 meses a quien, sin estar autorizado, acceda, se apodere, altere o utilice, en perjuicio de tercero datos de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, o de cualquier otra clase. Elevándose la pena a prisión de 2 a 5 años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos. Castigándose con pena de prisión de 1 a 3 años y multa de 12 a 24 meses, a quien con conocimiento de su origen ilícito pero sin haber participado en su descubrimiento, los difunda o revele. Si los hechos son cometidos por la persona encargada o responsable del fichero la pena de prisión será de 3 a 5 años, y si se difunden, revelan o ceden se impondrá la pena en su mitad superior.

Constituyen circunstancias agravantes, que supondrán la aplicación de las penas señaladas en su mitad superior, que los datos se refieran a la salud, a un menor o incapaz o que los hechos se cometan con carácter lucrativo. Si además esta última circunstancia va referida a datos de la salud, la pena será de 4 a 6 años de prisión.

El art. 197 del Código Penal establece:

"2. Las mismas penas (prisión de uno a cuatro años y multa de doce a veinticuatro meses) se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
4. Si los hechos descrito en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.
5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o incapaz, se impondrán las penas previstas en su mitad superior.
6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años."

Por su parte el art. 199 CP castiga propiamente la violación del secreto profesional en los siguientes términos:

"1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años."

El que suscribe, cuyos datos personales y ocupación profesional en el establecimiento sanitario de que se trate se consignan a continuación, declara expresa y formalmente conocer:

a) La obligación de guardar secreto que le incumbe con relación a los datos personales a los que está autorizado a acceder en virtud de su responsabilidad profesional, laboral o de cualquier otra naturaleza que ostenta, o con relación a los datos de esa naturaleza a los que accediese por cualquier otra circunstancia.
b) Las consecuencias sancionadoras de orden administrativo y penal que puede acarrear su incumplimiento, así como las eventuales indemnizaciones por responsabilidad de daños y perjuicios que la infracción puede llevar aparejadas.
c) **Y a estos efectos, declara expresa y formalmente su compromiso de cumplir con este deber de guardar secreto, aceptando y asumiendo, en otro caso, su responsabilidad personal frente al titular de los datos personales para resarcirle personalmente de los daños y perjuicios que se le pudieren irrogar al titular como consecuencia de su incumplimiento culpable, aceptando asimismo las consecuencias sancionadoras de orden laboral o profesional que se arbitren al efecto por los procedimientos legalmente procedentes.**

Centro o establecimiento sanitario:

Nombre	1er. Apellido	2º Apellido	Cargo, función, puesto de trabajo o equivalente

En....., ...de.....de 200..

Firmado:

Derechos y garantías de los afectados

Los principales derechos de los afectados en materia de protección de datos de carácter personal, con independencia de los que constituyen la contrapartida de los deberes y obligaciones del responsable del fichero hasta ahora expuestos, son los de acceso, rectificación y cancelación. Estos derechos han sido regulados por la Agencia de Protección de Datos mediante la Instrucción núm. 1/1998, de 19 de enero, sobre el ejercicio de los mismos en ficheros automatizados.

Siguiendo la línea de homogeneización y simplificación de procedimientos y de respeto a las disposiciones de la legislación aplicable del presente Código Tipo, se recoge a continuación la ordenación en la materia de la mencionada Instrucción núm. 1/1998, extendiendo su ámbito de aplicación, en aquello que resulte aplicable, también a los ficheros no automatizados.

Por lo que respecta a las garantías de los derechos de los afectados, y en relación con el derecho que les asiste de indemnización de los daños y perjuicios sufridos como consecuencia de la infracción de sus derechos en esta materia. Se ha establecido un procedimiento arbitral para su determinación por medio de un órgano mixto formado por un representante de la Agrupación y uno de la Organización de Consumidores y Usuarios de Cataluña (OCUC).

El procedimiento está caracterizado por su simplicidad, brevedad, voluntariedad y principio de vencimiento, pero implica renuncia a las correspondientes acciones civiles del afectado ante la jurisdicción ordinaria si concluye en término. En otro caso no perjudica el derecho a acudir a la jurisdicción ordinaria del afectado.

Requisitos generales de los derechos de acceso, rectificación, oposición y cancelación de datos

Derechos personalísimos

Estos derechos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad ante el responsable.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de sus derechos, en cuyo caso el representante legal deberá acreditar su condición.

De ejercicio independiente

Los derechos de acceso, rectificación y cancelación, son independientes, no constituyendo el ejercicio de ninguno de ellos requisito previo para el ejercicio de otro.

Solicitud

Los derechos se ejercitarán mediante solicitud dirigida al responsable del fichero que contendrá:

|| Nombre y apellidos del interesado y fotocopia del documento nacional de identidad del interesado, así como, en los casos excepcionalmente admitidos, de la persona que lo represente y del documento que acredite dicha representación.

|| Petición en que se concreta la solicitud.

|| Domicilio a efectos de notificaciones, fecha y firma del solicitante.

|| Documentos acreditativos de la petición que se formula, en su caso.

Respuesta debida

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros.

Si la solicitud no reúne los requisitos expuestos en el apartado anterior, el responsable del fichero deberá requerir la subsanación de los mismos.

En cualquier caso se empleará algún medio que permita acreditar el envío y la recepción de la respuesta.

Información y ayuda para su ejercicio

El responsable del fichero cuidará que el personal autorizado para acceder a los datos personales conozca y pueda prestar información a los interesados sobre sus derechos de acceso, rectificación y cancelación.

A este efecto, con la documentación que se entregará al personal autorizado junto con el **Compromiso Escrito** -regulado en el apartado 8.4.1- que tendrá que suscribir en orden al cumplimiento del deber de secreto y custodia de los datos, figurará la reproducción de las disposiciones de este Código sobre los referidos derechos.

Asimismo estarán a disposición del público los modelos de solicitudes para el ejercicio de estos derechos que se adjuntan al presente Código de **Formularios C, D y E**, para, respectivamente, el derecho de acceso, rectificación y cancelación.

Derecho de acceso

El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dicho datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Medios de acceso

El ejercicio del derecho de acceso podrá hacerse, a elección del interesado, por uno de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

e) Visualización en pantalla
f) Escrito, copia o fotocopia remitida por correo.
g) Telecopia.
h) Cualquier otro procedimiento que sea adecuado a la configuración implantación material del fichero, ofrecido por el responsable del mismo.

Resolución

El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación correspondiente.

En el caso de que no disponga de datos personales de los afectados deberá igualmente comunicárselo en el mismo plazo.

Si la resolución fuese estimatoria, el acceso se hará efectivo en el plazo de los 10 días siguientes a la notificación de aquélla.

Denegación

El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

Información

La información que se proporcione, cualquiera que sea el soporte en que fuera facilitada, se dará en forma legible e

inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

Derechos de rectificación y cancelación

Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

Efectividad

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

Solicitud de rectificación

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

Solicitud de cancelación

En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

Improcedencia de la cancelación

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

En este sentido, no procederá la cancelación de datos de la Historia Clínica del interesado en virtud del deber de conservación de la misma establecido en la legislación sanitaria.

Contestación

Si solicitada la rectificación o la cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación correspondiente.

Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

Efectos de la cancelación

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales. Cuando acabe el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento, deberá procederse al borrado físico de los datos.

Lo mismo se observará cuando la cancelación no proceda por tratarse de datos propios de la Historia Clínica del afectado protegidos por el deber de conservación de las mismas establecido en la legislación sanitaria.

Se exceptúa, no obstante, el supuesto en el 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 que aquéllos figuren.

FORMULARIO C. (EJERCICIO DEL DERECHO DE ACCESO)

Petición de información sobre los datos personales incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ....., mayor de edad, con domicilio en la C/....., nº...., Localidad....., Provincia.....,CP....., con DNI ..... del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94.

SOLICITA:

1.- Que se le facilite gratuitamente acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y 17 del Real Decreto.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En ....., ... de ..... de 200..

FORMULARIO D. (EJERCICIO DE LOS DERECHOS DE RECTIFICACION)

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamiento incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ....., mayor de edad, con domicilio en la C/ ....., nº ..., Localidad ....., Provincia .....,CP ...., con DNI ..... del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

1.- Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de la solicitud, de los datos inexactos relativos a mi persona que se encuentran en sus ficheros.

2.- Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3.- Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4.- Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ....., .. de ..... de 200..

HOJA ANEXA AL FORMULARIO D

FORMULARIO E. (EJERCICIO DEL DERECHO DE CANCELACION)

Petición de supresión de datos personales objeto de tratamiento incluidos en un fichero.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ..... , mayor de edad, con domicilio en la C/ ....., nº ..., Localidad ....., Provincia .....,CP ...., con DNI ..... del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

1.- Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros al no existir vinculación o disposición legal que justifique su mantenimiento.

2.- Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de datos una vez realizada.

3.- Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ....., .. de ..... de 200..

MEMORIA DE 2001 - ANEXO V - DECISIÓN DE LA COMISIÓN DE 27 DE DICIEMBRE DE 2001

II

(Actos cuya publicación no es una condición para su aplicabilidad)

COMISIÓN

DECISIÓN DE LA COMISIÓN

de 27 de diciembre de 2001

relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados

del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE

[Notificada con el número C(2001) 4540]

(Texto pertinente a efectos del EEE)

(2002/16/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (1), y, en particular, el apartado 4 de su artículo 26,

Considerando lo siguiente:

(1) Con arreglo a la Directiva 95/46/CE, los Estados miembros dispondrán que la transferencia a un tercer país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección de datos adecuado y las disposiciones de Derecho nacional de los Estados miembros, adoptadas con arreglo a los demás preceptos de la presente Directiva, se cumplan con anterioridad a la transferencia.

(2) No obstante, el apartado 2 del artículo 26 de la Directiva 95/46/CE establece que los Estados miembros podrán autorizar, con sujeción a determinadas garantías, una transferencia o una serie de transferencias de datos personales a terceros países que no garanticen un nivel de protección adecuado. Dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la serie de transferencias. El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales creado por dicha Directiva (2) ha emitido directrices que ayudan a realizar la evaluación (3).

(1) DO L 281 de 23.11.1995, p. 31.

(2) La dirección de Internet del Grupo de trabajo es la siguiente:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

(3) WP 4 (5020/97) «Primeras orientaciones sobre la transferencia de datos personales a terceros países Posibles formas de evaluar la adecuación, documento de debate adoptado por el Grupo de trabajo el 26 de junio de 1997. WP 7 (5057/97) Documento de trabajo: «Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?, adoptado por el Grupo de trabajo el 14 de enero de 1998.

WP 9 (5005/98) Documento de trabajo: «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países, adoptado por el Grupo de trabajo el 22 de abril de 1998.

WP 12 Documento de trabajo: «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea adoptado por el Grupo de trabajo el 24 de julio de 1998, se puede consultar en la siguiente dirección de Internet de la Comisión Europea:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp 1 2es.pd

(4) Las cláusulas contractuales tipo solamente están relacionadas con la protección de datos. El exportador de datos y

el importador de datos tienen plena libertad para incluir cualquier otra cláusula sobre cuestiones relacionadas con sus negocios que consideren pertinentes para el contrato, siempre que no contradiga las cláusulas contractuales tipo.

(5) La presente Decisión debe entenderse sin perjuicio de las autorizaciones nacionales que puedan conceder los Estados miembros de conformidad con las disposiciones nacionales de aplicación del apartado 2 del artículo 26 de la Directiva 95/46/CE. La presente Decisión tendrá como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales establecidas en ella proporcionan las garantías adecuadas, por lo que no afectará de ninguna manera a otras cláusulas contractuales.

(6) El ámbito de la presente Decisión se limita a establecer que las cláusulas que contiene pueden ser utilizadas por un responsable del tratamiento de datos establecido en la Comunidad para ofrecer garantías suficientes a efectos del apartado 2 del artículo 26 de la Directiva 95/46/CE para la transferencia de datos personales a un encargado del tratamiento establecido en un tercer país.

(7) La presente Decisión debe aplicar la obligación impuesta en el apartado 3 del artículo 1 7 de la Directiva 95/46/CE, sin perjuicio del contenido de contratos o actos jurídicos establecidos con arreglo a dicha disposición. Sin embargo, algunas de las cláusulas contractuales tipo, en particular las relativas a las obligaciones del exportador de datos, deberían incluirse para aumentar la claridad de las cláusulas que se inserten en los contratos entre responsables y encargados del tratamiento.

(8) Las autoridades de control desempeñan una función esencial en este mecanismo contractual al garantizar la adecuada protección de los datos personales una vez realizada la transferencia. En casos excepcionales en que los exportadores de los datos no quieran o no puedan informar adecuadamente a los importadores de los datos y exista un riesgo inminente de que los interesados sufran un daño grave, las cláusulas contractuales tipo permitirán a las autoridades de control realizar la auditoría de los importadores de los datos y, en su caso, adoptar decisiones vinculantes para éstos. Las autoridades de control de los Estados miembros tendrán la facultad de prohibir o suspender una transferencia o serie de transferencias que se fundamenten en las cláusulas contractuales tipo, en aquellos casos excepcionales en que se demuestre que una transferencia de este género podría tener efectos negativos considerables en las garantías y obligaciones de prestar la adecuada protección al interesado.

(9) La Comisión Europea considerará asimismo en el futuro si las cláusulas contractuales tipo remitidas por las organizaciones empresariales u otras partes interesadas, referidas a las transferencias de datos destinadas a los encargados del tratamiento establecidos en terceros países que no ofrecen un nivel adecuado de protección, ofrecen garantías adecuadas de conformidad con el apartado 2 del artículo 26 de la Directiva 95/46/CE.

(10) La divulgación de datos personales a los encargados del tratamiento establecidos fuera de la Comunidad es una transferencia internacional protegida por el capítulo IV de la Directiva 95/46/CE. Por consiguiente, la presente Decisión no abarca las transferencias de datos personales realizadas por los responsables del tratamiento establecidos en la Comunidad a los responsables del tratamiento establecidos fuera de la Comunidad comprendidas en el ámbito de aplicación de la Decisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE (1).

(11) Las cláusulas contractuales tipo deben estipular las medidas de seguridad técnicas y organizativas necesarias, que han de aplicar los encargados del tratamiento establecidos en un tercer país que no ofrece la protección adecuada, con el fin de garantizar el nivel de seguridad apropiado para los riesgos que entraña el tratamiento y a la naturaleza de los datos que han de protegerse. Las partes estipularán en el contrato aquellas medidas de seguridad técnicas y organizativas que, habida cuenta de la legislación sobre protección de datos aplicable, el estado de la técnica y el coste de su aplicación, resulten necesarias para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, alteración, divulgación o acceso no autorizados o cualquier otra forma ilícita de tratamiento.

(12) Con el fin de facilitar los flujos de datos procedentes de la Comunidad, es deseable que quienes prestan servicios de tratamiento a varios responsables del tratamiento en la Comunidad puedan aplicar las mismas medidas de seguridad técnicas y organizativas, independientemente del Estado miembro del que emane la transferencia, especialmente en aquellos casos en que el importador reciba datos para efectuar nuevos tratamientos desde distintos establecimientos del exportador de datos situados en la Comunidad, en cuyo caso será aplicable la legislación del Estado miembro de establecimiento designado.

(1) DO L 181 de 4.7.2001, p. 19.

(13) Resulta oportuno establecer los detalles mínimos que deberán especificar las partes en el contrato sobre la transferencia. Los Estados miembros deben conservar la capacidad de adaptar la información exigida a las partes. El funcionamiento de la presente Decisión será revisado a la luz de la experiencia adquirida.

(14) El importador de datos tratará los datos personales transferidos sólo en nombre del exportador de datos y de conformidad con las instrucciones que reciba y las obligaciones impuestas en las cláusulas. En particular, el importador de datos no revelará los datos personales a terceros salvo en determinadas circunstancias. El exportador de datos dará instrucciones al importador de datos durante la prestación de los servicios de tratamiento de los datos para que se lleve a cabo de conformidad con sus instrucciones, la legislación vigente de protección de datos y las obligaciones impuestas en las cláusulas. La transferencia de datos personales a los encargados del tratamiento establecidos fuera de la Comunidad se hará sin perjuicio de que las actividades de tratamiento se rijan en cualquier caso por la legislación de protección de datos aplicable.

(15) Las cláusulas contractuales tipo deben ser exigibles no solamente por las organizaciones que sean parte en el contrato, sino también por los interesados, en particular cuando éstos sufran un daño como consecuencia del incumplimiento del contrato.

(16) El interesado tendrá derecho a emprender acciones y, en su caso, percibir una indemnización del exportador de datos que sea el responsable del tratamiento de los datos personales transferidos. Excepcionalmente, también tendrá derecho a emprender una acción y, en su caso, percibir una indemnización del importador de datos en aquellos casos, surgidos del incumplimiento por el importador de datos de cualquiera de sus obligaciones mencionadas en el apartado 2 de la cláusula 3, en que el exportador de datos haya desaparecido de Jacto, haya cesado de existir jurídicamente o sea insolvente.

(17) En caso de conflicto que no se resuelva de manera amistosa entre el interesado, que invoca la cláusula de tercero beneficiario, y el importador de datos, éste aceptará ofrecer al interesado la elección entre mediación, arbitraje o procedimiento judicial. La amplitud de elección real del interesado dependerá de la disponibilidad de sistemas fiables y reconocidos de mediación y arbitraje. La mediación por parte de las autoridades de control de los Estados miembros debe constituir una opción posible, en caso de que éstas presten tal servicio.

(18) El contrato se regirá por la legislación del Estado miembro de establecimiento del exportador de datos que permita al tercero beneficiario exigir el cumplimiento de un contrato. Los interesados podrán ser representados por asociaciones u otros organismos si así lo desean y lo permite la legislación interna.

(19) El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE, ha emitido un dictamen sobre el nivel de protección que ofrecen las cláusulas contractuales tipo incluidas en el anexo, dictamen que se ha tenido en cuenta para la preparación de la presente Decisión (1).

(20) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el artículo 31 de la Directiva 95/46/CE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Se considera que las cláusulas contractuales tipo incluidas en el anexo ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige el apartado 2 del artículo 26 de la Directiva 95/46/CE.

(1) Dictamen n° 7/2001 emitido por el Grupo de trabajo el 13 de septiembre de 2001 (DG MARKT...); se puede consultar en el sitio Internet «Europa» de la Comisión Europea.

Artículo 2

La presente Decisión aborda únicamente la adecuación de la protección otorgada por las cláusulas contractuales tipo establecidas en el anexo para la transferencia de datos personales a los encargados del tratamiento. No afecta a la aplicación de otras disposiciones nacionales por las que se aplique la Directiva 95/46/CE, relacionadas con el tratamiento de datos personales en los Estados miembros.

La presente Decisión no se aplica a la transferencia de datos personales por responsables del tratamiento establecidos en la Comunidad a destinatarios establecidos fuera del territorio comunitario que actúen solamente como encargados del tratamiento.

Artículo 3

A efectos de la presente Decisión:

a) serán aplicables las definiciones contenidas en la Directiva 95/46/CE;

b) se entenderá por «categorías especiales de datos» los datos contemplados en el artículo 8 de dicha Directiva;

c) se entenderá por «autoridad de control» la autoridad contemplada en el artículo 28 de dicha Directiva;

d) se entenderá por «exportador de datos» el responsable del tratamiento que transfiera los datos personales;

e) se entenderá por «importador de datos» el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador de datos personales para su posterior tratamiento en nombre de éste, de conformidad con sus instrucciones y los términos de la presente Decisión, y que no esté sujeto al sistema de un tercer país por el que se garantice la protección adecuada;

se entenderá por «legislación de protección de datos aplicable» la legislación que protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la vida privada respecto del tratamiento de los

datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos;

g) se entenderá por «medidas de seguridad técnicas y organizativas» las destinadas a proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o cualquier otra forma ilícita de tratamiento.

Artículo 4

1. Las autoridades competentes de los Estados miembros, sin perjuicio de su facultad para iniciar acciones destinadas a garantizar el cumplimiento de las disposiciones Derecho nacional adoptadas con arreglo a los capítulos II, III, y VI de la Directiva 95/46/CE, podrán ejercer sus facultades para prohibir o suspender los flujos de datos hacia terceros países con objeto de proteger a las personas físicas en relación con el tratamiento de sus datos personales en los casos siguientes:

a) si se determina que la legislación a la que está sujeto el importador de datos le impone desviaciones de la legislación de protección de datos aplicable que vayan más allá de las restricciones necesarias en una sociedad democrática, como establece el artículo 13 de la Directiva 95/46/CE, cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías proporcionadas por las cláusulas contractuales tipo;

b) si una autoridad competente decide que el importador de datos no ha respetado las cláusulas contractuales del anexo, o

c) si existe la probabilidad sustancial de que las cláusulas contractuales tipo contenidas en el anexo no se estén respetando, o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados.

2. La prohibición o suspensión con arreglo al apartado 1 se levantará tan pronto como desaparezcan las razones para dicha prohibición o suspensión.

3. Cuando los Estados miembros adopten medidas de conformidad con los apartados 1 y 2, informarán inmediatamente de ello a la Comisión, que remitirá la información a los demás Estados miembros.

Artículo 5

La Comisión evaluará el funcionamiento de la presente Decisión basándose en la información disponible tres años después de su notificación a los Estados miembros. Informará de los resultados al Comité creado en virtud del artículo 31 de la Directiva 95/46/CE. Incluirá cualquier prueba que pudiera afectar a la evaluación relativa a la adecuación de las cláusulas contractuales tipo y cualquier prueba de que la presente Decisión se esté aplicando de manera discriminatoria.

Artículo 6

La presente Decisión será aplicable a partir del 3 de abril de 2002.

Artículo 7

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 27 de diciembre de 2001.

Por la Comisión

Frederik BOLKESTEIN

Miembro de la Comisión

ANEXO

Cláusulas contractuales tipo (del tratamiento»)

A efectos del apartado 2 del artículo 26 de la Directiva 95/46/CE para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos.

Nombre de la entidad exportadora de los datos ...

Dirección

..

Tel: fax: .. correo electrónico:

Otros datos necesarios para identificar a la entidad .

en adelante, el exportador de datos

Nombre de la entidad importadora de los datos ...

Dirección ..
..
Tel: fax: .. correo electrónico:

Otros datos necesarios para identificar a la entidad .

en adelante, el importador de datos

ACUERDAN las siguientes cláusulas contractuales (en adelante, «las cláusulas») con objeto de ofrecer garantías suficientes respecto de la protección de la vida privada y de los derechos y libertades fundamentales de las personas para la transferencia por el exportador de datos al importador de datos de los datos personales especificados en el apéndice 1.

Cláusula 1

Definiciones

A los efectos de las presentes cláusulas:

a) «datos personales», «categorías especiales de datos», «tratamiento», «responsable del tratamiento». «encargado del tratamiento», «interesado» y autoridad de control tendrán el mismo significado que en la Directiva 95J46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 995, 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 (en adelante, «la Directiva»((]);

h) por «exportador de datos» se entenderá el responsable del tratamiento que transfiera los datos personales:

c) por «importador de ciatos» se entenderá el encargado del tratamiento que convenga en recibir del exportador de ciatos personales para su posterior tratamiento en nombre de éste. De conformidad con sus instrucciones y los términos de las presentes cláusulas y que no esté sujeto al sistema de un tercer país por el que se garantice la protección adecuada:

ci) por «legislación de protección de datos aplicable» se entenderá la legislación que protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos:

e) por «medidas de seguridad técnicas y organizativas» se entenderán las destinadas a protegerlos datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o cualquier otra forma ilícita de tratamiento.

Cláusula 2

Detalles de la transferencia

Los detalles de la transferencia, en particular, las categorías especiales de los datos personales, quedan especificados si procede en el apéndice 1, que forma parte integrante de las presentes cláusulas.

1 a partes podrán reproducir en esta cláusula las definiciones y significados de la Directiva 95/46/CF. si consideran que ello beneficia a la autonomía del contrato.

Cláusula 3

Cláusula de tercero beneficiario

Los interesados podrán exigir al exportador de datos el cumplimiento de la presente cláusula, las letras h) ah) de la cláusula 4. las letras a) a e) y g) de la cláusula 5, los apartados 1 y 2 de la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9, 10 y 11 como terceros beneficiarios.

Los interesados podrán exigir al importador de datos el cumplimiento tic la presente cláusula, las letras a) a e) y g) de la cláusula 5, los apartados 1 y 2 de la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9. 10 y 11 cuando el exportador haya desaparecido de Jacto o haya cesado de existir jurídicamente.

Las partes no se oponen a que los interesados estén representados por tina asociación u otras entidades si así lo desean expresamente y lo permite el Derecho nacional.

Cláusula 4

Obligaciones del exportador de datos

El exportador de datos acuerda y garantiza lo siguiente:

a) el tratamiento de los datos personales, incluida la propia transferencia, ha sido efectuado y seguirá efectuándose de conformidad con las normas pertinentes de la legislación de protección de datos aplicable y, si procede, se ha notificado a las autoridades correspondientes del Estado miembro de establecimiento del exportador de datos) y no infringe las disposiciones legales o reglamentarias en vigor en dicho Estado miembro:

4 ha dado al importador de datos, y dará durante la prestación de los servicios de tratamiento de los datos personales. Instrucciones para que el tratamiento de los datos transferidos se lleve a cabo exclusivamente en nombre del exportador de datos y de conformidad con la legislación de protección de datos aplicable y con las presentes cláusulas:

c) el importador de datos ofrecer garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas en el apéndice 2 del presente contrato:

d) ha verificado que, de conformidad con la legislación de protección de datos aplicable, dichas medidas resultan apropiadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o contra cualquier otra forma ilícita de tratamiento y que dichas medidas garantizan un nivel de seguridad apropiado a los riesgos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y el coste de su aplicación;

e) asegurará que dichas medidas se lleven a la práctica:

O si la transferencia incluye categorías especiales de datos, se habrá informado a los interesados, o serán informados antes de que se efectúe aquélla, o en cuanto sea posible, de que sus datos podrán ser transferidos a un tercer país que no proporciona la protección adecuada:

g) aceptará enviar la notificación recibida del importador de ciatos a la autoridad de control de la protección de datos, de conformidad con la letra h) de la cláusula 5, en caso de que decida proseguir la transferencia o levantar la suspensión:

h) pondrá a disposición de los interesados, previa petición de éstos, una copia de las presentes cláusulas, a excepción del apéndice 2, que será sustituido por una descripción sumaría de las medidas de seguridad.

Cláusula 5

Obligaciones del importador de datos

El importador de datos acuerda y garantiza lo siguiente:

a) tratará los datos personales transferidos sólo en nombre del exportador de datos y de conformidad con sus instrucciones y las presentes cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, informará de ello sin demora al exportador de datos..cii cuyo caso éste estará facultado para suspender la transferencia de los datos y/o rescindir el contrato:

hj no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que en caso de modificación de la legislación que pueda tener un importante efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso éste estará facultado para suspender la transferencia de los datos y/o rescindir el contrato:

c) ha puesto en práctica las medidas de seguridad, técnicas y organizativas que se indican en el apéndice 2 antes de efectuar el tratamiento de los datos personales transferidos;

(1 Las obligaciones impuestas por la legislación nacional aplicables al importador de datos que no vayan más allá de las restricciones necesarias en una sociedad democrática con arreglo a los intereses recogidos en el apartado 1 del artículo 13 de la Directiva 95/46/ es decir, si dichas obligaciones constituyen una medida necesaria para la salvaguardia de la seguridad del Estado. la defensa, la seguridad pública, la prevención. investigación, detección y enjuiciamiento de cielitos o infracciones de la deontología en las profesiones reguladas, un interés económico o financiero importante del Estado. o la protección del interesado o de los derechos y libertades de otras personas no están en contradicción con las cláusulas contractuales tipo. Algunos e de obligaciones que no van más allá de las restricciones necesarias en tina sociedad democrática son, entre otras, las sanciones reconocidas en el ámbito internacional, las obligaciones de notificación en materia fiscal o las impuestas por la lucha contra el blanqueo de dinero.

d) notificación sin demora al exportador de datos:

i) toda solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de la ley a menos que esté prohibido, por ejemplo, por el Derecho penal para preservar la confidencialidad de una investigación llevada a cabo por una de dichas autoridades,

1) todo acceso accidental o no autorizado,

iii) toda solicitud sin respuesta recibida directamente de los interesados, a menos que se le autorice:

e) tratará adecuadamente en los períodos de tiempo prescritos todas las consultas del exportador de datos relacionadas con el tratamiento que éste realice de los datos personales sujetos a transferencia y se atendrá a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos;

U ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;

g) pondrá a disposición de los interesados, previa petición de éstos, una copia de las cláusulas establecidas en el presente anexo, a excepción del apéndice 2, que será sustituido por una descripción sumaría de las medidas de seguridad, en aquellos casos en que el interesado no pueda obtenerlas directamente del exportador de datos.

Cláusula 6

Responsabilidad

1. Las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las disposiciones mencionadas en la cláusula 3 tendrán derecho a percibir una compensación del exportador de datos por el daño sufrido.

2. En caso de que el interesado no pueda interponer contra el exportador de datos la acción a c se refiere el apartado 1 por incumplimiento de sus obligaciones impuestas en la cláusula 3 por haber desaparecido de Jacto, cesado de existir jurídicamente o ser insolvente, el importador de datos acepta que el interesado pueda demandarle a él en el lugar del exportador de datos.

3. Las partes acuerdan que si una de ellas es considerada responsable de un incumplimiento de las cláusulas cometido por la otra parle, ésta indemnizará, en la medida de su responsabilidad, a la primera parte por todo coste, carga, perjuicio, gasto o pérdida en que haya incurrido.

La indemnización dependerá de que:

a) el exportador de datos notifique sin demora al importador la reclamación. y

b) el importador tic datos tenga la posibilidad de colaborar con el exportador en la defensa y resolución de la reclamación (1).

Cláusula 7

Mediación y jurisdicción

1. El importador de datos acuerda que si el interesado invoca en su contra derechos de tercero beneficiario y/o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del interesado de:

a) someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control;

b) someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador de datos.

2. El importador de datos acuerda que, por convenio con el interesado, la resolución de un determinado conflicto podrá remitirse a un organismo de arbitraje, siempre que e importador de datos esté establecido en un país que haya ratificado la Convención de Nueva York sobre ejecución de laudos arbitrales.

3. Las partes acuerdan que las opciones del interesado no obstaculizaran sus derechos sustantivos o procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

Cláusula 8

Cooperación con las autoridades de control

1. El exportador de datos acuerda depositar una copia del presente contrato ante la autoridad de control si así lo requiere o si el depósito es exigido por la legislación de protección de datos aplicable.

2. Las partes acuerdan que la autoridad de control está facultada para auditar al importador en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable.

FI apartado 3 es optativo

Cláusula 9

Legislación aplicable

Las cláusulas se regirán por la legislación del Estado miembro de establecimiento del exportador de datos, a saber

Cláusula 10

Variación del contrato

Las partes se comprometen a no variar o modificar los términos de las presentes cláusulas.

Cláusula 11

Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales

1. Las partes acuerdan que una vez finalizada la prestación de los servicios de tratamiento de los datos personales, el importador deberá, a discreción del exportador. o bien devolver todos los datos personales transferidos y sus copias o bien destruirlos por completo y certificar esta circunstancia al exportador, a menos que la legislación aplicable al importador le impida devolver o destruir total o parcialmente los datos personales transferidos. En tal caso, el importa - dor de datos garantiza que guardará el secreto de los datos personales transferidos y que no volverá a someterlos a tratamiento.

2. El importador de datos garantiza que, a petición del exportador y/o de la autoridad de control, pondrá a disposición sus instalaciones de tratamiento de los datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1.

En nombre del exportador de datos:

Nornbre (completo) .

Cargo

Dirección .

.

Otros datos necesarios con vistas a la obligatoriedad del contrato (en caso de existir) ..

.

Firma .

(sello de la entidad)

En nombre del importador de datos:

Nombre (completo) ..

Cargo

Dirección ..

Otros datos necesarios con vistas a la obligatoriedad del contrato (en caso de existir) ...

..

Firma .

(sello de la entidad)

Apéndice 1

A las cláusulas contractuales tipo

El presente apéndice forma parte integrante de las cláusulas y deberá ser cumplimentado y suscrito por las panes.

(* Los Estados miembros podrán completar o especificar de acuerdo con sus procedimientos nacionales, cualquier información que deba incluirse en el presente apéndice.).

Exportador de datos

El exportador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

Importador de datos

El importador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

Interesados

Los datos personales transferidos se refieren a las siguientes categorías de interesados (especifíquense):

Categorías de datos

Los datos personales transferidos se refieren a las siguientes categorías de datos (especifíquense):

Categorías especiales de datos (si es pertinente)

Los datos personales transferidos se refieren a las siguientes categorías especiales de datos delicados (especifíquen - se)

Operaciones de tratamiento

Los datos personales transferidos serán sometidos a las operaciones básicas de tratamiento siguientes (especifíquen - se):

EXPORTADOR DE DATOS IMPORTADOR DE DATOS

Nombre .

Firma autorizada

Apéndice 2

A las cláusulas contractuales tipo

El presente apéndice forma parte integrante de las cláusulas y deberá ser cumplimentado y suscrito por las partes

Descripción de las medidas de seguridad técnicas y organizativas puestas en práctica por el importador de datos de conformidad con la letra c) de la cláusula 4 y la letra c) de la cláusula 5 (o documento o legislación adjuntos):

MEMORIA DE 2001 - ANEXO VI - DECISIÓN DE LA COMISIÓN DE 15 DE JUNIO DE 2001

II

(Actos cuya publicación no es una condición para su aplicabilidad)

COMISIÓN

DECISIÓN DE LA COMISIÓN

de 15 de junio de 2001

relativa a cláusulas contractuales tipo pan la transferencia de datos personales a un tercer país

previstas en la Directiva 95/46/CE

[notificada con el número C(2001) 1539]

(Texto pertinente a efectos del EEE)

(2001/497/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (1), y, en particular, el apartado 4 de su artículo 26,

Considerando lo siguiente:

(1) Con arreglo a la Directiva 95/46/CE, los Estados miembros dispondrán que la transferencia a un tercero país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección de datos adecuado y las disposiciones de Derecho nacional de los Estados miembros, adoptadas con arreglo a los demás preceptos de la presente Directiva, se cumplan con anterioridad a la transferencia.

(2) No obstante, el apartado 2 del artículo 26 de la Directiva 95/46/CE establece que los Estados miembros podrán autorizar, con sujeción a determinadas garantías, una transferencia o una serie de transferencias de datos personales a terceros países que no garanticen un nivel de protección adecuado. Dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la serie de transferencias. El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales creado por dicha Directiva (2) ha emitido directrices que ayudan a realizar la evaluación (3).

(1) DO L 281 de 23.11.1995, p. 31.

(2) La dirección web del Grupo de trabajo es la siguiente:

http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

(3) WP 4 (5020/97) «Primeras orientaciones sobre la transferencia de datos personales a terceros países Posibles formas de evaluar la adecuación, documento de debate adoptado por el Grupo de trabajo el 26 de junio de 1997. WP 7 (505 7/97) «Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un tercer país?, documento de trabajo adoptado por el Grupo de trabajo el 14 de enero de 1998.

WP 9 (3005/98) «Conclusiones preliminares sobre la utilización de disposiciones contractuales en caso de transferencia de datos personales a terceros países, documento de trabajo adoptado por el Grupo de trabajo el 22 de abril de 1998.

WP 12 «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», documento de trabajo adoptado por el Grupo de trabajo el 24 de julio de 1998; se puede consultar en la siguiente dirección web de la Comisión Europea:

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp 1 2es.pd

(4) El apartado 2 del artículo 26 de la Directiva 95/46/CE, que ofrece flexibilidad para una entidad que desee transferir datos a terceros países, y el apartado 4 del mismo artículo, que establece cláusulas contractuales tipo, son esenciales

para mantener el necesario flujo de datos personales entre la Comunidad Europea y terceros países sin imponer cargas innecesarias a los operadores económicos. Ambos artículos cobran especial importancia en vista de la escasa probabilidad de que la Comisión adopte resoluciones de adecuación de conformidad con el apartado 6 del artículo 25 para numerosos países a corto o incluso medio plazo.

(5) Las cláusulas contractuales tipo son sólo una de las diversas posibilidades recogidas en la Directiva 95/46/CE para la transferencia legítima de datos personales a un tercer país, junto con el artículo 25 y los apartados 1 y 2 del artículo 26. Facilitarán enormemente a las entidades la transferencia de datos personales a terceros países mediante la incorporación de las cláusulas contractuales tipo en un contrato. Las cláusulas contractuales tipo solamente están relacionadas con la protección de datos. El exportador de datos y el importador de datos tienen plena libertad para incluir cualquier otra cláusula sobre cuestiones relacionadas con sus negocios, tales como cláusulas sobre asistencia mutua en caso de conflicto con un interesado o una autoridad de control, que consideren pertinentes para el contrato, siempre que no contradiga las cláusulas contractuales tipo.

(6) La presente Decisión debe entenderse sin perjuicio de las autorizaciones nacionales que puedan conceder los Estados miembros de conformidad con las disposiciones nacionales de aplicación del apartado 2 del artículo 26 de la Directiva 95/46/CE. Las circunstancias de las transferencias específicas pueden exigir que los responsables del tratamiento de datos proporcionen distintas garantías a efectos del apartado 2 del artículo 26. En todo caso, la presente Decisión tendrá como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales descritas en ella proporcionan las garantías adecuadas, por lo que no afectará de ninguna manera a otras cláusulas contractuales.

(7) El ámbito de la presente Decisión se limita a establecer que las cláusulas contenidas en su anexo pueden ser utilizadas por un responsable del tratamiento establecido en la Comunidad para ofrecer garantías suficientes a efectos del apartado 2 del artículo 26 de la Directiva 95/46/CE. La transferencia de datos personales a terceros países es una operación de tratamiento en un Estado miembro, cuya legitimidad está sujeta a las disposiciones de Derecho nacional. Las autoridades de control de los Estados miembros, en ejercicio de sus funciones y capacidades recogidas en el artículo 28 de la Directiva 95/46/CE, seguirán siendo competentes para evaluar si el exportador de datos ha cumplido la legislación nacional por la que se aplica lo dispuesto en la Directiva 95/46/CE y, en particular, toda regla específica relativa a la obligación de comunicar la información a tenor de la misma.

(8) La presente Decisión no cubre la transferencia de datos personales por responsables del tratamiento establecidos en la Comunidad a destinatarios establecidos fuera del territorio comunitario que actúen solamente como encargados del tratamiento. Estas transferencias no exigen las mismas garantías porque el encargado del tratamiento actúa exclusivamente en nombre del responsable. La Comisión tiene la intención de abordar este tipo de transferencias en una decisión posterior.

(9) Resulta oportuno establecer los detalles mínimos que deberán especificar las partes en el contrato sobre la transferencia. Los Estados miembros deben conservar la capacidad de adaptar la información exigida a las partes. El funcionamiento de la presente Decisión será revisado a la luz de la experiencia adquirida.

(10) La Comisión Europea considerará asimismo en el futuro si las cláusulas contractuales tipo remitidas por las organizaciones empresariales u otras partes interesadas ofrecen garantías adecuadas de conformidad con la Directiva 95/46/CE.

(11) Así como las partes deben tener la libertad de convenir las normas sustantivas sobre protección de datos que debe cumplir el importador de los datos, existen determinados principios sobre protección de datos que deben aplicarse en todo caso.

(12) Los datos deben tratarse y usados o comunicados posteriormente sólo con objetivos precisos, sin que deban conservarse más tiempo del necesario.

(13) De conformidad con el artículo 1 2 de la Directiva 95/46/CE, el interesado debe tener el derecho de acceder a todos los datos que le conciernan y, en lo que proceda, a la rectificación, destrucción o bloqueo de determinados datos.

(14) Las posteriores transferencias de datos personales a otros responsables del tratamiento establecidos en un tercer país deben permitirse sólo bajo determinadas condiciones, a fin, en particular, de garantizar que se facilite a los interesados información correcta y que tengan éstos la posibilidad de formular objeciones o, en determinados casos, de denegar su consentimiento.

(15) Las autoridades de control, además de evaluar si las transferencias a terceros países cumplen la legislación nacional, deben desempeñar un papel clave en este mecanismo contractual, garantizando la adecuada protección de los datos personales tras la transferencia. Bajo circunstancias específicas, las autoridades de control de los Estados miembros deben conservar la facultad de prohibir o suspender una transferencia o una serie de transferencias de datos basada en las cláusulas contractuales tipo en aquellos casos excepcionales en los que se haya establecido que una transferencia sobre una base contractual pueda tener un importante efecto negativo sobre las garantías que proporcionan una protección adecuada al interesado.

(16) Las cláusulas contractuales tipo deben ser exigibles no solamente por las organizaciones que sean parte del contrato, sino también por los interesados, en particular cuando éstos sufran un daño como consecuencia del incumplimiento del contrato.

(17) La legislación aplicable al contrato debe ser la que esté en vigor en el Estado miembro en el que se halle establecido el exportador de datos y que permita a un tercer beneficiario exigir el cumplimiento de un contrato. Debe permitirse a los interesados ser representados por asociaciones u otras entidades si así lo desean y si lo autoriza la legislación nacional.

(18) Con objeto de reducir las dificultades prácticas que pudieran experimentar los interesados al intentar exigir el respeto de sus derechos a tenor de estas cláusulas contractuales tipo, el exportador de datos y el importador de datos se considerarán responsables solidarios de los daños y perjuicios resultantes de un incumplimiento de las estipulaciones sujetas a la cláusula de tercer beneficiario.

(19) El interesado tiene derecho a emprender acciones y percibir una indemnización del exportador de datos, del importador de datos o de ambos por daños y perjuicios resultantes de cualquier acción incompatible con las obligaciones estipuladas en las cláusulas contractuales tipo. Ambas partes podrán ser eximidas de esta responsabilidad si demuestran que ninguna de ellas es responsable.

(20) La responsabilidad solidaria no se amplía a las estipulaciones que no estén cubiertas por la cláusula de tercer beneficiario y no obliga a una parte a pagar los daños resultantes del tratamiento ilícito por parte de otra parte. Aunque esta indemnización entre las partes no es un requisito para la adecuación de la protección de los interesados y, por lo tanto, puede suprimirse, figura en las cláusulas contractuales a efectos de clarificación y para evitar a las partes la necesidad de negociar individual mente cláusulas de indemnización.

(21) En caso de conflicto entre las partes y el interesado que no se resuelva de manera amistosa, y si el interesado invoca la cláusula de tercer beneficiario, las partes aceptan ofrecer al interesado la elección entre mediación, arbitraje o procedimiento judicial. La amplitud de elección real del interesado dependerá de la disponibilidad de sistemas fiables y reconocidos de mediación y arbitraje. La mediación por parte de las autoridades de control de los Estados miembros debe constituir una opción posible, en caso de éstas presten tal servicio.

(22) El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE, ha emitido un dictamen sobre el nivel de protección que ofrecen las cláusulas contractuales tipo incluidas en el anexo, dictamen que se ha tenido en cuenta para la preparación de la presente Decisión (1).

(23) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el artículo 31 de la Directiva 95/46/CE.

(1) Dictamen n° 1/2001 adoptado por el Grupo de trabajo el 26 de enero de 2001 (DG MARKT 5102/00 WP 38); se puede consultar en el sitio web Europa de la Comisión Europea.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Se considera que las cláusulas contractuales tipo incluidas en el anexo ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige el apartado 2 del artículo 26 de la Directiva 95/46/CE.

Artículo 2

La presente Decisión aborda únicamente la adecuación de la protección otorgada por las cláusulas contractuales tipo para la transferencia de datos personales, establecidas en el anexo. No afecta a la aplicación de otras disposiciones nacionales por las que se aplique la Directiva 95/46/CE, relacionadas con el tratamiento de datos personales en los Estados miembros.

La presente Decisión no se aplica a la transferencia de datos personales por responsables del tratamiento establecidos en la Comunidad a destinatarios establecidos fuera del territorio comunitario que actúen solamente como encargados del tratamiento.

Artículo 3

A efectos de la presente Decisión:

a) serán aplicables las definiciones contenidas en la Directiva 95/46/CE;

b) se entenderá por «categorías especiales de datos» los datos contemplados en el artículo 8 de dicha Directiva;

c) se entenderá por «autoridad de control» la autoridad contemplada en el artículo 28 de dicha Directiva;

d) se entenderá por «exportador de datos» el responsable del tratamiento que transfiera los datos personales;

e) se entenderá por «importador de datos» el responsable del tratamiento que convenga en recibir del exportador de

datos personales para su posterior tratamiento de conformidad con los términos de la presente Decisión.

Artículo 4

1. Las autoridades competentes de los Estados miembros, sin perjuicio de su facultad para iniciar acciones destinadas a garantizar el cumplimiento de las disposiciones Derecho nacional adoptadas con arreglo a los capítulos II, III, y VI de la Directiva 95/46/CE, podrán ejercer sus facultades para prohibir o suspender los flujos de datos hacia terceros países con objeto de proteger a las personas físicas relación con el tratamiento de sus datos personales en los siguientes casos:

a) si se determina que la legislación a la que está sujeto el importador de datos le impone desviaciones de las normas correspondientes sobre protección de datos que vayan más allá de las restricciones necesarias en una sociedad democrática, como establece el artículo 13 de la Directiva 95/46/CE, cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías proporcionadas por las cláusulas contractuales tipo; o

b) si una autoridad competente decide que el importador de datos no ha respetado las cláusulas contractuales; o

c) si existe la probabilidad sustancial de que las cláusulas contractuales tipo contenidas en el anexo no se estén respetando, o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados.

2. La prohibición o suspensión con arreglo al apartado 1 se levantará tan pronto como desaparezcan las razones para dicha prohibición o suspensión.

3. Cuando los Estados miembros adopten medidas de conformidad con los apartados 1 y 2, informarán inmediatamente de ello a la Comisión, que remitirá la información a los demás Estados miembros.

Artículo 5

La Comisión evaluará el funcionamiento de la presente Decisión basándose en la información disponible tres años después de su notificación a los Estados miembros. Informará de los resultados al Comité creado en virtud del artículo 31 de la Directiva 95/46/CE. Incluirá cualquier prueba que pudiera afectar a la evaluación relativa a la adecuación de las cláusulas contractuales tipo y cualquier prueba de que la presente Decisión se esté aplicando de manera discriminatoria.

Artículo 6

La presente Decisión será aplicable a partir del 3 de septiembre de 2001.

Artículo 7

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 15 de junio de 2001.

Por la Comisión

Frederik BOLKESTEIN

Miembro de la Comisión

ANEXO

CLÁUSULAS CONTRACTUALES TIPO

a efectos del apartado 2 del artículo 26 de la Directiva 95/46/CE, con vistas a la transferencia de datos personales a terceros países que no garanticen un nivel adecuado de protección

Nombre de la entidad exportadora de los datos:

Dirección: ..

Tel: .. Fax: Correo electrónico:

Otros datos necesarios para identificar a la entidad: ..

.

(en adelante, el exportador de datos»)

Nombre de la entidad importadora de los datos:

Dirección: ..

Tel: .. Fax: Correo electrónico:

Otros datos necesarios para identificar a la entidad: ..

.

(en adelante, «el importador de datos»)

ACUERDAN las siguientes cláusulas contractuales (en adelante, las cláusulas) con objeto de ofrecer garantías suficientes respecto de la protección de la vida privada y de los derechos y libertades fundamentales de las personas para la transferencia por el exportador de datos al importador de datos de los datos personales especificados en el apéndice 1.

Cláusula 1

Definiciones

A los efectos de las presentes cláusulas:

a) datos personales», «categorías especiales de datos', «tratamiento», «responsable del tratamiento, «encargado del tratamiento», «interesado» y «autoridad de control» tendrán el mismo significado que en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos (en adelante, <'la Directiva»);

b) por ('exportador de datos» se entenderá el responsable del tratamiento que transfiera los datos personales;

c) por «importador de datos» se entenderá el responsable del tratamiento que acepte recibir del exportador datos personales para su posterior tratamiento de conformidad con los términos de las presentes cláusulas y que no esté sujeto al sistema de un tercer país por el que se garantice su protección adecuada.

Cláusula 2

Detalles de la transferencia

Los detalles de la transferencia y. en particular, las categorías de datos personales y la finalidad para la que éstos se transfieren, quedan especificados en el apéndice 1, que forma parte integrante de las presentes cláusulas.

Cláusula 3

Cláusula de tercero beneficiario

Los interesados podrán exigir la ejecución de la presente cláusula y de las letras h), c) y d) de la cláusula 4, las letras a), b), c) ye) de la cláusula 5, los apartados 1 y 2 de la cláusula 6 y las cláusulas 7, 9 y 11 como terceros beneficiarios. Las partes no se oponen a que los interesados estén representados por una asociación u otras entidades si así lo desean y lo permite el Derecho nacional.

Cláusula 4

Obligaciones del exportador de datos

El exportador de datos acuerda y garantiza lo siguiente:

a) el tratamiento, incluida la propia transferencia, de los datos personales por su parte ha sido efectuado y, hasta el momento de la transferencia, seguirá efectuándose con arreglo a todas las normas pertinentes del Estado miembro de establecimiento del exportador de datos (y, en caso necesario, se ha notificado a las autoridades pertinentes de dicho Estado) y no infringe las disposiciones pertinentes del mismo;

b) si la transferencia incluye categorías especiales de datos, se ha informado al interesado, o será informado antes de la transferencia, de que sus datos podrían ser transferidos a un tercer país que no proporcione una protección adecuada;

c) a petición de los interesados, les facilitará una copia de las presentes cláusulas como se ha acordado; y

d) responderá en un período de tiempo razonable y en la medida en que sea razonablemente posible, a las consultas de la autoridad de control sobre el tratamiento de los datos personales pertinentes por parte del importador de datos y a cualquier consulta del interesado relativa al tratamiento de sus propios datos personales por parte del importador de datos.

Cláusula 5

Obligaciones del importador de datos

El importador de datos acuerda y garantiza lo siguiente:

a) no llene motivos para creer que la legislación que le es de aplicación le impide cumplir sus obligaciones a tenor del contrato, y que en caso de modificación de la legislación que pueda tener probablemente un importante efecto negativo sobre las garantías proporcionadas por las cláusulas, notificará dicho cambio al exportador de datos y a la autoridad de control donde esté establecido el exportador de datos, en cuyo caso estará éste en su derecho de suspender la transferencia de datos o de rescindir el contrato;

h) tratará los datos personales de conformidad con los principios obligatorios para la protección de datos, establecidos en el apéndice 2, o bien, con el acuerdo explícito de las partes indicándolo con una marca a continuación, y con sujeción a los principios obligatorios para la protección de datos, establecidos en el apéndice 3, tratará en todos los demás casos los datos personales de conformidad con:

— las disposiciones pertinentes de Derecho nacional (anejas a las presente cláusulas) cuyo objeto sea la protección de los derechos y libertades fundamentales de las personas físicas y, en particular, el derecho a la vida privada en relación con el tratamientos de datos personales aplicables a un responsable del tratamiento en el país de establecimiento del exportador de datos, o bien, las normas correspondientes de toda Decisión de la Comisión de conformidad con el apartado 6 del artículo 25 de la Directiva 95/46/CE, donde se haga constar que un tercer país garantiza un nivel de protección adecuado en determinados sectores de actividad únicamente, si el importador de datos está establecido en dicho tercer país y no está afectado por dichas normas, en la medida en que éstas, por su naturaleza, sean aplicables en el sector de la transferencia;

c) tratará adecuadamente en los períodos de tiempo prescritos todas las consultas razonables procedentes del exportador de datos o de los interesados relacionadas con su tratamiento de los datos personales sujetos a transferencia y cooperará con la autoridad de control competente en el transcurso de toda su investigación y se someterá al dictamen de la misma en lo que respecta al tratamiento de los datos transferidos;

d) a petición del exportador de datos, someterá sus instalaciones de tratamiento de datos con fines de auditoria, que será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes y que posean las cualificaciones profesionales exigidas, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;

e) pondrá a disposición de los interesados, previa petición de éstos, una copia de las presentes cláusulas e indicará la oficina encargada de gestionar las quejas.

Cláusula 6

Responsabilidad

1. Las partes acuerdan que los interesados que hayan sufrido dados como resultado del incumplimiento de las disposiciones mencionadas en la cláusula 3 tendrán derecho a percibir una compensación de las partes por el daño sufrido. Las partes acuerdan que solamente podrán considerarse exentas de esta responsabilidad si demuestran que ninguna de ellas es responsable del incumplimiento de dichas disposiciones.

2. El exportador de datos y el importador de datos acuerdan que serán responsables solidarios por los daños a los interesados resultantes de todo incumplimiento contemplado en el apartado 1. En caso de tal incumplimiento, el interesado podrá interponer una demanda judicial contra el exportador de datos, contra el importador de datos o contra ambos.

3. Las partes acuerdan que si se demuestra que una de ellas e. responsable de un incumplimiento contemplado en el aparado 1 por la otra parle, esta última indemnizará a la primera parte por cualquier coste, carga, perjuicio gasto o pérdida en que haya incurrido (*)

Cláusula

Mediación y jurisdicción

1. las partes acuerdan que, en caso de conflicto entre el interesado y cualquiera de las partes, que no se resuelva de manera amistosa, y si el interesado invoca la cláusula 3 de tercer beneficiario, aceptan la decisión del interesado de:

a) someter el conflicto a mediación por parte de una persona independiente, o, si procede, por parte de la autoridad de control:

h) someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador de datos.

2. 1 as partes acuerdan que, por acuerdo entre el interesado y la parte correspondiente, el conflicto específico podrá someterse a un organismo de arbitraje, si dicha parte está establecida en un país que haya ratificado la (‘onvención de Nueva York sobre ejecución de laudos arbitrales.

3. las partes acuerdan que los apartados 1 y 2 se aplicarán sin perjuicio de los derechos sustantivos o procedimentales del interesado a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

Cláusula 5

Cooperación con las autoridades de control

Las partes acuerdan depositar una copia del presente contrato ante la autoridad de control si así lo requiere o si el depósito es exigido con arreglo al Derecho nacional.

Cláusula 9

Resolución de las cláusulas

Las partes acuerdan que la resolución de las presentes cláusulas en cualquier momento. en cualquier circunstancia y por cualquier motivo no las eximirá del cumplimiento de las obligaciones y condiciones estipuladas en estas cláusulas en lo que respecta al tratamiento de los datos transferidos.

Cláusula 10

Legislación aplicable

Las cláusulas se regirán por la legislación del Estado miembro de establecimiento del exportador de datos, a saber:

Cláusula 11

Variación del contrato

Las parles se comprometen a no variar o modificar los términos de las presentes cláusulas.

En nombre del exportador de datos:

Nombre (completo) .

Cargo

Dirección .

(*) FI apartado 3 es optativo

Otros datos necesarios con vistas a la obligatoriedad del contrato (en caso de existir): .

.

(Firma)

(sello de la entidad)

En nombre del importador de datos:

Nombre (completo) .

Cargo

Dirección .

(*) FI apartado 3 es optativo

Otros datos necesarios con vistas a la obligatoriedad del contrato (en caso de existir): .

.

(Firma)

(sello de la entidad)

Apéndice 1

a las cláusulas contractuales tipo

El presente apéndice forma parte integrante de las cláusulas y deberá ser cumplimentado y suscrito por las partes.

(Los Estados miembros podrán completar o especificar de acuerdo con sus procedimientos nacionales, cualquier información adicional necesaria que deba incluirse en el presente apéndice.)

Exportador de datos

El exportador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

Importador de datos

El importador de datos es (especifique brevemente sus actividades correspondientes a la transferencia):

Interesados

Los datos personales transferidos se refieren a las siguientes categorías de interesados (especifíquense):

Finalidad de la transferencia

La transferencia es necesaria para los siguientes objetivos (especifíquense):

Categorías de datos

Los datos personales transferidos entran dentro de las siguientes categorías de datos (especifíquense):

Información delicada (si es pertinente)

Los datos personales transferidos entran dentro de las siguientes categorías de datos delicados (especifíquense):

Destinatarios

Los datos personales transferidos podrán ser facilitados únicamente a los siguientes destinatarios o categorías (especifíquense):

Período máximo de almacenamiento

Lo datos personales transferidos podrán almacenarse durante un período máximo de (indíquese) ..(meses/años)

Exportador de datos Importador de datos

Nombre y apellidos Nombre y apellidos: .

(Firma autorizada) . (Firma autorizada)

Apéndice 2

a las cláusulas contractuales tipo

Principios obligatorios para la protección de datos contemplados en el párrafo primero de la letra b) de la cláusula 5

Los presentes principios para la protección de datos se leerán e interpretarán a la luz de lo dispuesto (principios y excepciones pertinentes) en la Directiva 95/46/CE.

Se aplicarán con sujeción a las normas obligatorias de la legislación nacional aplicable a los importadores de datos, que no excedan de lo necesario en una sociedad democrática sobre la base de uno de los intereses enumerados en el apartado 1 del artículo 13 de la Directiva 95/46/CE, es decir, cuando constituyan una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas, un interés económico y financiero importante del Estado, o la protección del interesado o de los derechos y libertades de otras personas:

1. Limitación de la finalidad: Los datos se tratarán y se utilizarán o transferirán ulteriormente sólo para las finalidades concretas del apéndice 1 de las cláusulas. Los datos no se conservarán durante más tiempo del necesario para dichas finalidades.

2. Calidad y proporcionalidad de los datos: Los datos serán precisos y, en caso necesario, se mantendrán actualizados. Los datos serán adecuados, pertinentes y no excesivos en relación con la finalidad de su transferencia y tratamiento posterior.

3. Transparencia: Se deberá facilitar a los interesados información sobre la finalidad del tratamiento y la identidad del responsable del tratamiento de los datos en el tercer país, así como cualquier otra información en la medida en que sea necesaria para garantizar el tratamiento leal, a menos que dicha información ya la haya proporcionado el exportador de

datos.

4. Seguridad y confidencialidad: El responsable del tratamiento de los datos deberá adoptar medidas técnicas y de organización apropiadas para la seguridad frente a los riesgos que presente el tratamiento, por ejemplo, el acceso no autorizado. Las personas que actúen bajo la autoridad del responsable del tratamiento, incluyendo el encargado del tratamiento, no tratarán los datos a menos que reciban instrucciones del responsable.

5. Derechos de acceso, rectificación, supresión y bloqueo de los datos: Según prevé el artículo 12 de la Directiva 95/46/CE, el interesado tendrá el derecho de acceso a todos los datos que le conciernan y que estén siendo tratados, así como el derecho a rectificar, suprimir o bloquear dichos datos cuando su tratamiento no cumpla los principios establecidos en el presente apéndice, en particular porque sean incompletos o inexactos. También podrá oponerse al tratamiento de los datos que le conciernan por motivos legítimos imperiosos relacionados con su situación particular.

6. Restricciones a la transferencia ulterior: La posterior transferencia de datos personales del importador de datos a otro responsable del tratamiento establecido en un tercer país que no proporcione protección adecuada o no amparado por una Decisión de la Comisión adoptada con arreglo al apartado 6 del artículo 25 de la Directiva 95/46/CE (transferencia ulterior) solamente podrá tener lugar si:

a) los interesados, en el caso de categorías especiales de datos, han dado su consentimiento de forma inequívoca para la transferencia ulterior, o, en otros casos, han tenido la oportunidad de ejercer su derecho de formular objeciones.

La información mínima que se debe proporcionar a los interesados incluirá, en un idioma comprensible para ellos:

la finalidad de la transferencia ulterior, la identificación del exportador de datos establecido en la Comunidad, las categorías de destinatarios posteriores de los datos y los países de destino, así como una explicación de que, tras la transferencia ulterior, los datos podrán ser tratados por un responsable del tratamiento establecido en un país donde no haya un nivel adecuado de protección de la vida privada de las personas; o

b) el exportador de datos y el importador de datos acuerdan la adhesión a las cláusulas de otro responsable del tratamiento, que pase con ello a ser parte de las presentes cláusulas y asuma las mismas obligaciones que el importador de datos.

7. Categorías especiales de datos: Cuando se traten datos que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas o pertenencia a organizaciones sindicales, datos relativos a la salud o a la vida sexual, y datos relacionados con infracciones, condenas penales o medidas de seguridad, deberán disponerse garantías adicionales, a efectos de la Directiva 95/46/CE, en particular medidas apropiadas de seguridad como la codificación de los datos para su transmisión o el mantenimiento de un registro de acceso a datos delicados.

8. Marketing directo: Cuando el tratamiento de los datos se realice con fines de marketing directo, deberán, existir procedimientos efectivos que permitan al interesado ejercer en cualquier momento el derecho de «exclusión» de su información personal para estos fines.

9. Decisión individual automatizada: Los interesados tendrán derecho a no ser objeto de una decisión basada exclusivamente en un tratamiento automatizado de los datos, a menos que se tomen otras medidas que garanticen el interés legítimo de la persona, tal como establece el apartado 2 del artículo 15 de la Directiva 95/46/CE. Cuando la finalidad de la transferencia sea tomar una decisión automatizada contemplada en el artículo 15 de la Directiva 95/46/CE, que tenga efectos jurídicos sobre el interesado o que le afecte de manera significativa y que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. el interesado tendrá el derecho de conocer los motivos de dicha decisión.

Apéndice 3

a las cláusulas contractuales tipo

Principios obligatorios para la protección de datos contemplados en el párrafo segundo de la letra b) de la cláusula 5

1. Limitación de la finalidad: Los datos se tratarán y se utilizarán o transferirán ulteriormente sólo para las finalidades concretas del apéndice 1 de las cláusulas. Los datos no se conservarán durante más tiempo del necesario para dichas finalidades.

2. Derechos de acceso, rectificación, supresión y bloqueo de los datos: Según prevé el artículo 12 de la Directiva 95/46/CE, el interesado tendrá el derecho de acceso a todos los datos que le conciernan y que estén siendo tratados, así como el derecho a rectificar, suprimir o bloquear dichos datos cuando su tratamiento no cumpla los principios establecidos en el presente apéndice, en particular porque sean incompletos o inexactos. También podrá oponerse al tratamiento de los datos que le conciernan por motivos legítimos imperiosos relacionados con su situación particular.

3. Restricciones a la transferencia ulterior: La posterior transferencia de datos personales del importador de datos a otro responsable del tratamiento establecido en un tercer país que no proporcione protección adecuada o no amparado por una Decisión de la Comisión adoptada con arreglo al apartado 6 del artículo 25 de la Directiva 95/46/CE (transferencia ulterior) solamente podrá tener lugar si:

a) los interesados, en el caso de categorías especiales de datos, han dado su consentimiento de forma inequívoca para la transferencia ulterior, o, en otros casos, han tenido la oportunidad de ejercer su derecho de formular objeciones.

La información mínima que se debe proporcionar a los interesados incluirá, en un idioma comprensible para ellos:

la finalidad de la transferencia ulterior, la identificación del exportador de datos establecido en la Comunidad, las categorías de destinatarios posteriores de los datos y los países de destino, así como una explicación de que, tras la transferencia ulterior, los datos podrán ser tratados por un responsable del tratamiento establecido en un país donde no haya un nivel adecuado de protección de la vida privada de las personas; o

b) el exportador de datos y el importador de datos acuerdan la adhesión a las cláusulas de otro responsable del tratamiento, que pase con ello a ser parte de las presentes cláusulas y asuma las mismas obligaciones que el importador de datos.

MEMORIA DE 2001 - ANEXO VII - DECISIÓN DE LA COMISIÓN DE 20 DE DICIEMBRE DE 2001
DECISIÓN DE LA COMISIÓN

de 20 de diciembre de 2001

con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act

[notificada con el número C(2001) 4539]

(2002/2/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (1), y, en particular, el apartado 6 de su artículo 25,

Considerando lo siguiente:

(1) De conformidad con la Directiva 95/46/CE, los Estados miembros sólo permitirán la transferencia de datos personales a un país tercero si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.

(2) Para transferir datos personales desde los Estados miembros bastará con que la Comisión dictamine, en ejercicio de sus competencias, que un país tercero proporciona un nivel de protección adecuado.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en una transferencia o categoría de transferencias de datos, con respecto a unas condiciones determinadas. El Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, que se creó en virtud del artículo 29 de la Directiva 95/46/CE, ha dado a conocer una serie de orientaciones sobre la evaluación (2).

(4) Ante los diferentes enfoques sobre la protección de datos adoptados en los terceros países, tanto la evaluación de la adecuación como la ejecución de las decisiones en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE deben hacerse sin que originen, en igualdad de condiciones, una discriminación arbitraria o injustificada contra terceros países o entre ellos, ni constituyan una restricción comercial encubierta contraria a los compromisos internacionales de la Comunidad.

(5) La Ley canadiense Personal Information and Electronic Documents A (en adelante «la Ley canadiense») de 13 de abril de 2000 (3) se aplica a las entidades privadas que recojan, utilicen o divulguen datos personales en sus actividades comerciales. Entrará en vigor en tres etapas:

A partir del 1 de enero de 2001, la Ley canadiense se aplicará a los datos personales, excluidos los de carácter sanitario, que las entidades que operen como «empresa federal» recojan, utilicen o divulguen en el transcurso de sus actividades económicas. Dichas empresas operan en sectores como el transporte aéreo, la banca, la radiotelevisión, el transporte interprovincial y las telecomunicaciones. También se aplicará a todos las entidades que comercian con datos personales fuera de su provincia o fuera del Canadá y a los datos laborales sobre los asalariados de las empresas federales.

(1) DO L 281 de 23.11.1995, p. 31.

(2) WP12: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998. Puede consultarse en http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_9 8 .htm

(3) Pueden consultarse las versiones electrónicas (papel y web) de la Ley en http://www.parl.gc.ca/ 36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html y http://www.parl.gc.ca/ 36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html. La versión impresa puede obtenerse en Public Works and Government Services Canada - Publishing, Ottawa, Canada K 0S9.

(4) A partir del 1 de enero de 2002, se aplicará a los datos personales sanitarios de las entidades y actividades ya cubiertos en la primera etapa.

(5)A partir del 1 de enero de 2004, se ampliará a cualquier organismo que recoja, utilice o divulgue datos personales en el transcurso de una actividad comercial dentro de una provincia, independiente mente de que dicho organismo esté o no regulado a escala federal. No están sujetas a la Ley canadiense las entidades a quienes se aplique la Federal

Privacy Act o se regulen por el sector público de ámbito provincial. Del mismo modo, las actividades filantrópicas o sin fines lucrativos tampoco están sujetas a la Ley canadiense a no ser que tengan carácter comercial. No se aplica, por último, a los datos laborales utilizados con fines no comerciales siempre que no se refieran a los asalariados del sector privado sujeto a regulación federal. En tales casos, la autoridad canadiense de protección de la vida privada podrá proporcionar información adicional.

(6) A fin de que se respete el derecho de las provincias a legislar en su ámbito competencial, la Ley federal dispone que cuando éstas adopten una legislación básicamente similar, las entidades y ámbitos de organización y actividad que dicha legislación cubra estarán exentos de la Ley federal. El apartado 2 del artículo 26 de la Personal Information Protection and Electronic Documents A faculta al Gobierno federal para, «si tiene el convencimiento de que una Ley provincial esencialmente similar a la presente parte se aplica a una organización -o categoría de entidades——o a una actividad —o categoría de actividades—, excluir la organización, actividad o categoría de la aplicación de la presente parte en lo relativo a la recogida, utilización o comunicación de datos personales realizadas en el interior de la provincia». El Governor in Council (Gobierno federal canadiense) concede por decreto (Order-in-Council) las excepciones a la legislación que sea básicamente similar.

(7) Siempre que una provincia adopte una legislación básicamente similar, las entidades y ámbitos de organización y actividad que cubra estarán exentos de aplicar la Ley federal en transacciones en el interior de la provincia. La Ley federal seguirá aplicándose a toda recogida, utilización o divulgación de datos interprovincial e internacional, así como en todos aquellos casos en que las provincias no hayan creado una legislación que sea básicamente similar ni total ni parcialmente.

(8) Canadá se adhirió formalmente el 29 de junio de 1984 a las Orientaciones de la OCDE sobre la protección de la vida privada y los flujos de datos transfronterizos de 1980. Canadá fue uno de los países que apoyó las Orientaciones de Naciones Unidas sobre los sistemas de información datos de carácter personal aprobadas por la Asamblea General el 14 de diciembre de 1990.

(9) La Ley canadiense comprende todos los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada, pese a que también se dispongan excepciones y limitaciones para proteger importantes intereses públicos y dar reconocimiento a cierta información de dominio público. La aplicación de estas normas se garantiza mediante recursos jurisdiccionales y el control independiente que ejercen autoridades como el Comisario federal de protección de la vida privada, dotado de facultades de investigación e intervención. Además, las disposiciones de Derecho canadiense relativas a la responsabilidad civil se aplican en caso de tratamiento ilícito que haya causado daños.

(10) Aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar en la presente Decisión las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.

(11) El Grupo de Trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, previsto en el artículo 29 de la Directiva 95/46/CE ha evacuado un dictamen sobre el nivel de protección que proporciona la Ley canadiense que se ha tenido en cuenta al preparar la presente Decisión (1).

(1) Dictamen 2/2001 sobre el nivel adecuado de protección de la ley canadiense Personal Information and Electronic Documents Act WP 39 de 26 de enero de 2001. Puede consultarse en http://europa.eu.int/comm/intemal_market/en/dataprot/wpdocs/index.htm

(12) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité previsto en el artículo 31 de la Directiva 95/46/CE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, Canadá garantiza un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a los receptores sujetos a la Personal Information Protection and Electronic Documents Act (en adelante «la Ley canadiense»).

Artículo 2

La presente Decisión se refiere únicamente a la adecuación de la protección que proporciona en Canadá la Ley canadiense, con arreglo a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE, y no afecta a otras condiciones o restricciones que se impusieren en aplicación de otros preceptos de la Directiva referentes al tratamiento de los datos personales en los Estados miembros.

Artículo 3

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con preceptos diferentes a los contemplados en el artículo 25 de la Directiva 95/46/CE, las autoridades de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia

un receptor canadiense cuyas actividades entren en el ámbito de la Ley canadiense, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos en que:

a) la autoridad competente canadiense compruebe que el receptor ha vulnerado las normas de protección aplicables,

b) existan grandes probabilidades de que se estén vulnerando las normas de protección; existan razones para creer que la autoridad competente canadiense no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad responsable del tratamiento en Canadá y proporcionarle la oportunidad de alegar.

La suspensión cesará en cuanto esté garantizado el cumplimiento de las normas de protección y las autoridades correspondientes de la Comunidad hayan sido notificadas de ello.

2. Los Estados miembros informarán a la Comisión con la mayor brevedad de la adopción de medidas con arreglo al apartado 1.

3. Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de las normas de protección en Canadá no garantice dicho cumplimiento.

4. Si la información recogida con arreglo a los apartados 1 a 3 demuestra que los organismos responsables del cumplimiento de las normas de protección en Canadá no están ejerciendo su función, la Comisión lo notificará a la autoridad competente canadiense y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que contempla el apartado 2 del artículo 31 de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

Artículo 4

1. La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia de su funcionamiento o los cambios que se introduzcan en la legislación canadiense, señaladamente en las medidas por las que se reconoce que una provincia canadiense tiene una legislación substancialmente similar. La Comisión analizará, basándose en la información disponible, la aplicación de la presente Decisión tres años después de su notificación a los Estados miembros. Informará al Comité contemplado en el artículo 31 de la Directiva 95/46/CE de cualquier hecho que venga al caso, en particular de cualquier prueba que pueda afectar a la resolución contenida en el artículo 1 de la presente Decisión de que la protección en Canadá es adecuada a efectos del artículo 25 de la Directiva 95/46/CE, así como de cualquier prueba de que la presente Decisión se está aplicando de forma discriminatoria.

2. La Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el apartado 2 del artículo 31 de la Directiva 95/46/CE.

Artículo 5

Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión, a más tardar en un plazo de noventa días a partir de la fecha de su notificación a los Estados miembros.

Artículo 6

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 20 de diciembre de 2001.

Por la Comisión

Frederik BOLKESTEIN

Miembro de la Comisión

MEMORIA DE 2001 - ANEXO VIII - DOCUMENTOS DE TRABAJO PROTECCIÓN DE DATOS DEL ARTÍCULO 29

Dictamen 4/2001 acerca del proyecto de convenio del Consejo de Europa sobre el ciberdelito

WP41 - DICTÁMEN PROYECTO CONVENIO CIBERCRIMEN CoE
ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

5001/01/ES/Final

WP41

Dictamen 4/2001

acerca del proyecto de convenio del Consejo de Europa sobre el ciberdelito

Aprobado el 22 de marzo de 2001

El Grupo de trabajo se creó en virtud del articulo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo indepen - diente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el articulo 30 de la Directiva 95/46/CE yen el articulo 14 de la Directiva 97/66/CE. La secretaria encargada es la siguiente:

Comisión Europea, DG Mercado Interior, Dirección de libre circulación de la información y protección de datos.

Rue de la Loi 200, B-1049 Bruselas/Wetstraat 200, B-1049 Brussel - Belgium - Despacho: Ci 00-2/1 33

Dirección Internet: http://europa.eu.int/comm/dgl 5/en/media/dataprot/wpdocs/index.htm

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado en virtud del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995',

Vistos el artículo 29 y los apartados 1, letra a), y 3 del artículo 30 de dicha Directiva, Visto su Reglamento interno y, en particular, sus artículos 12 y 14,

ha adoptado el presente DICTAMEN:

Introducción

El ciberdelito forma parte de la vertiente sórdida de la sociedad de la información. Las nuevas tecnologías tienen ventajas enormes para las sociedades, pero también dan pie a la comisión de nuevas infracciones penales, o viejas por nuevos procedimientos. Los Estados y diversos organismos son conscientes del problema, del cual se ocupan ya, por ejemplo, la Unión Europea el G8 la OCDE, las Naciones Unidas y el Consejo de Europa. El objetivo de estas iniciativas es crear una sociedad de la información en la que los ciudadanos disfruten de libertad y seguridad.

El Consejo de Europa tiene una larga experiencia y tradición de cooperación internacional en materia penal y de derechos humanos. Trabaja desde 1997 en un proyecto de convenio sobre el ciberdelito. La Comisión de expertos en infracciones penales en el ciberespacio (PC-CY) terminó su cometido en diciembre de 2000. Por su parte, la Asamblea Parlamentaria del Consejo de Europa tendrá que evacuar dictamen (en primavera de 2001 según las previsiones) antes de que el texto se presente a aprobación del Comité de Ministros del Consejo de Europa. Se encomendará a un equipo de redacción que modifique el texto con arreglo al dictamen de la Asamblea.

Podrán firmar este proyecto de convenio países que no son miembros del Consejo de Europa. Los Estados Unidos, Canadá, Japón y Suráfrica participan ya activamente en su redacción.

1 Diario Oficial L 281 de 23 11 1995, p. 31, disponible en inglés en la siguiente dirección:

http://europa.eu.int/commldg 1 5/en/media/dataprot/index.htm

2 Véase la Comunicación de la Comisión al Consejo y al Parlamento Europeo titulada: "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos", que se adoptó el 26 de enero de 2001

(http://europa.eu.int/ISPO/eif/IntemetPoliciesSite/Crime/crime 1 html).

Véase la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, que se adoptó el 7 de septiembre de 1999. WP 25 (http://europa. eu/conmilintemal_market/en/media/dataprot/wpdocs/index.htm).

Desde el mes de abril de 2000, se han puesto en conocimiento del público diferentes versiones del proyecto de convenio a través del sitio web del Consejo de Europa. El proyecto de Exposición de motivos se publicó por primera vez recientemente, en febrero de 2001. La redacción de ambos documentos sigue su curso. El presente dictamen aborda el texto del proyecto de convenio en la versión que se publicó el 22 de diciembre de 2000 (versión pública 25 pero no la Exposición de motivos.

El Grupo de trabajo señala el esfuerzo que se está haciendo en muchos campos para luchar contra el ciberdelito, y cuyos objetivos generales apoya por cuanto contribuyen a mejorar el nivel de seguridad de los ciudadanos y, en particular, del tratamiento de los datos personales. Desea, no obstante, enviar un claro mensaje de que las medidas que se propongan en el proyecto de convenio deben lograr un justo equilibrio entre la batalla contra el ciberdelito y los derechos fundamentales de la persona a la vida privada y a la protección de los datos personales. Estos derechos se consagran singularmente en el Convenio europeo para la protección de los derechos humanos del Consejo de Europa, el Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, la Recomendación n° R (87) 15 por la que se regula el uso de datos personales por parte de la policía, la Recomendación n° R (95) 4 sobre la protección de datos personales en el campo de los servicios de telecomunicaciones y, en particular, los servicios telefónicos, la Carta de derechos fundamentales de la UE, las directivas de protección de datos de la UE y el Pacto internacional de derechos civiles y políticos de 1966.

Estas son las razones por las que el Grupo de trabajo aporta las observaciones siguientes sobre el actual proyecto de convenio sobre el ciberdelito del Consejo de Europa.

El proyecto de convenio

Los contenidos del proyecto de convenio referidos a la armonización de las medidas procesales Capítulo II) y la asistencia judicial internacional Capítulo III) tienen como resultado que, en el curso de la cooperación penal internacional, se intercambian datos personales (datos de tráfico, contenido de las comunicaciones y demás categorías) que no están exclusivamente relacionados con el ciberdelito.

El Capítulo III trata de la cooperación internacional "a los efectos de las investigaciones o procesos sobre infracciones penales relacionadas con los sistemas y los datos informáticos o para la recogida de pruebas en formato electrónico sobre una infracción penal". La mayor parte de las obligaciones de asistencia mutua que se establecen en este capítulo pueden afectar a cualquier infracción penal sea o no de carácter informático. Entre ellas se incluyen la asistencia mutua en materia de extradición, comunicación espontánea de información, conservación de los datos informáticos y los datos de tráfico, divulgación de ambos tipos de datos y acceso a ello, acceso transfronterizo a los datos almacenados, recogida en tiempo real de los datos de tráfico e interceptación de las comunicaciones. En este Capítulo se contemplan las modalidades de solicitud de asistencia mutua por medios de comunicación urgente, como el fax y el correo electrónico, en cuyo caso sólo será necesaria la confirmación formal si así lo solicita la parte requerida.

Véase http://coe.fr
3 En el proyecto de convenio (sección 2 del Capítulo II) se exige también que las partes armonicen sus normas de enjuiciamiento para habilitar las medidas siguientes:

conservación rápida de los datos informáticos almacenados; conservación y divulgación rápida de los datos de tráfico; mandato de entregar los datos informáticos que obren en poder de una persona y de facilitar la información sobre los abonados en poder de un proveedor de servicios; búsqueda y utilización autorizada de datos informáticos almacenados; recogida en tiempo real de los datos de tráfico e interceptación de los datos de contenido.

En cuanto al Derecho penal material, el proyecto de convenio (sección 1 del Capítulo II) exige a las partes que den a ciertos actos la consideración de infracción penal con todas las consecuencias, señaladamente, el ejercicio de las facultades de investigación específicas de las investigaciones penales. Tal es el caso, por ejemplo, del acceso ilegal a los datos informáticos, la intercepción ilegal, el abuso de dispositivos como los programas o las contraseñas informáticas, la falsificación y el fraude informático, los delitos relacionados con la pornografia o las violaciones de los derechos de autor y afines. El Grupo de trabajo lamenta que no se haya contemplado la incriminación por infracción de las normas en materia de protección de datos.

Protección de los derechos humanos, la vida privada y los datos

El preámbulo del proyecto de convenio menciona el Convenio europeo para la protección de los derechos humanos y las libertades fundamentales de 1950 (CEDH) del Consejo de Europa, el Pacto internacional de derechos civiles y políticos de 1966 de las Naciones Unidas, [Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 del Consejo de Europa], y [Recomendación n° R (87) 15 por la que se regula el uso de datos personales por parte de la policía].

No se armonizan en el proyecto de convenio, sin embargo, las garantías y requisitos que habrán de aplicarse a las medidas que se tomen conforme a los textos citados. Aunque no se exige su existencia efectiva, el proyecto de convenio (artículo 15) menciona en el contexto del derecho procesal que la "creación, aplicación y ejecución de las competencias y procedimientos contemplados en esta sección (sección 2 del Capítulo II) estarán sujetas a las garantías y requisitos previstos en el Derecho interno de las Partes implicadas".

Los países pertenecientes al Consejo de Europa tienen la obligación de aplicar el CEDH (que garantiza el derecho a la vida privada y a la protección de los datos, los principios de secreto de correspondencia, juicio justo, legalidad de las

penas, libertad de expresión y claridad de los requisitos para limitar dichos principios en las disposiciones legales) y los demás instrumentos que hagan al caso. Deben tener en vigor, por tanto, garantías y requisitos, aunque su naturaleza y alcance no sea idéntico en todos los Estados miembros. Sin embargo, el proyecto de convenio se destina también a países no pertenecientes al Consejo de Europa, que no están sujetos a las mismas obligaciones que los miembros y a quienes el proyecto de convenio no obliga a introducir garantías y requisitos conformes con las disposiciones internacionales sobre derechos humanos.

4 Además, el tenor del artículo 15 del proyecto de convenio podría dar la impresión de que la protección de los derechos humanos sólo ha de tenerse en cuenta cuando sea "obligatorio", y que sólo ha de ser "adecuada". Por otra parte, la proporcionalidad de las competencias o procedimientos respecto de la naturaleza y circunstancias de la infracción no se considera una cuestión de principio, sino que se aplica sólo "en su caso". Si este extremo fuese objeto de una interpretación limitativa de las garantías y requisitos, se reduciría considerablemente, si es que no se socava por completo, la protección de los derechos fundamentales.

En el Capítulo III, dedicado a la cooperación internacional, se da una falta de armonización similar de las garantías y requisitos. Algunas de las obligaciones de ayudar a la parte requirente están sujetas a las garantías y requisitos establecidas en el Derecho nacional (recogida en tiempo real de los datos de tráfico e intercepción de los datos de contenido) . Las demás obligaciones no están sujetas a ninguna otra condición. Esto significa que un miembro del Consejo de Europa no puede negarse a cooperar, excepto en los casos en que se reconoce que la violación de su orden público es motivo de denegación Asimismo, el requisito de doble tipicidad (otra garantía muy importante) sólo puede alegarse en unos pocos casos Como consecuencia de ello, por lo general y con independencia de las concepciones de ámbito nacional o más amplio sobre las garantías y requisitos, la parte requerida habrá de proporcionar la información, material etc., solicitada por la otra parte. Este es un objetivo deseable desde el punto de vista de la acción policial y la lucha contra el delito. Sin embargo, no pasaría las pruebas de necesidad, procedencia y proporcionalidad que exigen los instrumentos en materia de derechos humanos incorporados en las constituciones y leyes nacionales.

En este contexto, el Grupo de trabajo señala también que en el proyecto de convenio se hace referencia a la "ley y otras medidas" que los signatarios están obligados a tomar en aplicación del Convenio. El Grupo de trabajo desearía hacer presente al Consejo de Europa, señaladamente a los órganos que se ocupan del proyecto y a los posibles signatarios, el hecho de que estos términos han de interpretarse a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos si las medidas que encuentran su justificación en ellos conllevan limitaciones legales de los derechos y libertades fundamentales.

Varios de los Estados miembros de la UE aplican la Directiva 95/46/CE también en el "tercer pilar", esto es, para el tratamiento de datos personales en materia penal. Por consiguiente, sus ordenamientos jurídicos permiten en principio que los datos personales se envíen a países no comunitarios, siempre que estos proporcionen a los particulares una protección adecuada de sus datos sometidos a tratamiento. Dichos países necesitan pues estar en condiciones de verificar que la protección que se ofrece en el tercer país es

Véase los artículos 33 y 34 del proyecto de convenio.

6 Véase el artículo 27 (4b) en caso de no aplicarse ningún tratado de asistencia judicial mutua, excepto este capítulo del proyecto de convenio. Véase el artículo 29 (5b), relativo a la conservación rápida de datos informáticos almacenados, y el artículo 30 (2b) relativo a la divulgación rápida de los datos de tráfico conservados.

Véase los apartados (3) y (4) del artículo 29 conservación rápida de datos informáticos almacenados y el artículo 30 (2b) relativo a la divulgación rápida de los datos de tráfico conservados.

Véase los artículos 14, 16, 17, 18, 19, 20 sobre la recogida en tiempo real de los datos de tráfico (es decir, sin mandamiento o fundamento similar), 21 sobre la interceptación de los datos de contenido, 23 y 26 del proyecto de convenio.

5 adecuada. Podría darse el caso de que no lo sea y fuese necesaria una transferencia de datos personales dentro de la lucha contra la delincuencia. La legislación nacional podría haber previsto este caso introduciendo excepciones en el principio de adecuación. En otros países podría surgir la misma necesidad de imponer condiciones como consecuencia de sus normas constitucionales y procesales. Por consiguiente, el proyecto de convenio debería, en su mínima expresión, contemplar la posibilidad de reconciliar ambos objetivos permitiendo que la parte requerida imponga garantías y requisitos específico para que tenga lugar la transferencia. De lo contrario, podrían entrar en conflicto la obligación de proporcionar asistencia y la de respetar los derechos fundamentales consagrados en los instrumentos europeos y la jurisprudencia correspondiente.

Abordan esta cuestión, aparentemente, el artículo 27bis junto con el apartado (6) del artículo 27, aunque no queda muy claro cómo. El artículo 27bis no menciona explícitamente la protección de los datos personales, sino la "confidencialidad y limitación del uso" de "información o material". Contempla únicamente la posibilidad ("may" en la versión inglesa: «puede») de que la parte requerida someta la entrega de información o material a confidencialidad o limitaciones de uso. Al mismo tiempo, tales posibilidades parecen muy restringidas: en la nota 48 se indica que si las normas procesales exigen la publicación, podría no garantizarse la confidencialidad. La nota 49 explica que el artículo 27bis se aplica sin perjuicio del artículo 27 sobre asistencia mutua en ausencia de acuerdos internacionales. El apartado (4) del artículo 27 permite denegar la asistencia mutua por las razones enumeradas en él, si la ejecución del requerimiento puede perjudicar el "orden público", soberanía, seguridad u otros intereses esenciales de la parte requerida. Antes de denegar o posponer la asistencia, la parte requerida tiene que sopesar si el requerimiento puede concederse parcialmente o con arreglo al apartado (6) del artículo 27. No queda claro, sin embargo, si las condiciones aplicables a la protección de

datos pueden basarse en este precepto, puesto que está relacionado con los motivos de denegación que se citan en el apartado (4) del artículo 27 y no comprenden necesariamente la protección de datos.

En opinión del Grupo de trabajo, estos preceptos y las limitaciones que conllevan no son suficientes para garantizar plenamente los derechos fundamentales de la persona a la vida privada y la protección de los datos personales. Los ciudadanos no estarán en condiciones de prever cuándo y cómo van a limitarse sus derechos fundamentales. El proyecto de convenio debería, pues, contener cuando menos preceptos en materia de protección de datos que esbocen la protección que debe proporcionarse a los sujetos de las medidas contempladas en el proyecto de convenio. Además, debería pedirse a los signatarios que suscriban el Convenio 1O8 del Consejo de Europa que está abierto a los países no pertenecientes al Consejo de Europa.

Especialmente, deben aclararse con arreglo a los comentarios que anteceden el artículo 27bis y su relación con los apartados (4) y (6) del artículo 27. Dado que la Directiva 95/46/CE suele aplicarse sin restricciones, es decir, incorpo - rando el tratamiento de los datos personales dentro del "tercer pilar", hay sólidos argumentos para llegar a la conclusión de que el concepto de "orden público" podía también abarcar aquellas Esta propuesta sigue el modelo de Schengen, según el cual la asistencia mutua entre los servicios de policía con fines específicos y el intercambio de datos persona - les se basa en la adhesión al Convenio 108 y el precepto en materia de protección de datos contenido en el propio tratado de Schengen.

6 situaciones en que el país requirente ofrece un inadecuado nivel de protección de los particulares, en lo referente al tratamiento de sus datos personales, susceptible de amenazar los derechos y libertades fundamentales de los afecta - dos. En este contexto, ha de referirse explícitamente que el derecho a la protección de los datos ha quedado consa - grado recientemente en el artículo 8 de la Carta de derechos fundamentales de la UE. La existencia o inexistencia de un adecuado nivel de protección en el tercer país se menciona también en el Convenio Europol como criterio impor - tante para decidir si Europol comunica, y en qué medida, datos personales a dicho tercer país con fines policiales.

Pese a que el artículo 27bis pueda de alguna manera, si se aclara y modifica según se ha propuesto, abordar las cues - tiones de confidencialidad y de limitación con arreglo a los fines en el contexto específico de la transferencia de datos personales a países no pertenecientes al Consejo de Europa o a la UE, el Grupo de trabajo opina que el compromiso de los signatarios de cumplir los requisitos del artículo 27bis no constituirá necesariamente un compromiso de protec - ción de la vida privada adecuado (véase más arriba). La inclusión de preceptos en materia de protección de datos ayudará a codificar y aclarar la prueba de necesidad, procedencia y proporcionalidad que imponen los instrumentos citados anteriormente.

El Grupo de trabajo opina también que los signatarios del convenio deben cumplir los requisitos contemplados en los preceptos sobre protección de datos, antes de que se decida que ofrecen un nivel adecuado de amparo de los dere - chos y libertades de los afectados. Este planteamiento contribuirá a la armonización de las garantías y requisitos que han de aplicarse a las medidas previstas en el proyecto de convenio. Si una parte de un tercer país va a disfrutar de las ventajas que supone la transferencia de datos personales, debe aceptar una vez que los datos obren en su poder la debida responsabilidad de proteger adecuadamente los derechos fundamentales de las personas afectadas.

Datos de tráfico

El Grupo de trabajo se congratula de que, contrariamente a los anteproyectos previos, la versión actual del Convenio (versión n° 25) no incluya ya una obligación general de supervisión, que conlleva la retención sistemática de los datos de tráfico. Este cambio coincide con la Recomendación 3/99 del Grupo de trabajo sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, que se aprobó el 7 de septiembre de 199910 y aduce los argumentos jurídicos" contra tal obligación general.

También las autoridades de protección de datos de la UE, en la conferencia que mantuvieron en la primavera de 2000 en Estocolmo, manifestaron su firme oposición a esta medida. Aprobaron entonces una resolución en la que señalaron "con preocupación que, según las propuestas presentadas, los proveedores de servicios de Internet deberían almace - nar habitualmente los datos sobre tráfico no sólo con fines de facturación, con objeto de permitir un posible acceso de los organismos encargados de velar por el cumplimiento de la ley. La Conferencia señaló que esta retención constitui - ría una invasión ilegal de los derechos fundamentales que garantiza el artículo 8 del Convenio

Puede consultarse en:

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wpdocs_99.htm

Con referencia en particular a la Directiva 97/66/CE.

7 Europeo de Derechos Humanos y declaró que en los casos específicos en que se hayan de conservar datos sobre tráfico, debería existir una necesidad demostrable, el período de conservación debería ser lo más breve posible y la práctica debería estar claramente regulada por la ley."

Las opiniones sobre esta cuestión son convergentes. Otras instituciones y grupos, como el Grupo internacional de trabajo sobre protección de datos en las telecomunicaciones en su Posición Común sobre los aspectos de protección de datos en el proyecto de convenio 12, han expresado fuertes reservas al respecto.

No obstante, los preceptos del proyecto de convenio sobre datos de tráfico plantean graves dudas: los artículos 29 y 30

sobre conservación y divulgación rápida de los datos de tráfico y otros no dan la posibilidad a la parte requerida de denegar la asistencia por razones de protección de datos, sino sólo por motivos generales similares a los citados anteriormente ("orden público", etc.). Al mismo tiempo, la obligación de conservar los datos informáticos y de tráfico almacenados, si así se solicita, durante un plazo mínimo de 60 días para que pueda tomarse una decisión sobre su necesidad y las modalidades de utilización, conlleva una carga enorme sobre las empresas (operadores de telecomunicaciones, proveedores de servicio internet y otros) y los particulares. Preocupaciones parecidas recaen sobre el artículo 20, por el que se obliga a los proveedores de servicio a recoger o registrar los datos de tráfico en tiempo real con arreglo a su capacidad técnica.

De manera general, las empresas pueden precisar de una mayor seguridad jurídica sobre sus obligaciones y la concreta aplicación de éstas. Por otra parte, podrían albergar temores de que los consumidores no tengan suficiente confianza en sus productos y servicios si no estuviese claro quién tiene acceso a la información y las comunicaciones confidenciales y en qué momento.

Conclusiones

El Grupo de trabajo destaca la importante función que el Consejo de Europa desempeña desde hace décadas como eficaz guardián de los derechos y libertades fundamentales. Opina que ésta institución, al fomentar la cooperación internacional en materia de ciberdelito más allá de sus propios miembros, tiene que prestar especial atención a la protección de los derechos y libertades fundamentales y, señaladamente, del derecho a la protección de la vida privada y los datos personales.

12 Grupo internacional de trabajo sobre protección de datos en las telecomunicaciones, Posición

Común sobre los aspectos de protección de datos en el proyecto de convenio sobre el ciberdelito del Consejo de Europa, aprobada en su 28 reunión de los días 13/14 de septiembre de 2000 en Berlín. Se puede consultar en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm.

8 El Grupo de trabajo considera, pues, que es necesario aclarar el texto de los artículos del proyecto de convenio porque su redacción resulta con frecuencia demasiado vaga y confusa, y podría no constituir fundamento suficiente para las leyes y medidas vinculantes destinadas a limitar legalmente los derechos y libertades fundamentales. Las explicaciones de la Exposición de motivos no pueden suplantar la claridad jurídica del propio texto.

La mayor parte de los preceptos del proyecto de convenio tienen una repercusión enorme sobre los derechos fundamentales de la persona a la vida privada y la protección de los datos personales. Como se dijo anteriormente, las opciones expresadas en el texto actual anticipan, hasta cierto punto, el resultado del examen que es necesario efectuar si el derecho fundamental a la vida privada (artículo 8 del CEDH) y otros van a ser objeto de limitaciones' Uno de los problemas básicos al respecto es determinar cuándo es necesaria una medida en un caso concreto y, si lo es, cuándo es procedente, proporcionada y no excesiva. Algunos de los elementos del proyecto de convenio son completamente nuevos y su repercusión en los derechos fundamentales, especialmente en el derecho fundamental de la persona a la vida privada y la protección de los datos personales, podría no haberse evaluado de manera suficiente por la Comisión de expertos en infracciones penales en el ciberespacio (PC-CY). El Grupo de trabajo considera que es preciso mejorar la justificación de las medidas previstas desde el punto de vista de la necesidad, la procedencia y la proporcionalidad tal como exigen los instrumentos citados anteriormente en materia de derechos humanos y protección de datos.

El Grupo de trabajo recomienda enérgicamente que el proyecto de convenio incorpore preceptos en materia de protección de datos, que esbocen la protección que debe proporcionarse a los sujetos de la información susceptible de tratamiento en relación con las medidas contempladas en el proyecto de convenio. También habrá de incluirse y mejorarse, según se indica, el artículo 27bis (por tanto, habrán de borrarse los paréntesis). La inclusión de estos preceptos ayudará a codificar y aclarar los requisitos de necesidad, procedencia y proporcionalidad que exige el acervo del Consejo de Europa y los Estados miembros de la UE.

El Grupo de trabajo opina, además, que debe incluirse en el preámbulo la referencia al Convenio 108 (por tanto, habrán de borrarse los paréntesis), aunque no tenga carácter vinculante, así como invitarse a los signatarios del Convenio sobre el ciberdelito a firmar el Convenio 108 sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Asimismo, el Grupo de trabajo lamenta que no se haya contemplado la incriminación por infracción de las normas en materia de protección de datos.

El Grupo de trabajo observa una discrepancia en el trato que reciben los países del Consejo de Europa frente a otros, porque aquéllos deben cumplir las obligaciones derivadas del Convenio europeo para la protección de los derechos humanos, el Convenio 108, las Recomendaciones pertinentes del Consejo de Europa, la Carta de derechos fundamentales de la UE, las directivas de protección de datos de la UE y la legislación nacional que haga al caso, mientras que los países no pertenecientes al Consejo de Europa no tienen, con arreglo al actual proyecto de convenio, las mismas o parecidas obligaciones.

13 Por ejemplo, la interceptación de comunicaciones y datos de tráfico violan plenamente el secreto de correspondencia (Véase la sentencia Malone del Tribunal Europeo de Derechos Humanos).

9 El Grupo de trabajo opina además que los signatarios del Convenio deben aceptar la debida responsabilidad de

proteger adecuadamente los derechos fundamentales de las personas afectadas, desde el momento que los datos sobre ellas procedan de los Estados miembros de la Unión Europea y el Consejo de Europa.

No debe de ninguna manera revisarse la posición propuesta en el actual proyecto de convenio (versión pública 25) de no imponer a los signatarios la obligación de apremiar a los proveedores de servicios la retención de los datos de tráfico de todas las comunicaciones.

El Grupo de trabajo lamenta la muy tardía difusión de los documentos correspondientes.

Considera muy deseable que el debate público se prolongue y participen en él todos los interesados (organizaciones de derechos humanos, industria, etc.), antes de que la Asamblea Parlamentaria del Consejo de Europa debata y decida.

El Grupo de trabajo opina que el gran número de deficiencias señaladas en el presente dictamen es, aparentemente, resultado de no haber hecho el Consejo de Europa el mejor uso posible de la experiencia existente en asuntos de protección de datos. Por consiguiente, invita al Consejo de Europa, y especialmente a los Estados miembros de la UE, a consultar con sus especialistas en la materia antes de adoptar una posición definitiva sobre el proyecto de convenio y a hacer el mejor uso posible de su contribución.

El Grupo de trabajo invita al Consejo de Europa, la Comisión Europea, el Parlamento Europeo y los Estados miembros a tener en cuenta el presente dictamen.

El Grupo de trabajo se reserva la posibilidad de efectuar nuevos comentarios.

Hecho en Bruselas, a 22 de marzo de 2001

Por el Grupo de trabajo

El Presidente

Stefano RODOTA

Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

5020/01/ES/Final

WP 43

RECOMENDACIÓN

sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea

Aprobada el 17 de mayo de 2001

El Grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE. La secretaría encargada es la siguiente:

Comisión Europea, DG Mercado Interior, Funcionamiento e Impacto del Mercado Interior, Coordinación y Protección de Datos.

Rue de la Loi 200, B-1 049 Bruxelles/Wetstraat 200, B-1049 Bruselas - Bélgica - Despacho: Ci 00-6/136

Teléfono: directo (32-2)295.72.58 o 299.27.19. central: 299.11.11 .Telefax: (32-2)296.80.10.

Dirección Internet: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

2 EL GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995',

Vistos el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de la mencionada Directiva,

Visto su reglamento interno y, en particular, sus artículos 12 y 14, ha aprobado la presente recomendación:

1 Introduccion

1. En su documento de trabajo titulado «Privacidad en Internet: enfo que comunitario integrado de la protección de

datos en línea» de 21 de noviembre de 20012, El Grupo de trabajo destacó la importancia de garantizar que se aplican los medios adecuados para garantizar que los usuarios individuales de Internet obtienen toda la información necesaria para depositar su confianza, con pleno conocimiento de causa, en los sitios con los que establecen contacto y, en caso necesario, para ejercer determinadas opciones de conformidad con sus derechos según la legislación europea. Esto cobra especial importancia dado que el uso de Internet multiplica las oportunidades de recopilar datos personales y, por tanto, el riesgo de incumplimiento de los derechos y libertades fundamentales de las personas, en especial el derecho a la vida privada. En su Dictamen 4/2000, de 16 de mayo de 2000, sobre el nivel de protección que proporcionan los «principios de puerto seguro», el Grupo de trabajo invitó a la Comisión a considerar con urgencia la creación de un sistema de sello comunitario para los sitios Internet basado en criterios comunes de evaluación de la protección de los datos que pueda determinarse a escala comunitaria.

La presente Recomendación se basa en los dos documentos antes citados. Su objetivo es contribuir a la aplicación eficaz y homogénea de las disposiciones nacionales adoptadas de conformidad con las Directivas de protección de datos personales aportando indicaciones concretas sobre la manera en que se deberían aplicar las

1 Diario Oficial L 281 de 23.11.1995, p. 31,disponible en:

2 WP 37 (5063/00): Documento de trabajo - Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. Adoptado el 21 de noviembre de 2000.

Se puede consultar en: http://europa.eu.int/comrn/internai rnarket'en!media/dataprot/wpdocs/wp37es.pdf

Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas fisicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sectordelastelecomunicaciones. Se pueden consultar en:

http://europa.eu.int/comm/internal_market/enlmedia/dataprot/law.

3 normas establecidas en las Directivas a las tareas de tratamiento más habituales llevadas a cabo a través de Internet. Este tratamiento se produce, especialmente, durante «el contacto inicial» entre un usuario de Internet y un sitio web, ya sea únicamente para buscar información o bien parar concluir una transacción comercial paso a paso.

Las indicaciones que se ofrecen a continuación se refieren básicamente a la recogida de datos personales en la web y su intención es identificar las medidas concretas que habrán de aplicar los agentes participantes a fin de garantizar que el tratamiento es lícito y leal (en aplicación de los artículos 6, 7, 10 y 11 de la Directiva 95/46/CE). Se centran especialmente en cuándo, cómo y qué información debe facilitarse al interesado, pero añaden detalles prácticos sobre otros derechos y obligaciones procedentes de las Directivas.

El principal objetivo de la presente Recomendación, por tanto, es aportar un valor añadido práctico para la aplicación de los principios generales de la Directiva. El Grupo de trabajo considera la presente Recomendación una iniciativa inicial para detallar, a escala europea, un conjunto «mínimo» de obligaciones que puedan seguir fácilmente los sitios web operativos responsables del tratamiento (la persona fisica o jurídica responsable del tratamiento de datos personales en el contexto de un sitio web) que quizá sea preciso completar añadiendo detalles o asuntos adicionales Por supuesto, esto no dispensa a los responsables del tratamiento de sus actuales obligaciones de verificar el tratamiento respecto a todos los requisitos y condiciones establecidos en la legislación nacional que les sea de aplicación a fin de que sea lícito.

La presente Recomendación es de aplicación si el responsable del tratamiento está establecido en un Estado miembro de la Unión Europea. En este caso, la legislación nacional del Estado miembro en cuestión será de aplicación para el tratamiento de datos personales en el marco de las actividades de dicho establecimiento. La Recomendación también se aplicará cuando el responsable del tratamiento no esté establecido en territorio comunitario pero, para fines de tratamiento de datos personales, recurra a medios, automatizados o no, situados en el territorio de uno de los Estados miembros de la UE. Este tratamiento quedará cubierto por la legislación

4 Para facilitar la referencia, el articulo 2 de la Directiva 95/46/CE defme al responsable del tratamiento como «la persona fisica o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fmes y los medios del tratamiento de datos personales; en caso de que los fmes y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario».

Las recomendaciones concretas realizadas en la presente Recomendación son requisitos mínimos, en el sentido de que no son los únicos. En el futuro deberán complementarse con recomendaciones adicionales sobre el tratamiento de datos personales más delicados, tales como el tratamiento en relación son sitios médicos, sitios destinados a niños o servicios de portal. En lo que respecta a otros tratamientos específicos, como la difusión de datos personales en un sitio o el almacenamiento de datos sobre tráfico por proveedores de servicios de Internet o proveedores de contenidos y servicios de Internet, consúltense las recomendaciones del Grupo de trabajo en el documento citado en la nota 1 y otras posiciones pertinentes tomadas por el Grupo de trabajo, por ejemplo, el WP 25 (5085/99): Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999. WP 18 (5005/99): Recomendación 2/99 sobre la protección de la

intimidad en el contexto de la interceptación de las telecomunicaciones, aprobada el 3 de mayo de 1999. WP 17 (5093/98):

Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, aprobada el 23 de febrero de 1999. Todas ellas se pueden consultar en: véase la nota 1.

nacional del Estados miembro donde estén situadas dichas instalaciones o medios técnicos

2. Para alcanzar este objetivo, la recomendación se dirige en particular:

- A los responsables del tratamiento que recogen datos en línea, a los que se facilita una guía práctica que enumera un conjunto mínimo de medidas concretas que deberán aplicar.

- A los usuarios individuales de Internet para que se estén informados sobre sus derechos y puedan ejercerlos.

- A los organismos que deseen conceder etiquetas que certifiquen la adecuación de los procedimientos de tratamiento utilizados con las Directivas europeas sobre protección de datos, proporcionándoles criterios de referencia para conceder dichas etiquetas en relación con la información que deben proporcionar y la recogida de datos personales. Por supuesto, a la hora de conceder etiquetas, además de estos criterios de referencia, deberán tenerse en cuenta necesariamente otros criterios relativos a distintas obligaciones y derechos. El Grupo de trabajo elaborará más adelante un documento completo sobre este asunto.

- A las autoridades europeas de protección de datos para facilitarles un marco de referencia común para su tarea de verificar el cumplimiento de las disposiciones nacionales adoptadas por los Estados miembros de conformidad con las Directivas antes mencionadas.

3. Además, el Grupo de trabajo opina que la presente Recomendación debería asimismo servir como referencia para desarrollar normas para software y hardware destinados a la recogida y el tratamiento de datos personales en Internet.

11 Recomendaciones sobre Ja información que deberá facilitarse al recoger datos personales en el territorio de los Estados miembros de la Unión Europea

2.1. Información que debe facilitarse al interesado y en qué momento

4. Toda recogida de datos personales de un interesado a través de un sitio web implica facilitar previamente determinada información. Respecto al contenido, para cumplir esta obligación es necesario:

5. Declarar la identidad y las direcciones postal y electrónica del responsable del tratamiento y, cuando sea aplicable, la del representante designado en virtud del apartado 2 del artículo 4 de la Directiva.

6. Indicar claramente para qué fines de tratamiento recoge los datos el responsable a través de un sitio. Por ejemplo, cuando los datos se recogen tanto para firmar un

6 Véanse letras a) y c) del apartado 1 del artículo 4 de la Directiva 95/46/CE. Es preciso distinguir claramente este caso de la cuestión de si los datos personales se pueden transferir legítimamente desde la UE hasta un tercer país, que se aborda en los artículos 25 y 26 de la Directiva 95/46/CE, y de las decisiones correspondientes de la Comisión Europea sobre la adecuación del nivel de protección de un tercer país. Por ejemplo, si un sitio web estadounidense utiliza medios dentro de la UE para recoger y tratar datos personales, la legislación del país europeo en cuestión será aplicable a dicha recogida, así como a las operaciones de tratamiento, independientemente de si se considera o no que esta entidad ofrece un nivel de protección adecuado de conformidad con la decisión de la Comisión Europea relativa al puerto seguro. La cuestión de si el destinatario de los datos se ha adherido al puerto seguro solamente será relevante para la legalidad de la transferencia ulterior a dicha entidad de datos personales por parte de una entidad establecida en la UE.

5 contrato (suscripción a Internet, pedido de un producto, etc.) como para márketing directo, el responsable del tratamiento debe indicar claramente ambos fines.

7. Informar claramente sobre si la información solicitada es obligatoria u opcional. La información obligatoria es aquella necesaria para prestar el servicio solicitado. La naturaleza obligatoria u opcional se podría indicar, por ejemplo, mediante un asterisco junto a los datos obligatorios o bien añadiendo la palabra «opcional» junto a la información no obligatoria. El hecho de que el interesado no facilite la información opcional no se utilizará en su contra de ninguna manera.

8. Mencionar la existencia de los derechos de consentimiento u oposición, según el caso, respecto al tratamiento de datos personales, y de las condiciones para ejercer tales derechos así como los derechos de acceso, rectificación y eliminación de datos. Deberá facilitarse información, en primer lugar, sobre la persona o el servicio al que acudir para ejercer estos derechos y, en segundo lugar, sobre la posibilidad de ejercerlos tanto en línea como en la dirección postal del responsable del tratamiento.

9. Enumerar los destinatarios o las categorías de destinatarios para la información recopilada Al recoger cualquier tipo de datos, los sitios deberán indicar si los comunicarán o pondrán a disposición de terceros, en particular socios

empresariales, filiales, etc., y por qué motivo (fines distintos de prestar el servicio solicitado y de márketing directo 8)

Si se da este caso, los usuarios de Internet tendrán la posibilidad real de oponerse a ello en línea marcando una casilla relativa a la comunicación de datos para fines distintos de la prestación del servicio solicitado. Puesto que el derecho de oposición se puede ejercer en cualquier momento, la posibilidad de ejercerlo en línea también debería indicarse en la información facilitada al interesado. El Grupo de trabajo, consciente del inconveniente que supone sobrecargar de información las pantallas, es de la opinión de que no mencionar los destinatarios equivale a que el responsable de los datos se compromete a no comunicar ni transmitir la información recogida a terceras partes cuya denominación y dirección no haya facilitado, a menos que la identidad de dicha tercera parte sea obvia y la comunicación de los datos sea estrictamente necesaria para prestar el servicio solicitado por el usuario de Internet y siempre que la comunicación se realice exclusivamente para ese fin.

El tratamiento para un fin específico solamente es legítimo si se basa en uno de los supuestos enumerados en el artículo 7 de la Directiva 95/46/CE (entre otros, si el interesado ha dado su consentimiento de forma inequívoca, si el tratamiento es necesario para la ejecución de un contrato en el que el interesado sea parte, si el tratamiento es necesario para el cumplimiento de una obligaciónjurídica a la que esté sujeto el responsable del tratamiento, si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés del interesado).

Los Estados miembros reconocerán el derecho de oposición (véase el artículo 14) al menos en dos situaciones recogidas en el artículo 7, incluida la última citada en el párrafo anterior. El interesado tendrá el derecho a oponerse, 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. El derecho de oposición previa petición y sin gastos existe en cualquier caso cuando el tratamiento en cuestión está destinado a fmes de márketing directo. Además, el interesado podrá oponerse sin gastos (una vez informado y desde la primera vez que se comuniquen sus datos) a que sus datos personales se comuniquen a terceros o se usen en nombre de éstos con fines de márketing directo.

8 La comunicación a terceros solamente se autorizará si el fin previsto no es incompatible con el fin para el cual se recopilaron los datos y si se basa en uno de los supuestos enumerados en el artículo 7 que legitiman el tratamiento.

10. Si se prevé que el responsable de los datos transfiera dichos datos a países no miembros de la Unión Europea, indicar si estos países ofrecen una adecuada protección de los interesados en cuanto al tratamiento de sus datos personales en el sentido que recoge el artículo 25 de la Directiva 95/46/CE. En este caso, se deberá facilitar información específica sobre la identidad y la dirección de los destinatarios (dirección postal y/o electrónica)

11. Proporcionar el nombre y la dirección (postal y electrónica) del servicio o la persona responsable de responder a las preguntas relacionadas con la protección de los datos personales.

12. Mencionar con claridad la existencia de procedimientos automáticos de recogida de datos, antes de usar dichos métodos'°.

Cuando se utilicen tales procedimientos, el interesado deberá recibir la información indicada en este documento. Además, se le deberá informar del nombre de dominio del servidor de sitios que transmite los procedimientos automáticos de recogida, la finalidad de dichos procedimientos, su plazo de validez, si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio y la opción de que dispone todo usuario de Internet de oponerse a su uso, además de las consecuencias de desactivar dichos procedimientos. En caso de que otros responsables del tratamiento de los datos participen en la recogida de datos personales, el interesado deberá recibir información sobre la identidad de los responsables del tratamiento y la finalidad del tratamiento en relación con cada controlador.

La información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio web, por ejemplo, cuando un sitio web conecta automáticamente al usuario a otro sitio para mostrarle publicidad en forma de pancarta publicitaria, con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello.

Por ejemplo, si el servidor de un responsable del tratamiento coloca una cookie, la información deberá facilitarse antes de que ésta se envíe al disco duro del usuario de Internet, además de la información facilitada por la tecnología actual, que se limita a dar el nombre del sitio transmisor y el periodo de validez de la cookie".

13. Destacar las medidas de seguridad que garantizan la autenticidad del sitio, la integridad y la confidencialidad de la información transmitida a través de la red y que se hayan tomado en aplicación de la legislación nacional en vigor.'

La información relativa a las resoluciones sobre idoneidad se puede consultar en la siguiente dirección del sitio web de la Comisión: http://europa.eu.int/eornrn/internal rnarket/enImedia/data

O El tratamiento «invisible» y automático de datos personales está sujeto a los mismos términos, condiciones y garantías que los demás tratamientos de estos datos. Consúltese la Recomendación 1/99 del Grupo de trabajo sobre el tratamiento invisible y automático de datos personales en Internet efectuado por , y hardi de febrero de 1999), en el sitio web mencionado en la nota 1.

Si una organización deposita una cookie a través de su propio sitio web y esta organización es la única que puede

acceder al contenido de dicha cookie, no existe ningún requisito adicional de información identificativa de la organización responsable de colocarla, siempre que ya esté adecuadamente identificada la organización a la que pertenece el sitio web.

12 Véanse las normas específicas en el apartado 1 y en el segundo guión del apartado 3 del artículo 17 de la Directiva 95/46/CE.

14. La información se proporcionará en todos los idiomas utilizados en el sitio y, en particular, en los lugares donde vayan a recogerse datos personales.

15. Los responsables del tratamiento deberán verificar la coherencia de la información proporcionada en los diversos «documentos» que comprometen al sitio (encabezado «datos personales y protección de la intimidad», formularios electrónicos, texto relativo a las condiciones generales de venta y otras comunicaciones comerciales).

2.2. Cómo debe facilitarse la infbrmación

16. El Grupo de trabajo considera que la información siguiente debe mostrarse directamente en la pantalla antes de la recogida para garantizar el tratamiento leal de los datos:

- la identidad del responsable del tratamiento

- la finalidad

- el carácter obligatorio o no de la información solicitada

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

- la existencia de los derechos de acceso y rectificación

- la existencia del derecho de oposición a que los datos se comuniquen a terceros para fines distintos de la prestación del servicio solicitado y la manera de ejercerlo (por ejemplo, mediante una casilla que el usuario pueda marcar)

- la información que se deberá proporcionar al utilizar procedimientos automáticos de recogida

- el nivel de seguridad durante todas las fases del tratamiento incluida la transmisión, por ejemplo, entre redes.

En estos casos, la información deberá proporcionarse de manera interactiva y en pantalla. Así, en el caso de los métodos automáticos de recogida de datos, si es necesario esta información podría facilitarse mediante la técnica de una ventana «emergente».

En lo que respecta al nivel de seguridad durante la transmisión de los datos desde el equipo del usuario hasta el sitio web, se podría emplear un encabezado del tipo:

«Está iniciando una sesión segura» o los procedimientos de información automática de que disponen los navegadores, como la aparición de iconos específicos en forma de llave o de candado.

17. Además, el Grupo de trabajo considera que en la página inicial del sitio y en todos los lugares donde se recojan datos personales en línea deberá poderse acceder directamente a información completa sobre la política de protección de la intimidad (incluida la forma de ejercer el derecho de acceso). El título del encabezado que deba seleccionarse con el ratón deberá estar resaltado, ser explícito y específico, de manera que transmita al usuario de Internet una idea clara del contenido que se le va a mostrar. Por ejemplo, el encabezado podría indicar «Esta página recoge y trata datos personales relacionados con usted. Si desea más información, pinche aquí» o bien «Protección de datos personales o de la intimidad». También deberá ser lo bastante específico el contenido de la información a la que se dirige el usuario de Internet.

111. Recomendaciones para la aplicación de otros derechos y obligaciones

El Grupo de trabajo también desearía llamar la atención de los destinatarios de la presente Recomendación sobre otros derechos de las personas y otras obligaciones de los responsables del tratamiento basados en las directivas que cobran especial importancia en el contexto de la recogida de datos personales en los sitios web. Como sucede con las indicaciones sobre la información, el Grupo de trabajo considera que las recomendaciones siguientes ofrecen un valor práctico inmediato tanto para los responsables del tratamiento como para los usuarios de Internet.

18. Recoger únicamente los datos que sean necesarios para alcanzar la finalidad especificada

19. Asegurarse de que los datos sean tratados únicamente de manera legítima según alguno de los criterios enumerados en el artículo 7 de la Directiva 95/46/CE.

20. Garantizar el ejercicio efectivo de los derechos de acceso y rectificación derechos que deberán poderse ejercer tanto en la dirección postal del responsable del tratamiento como en línea. Deberán existir medidas de seguridad para garantizar que únicamente el interesado tenga acceso en línea a la información que le concierne.

21. Aplicar el principio de «finalidad» o «propósito», que exige el uso de los datos personales únicamente cuando sea necesario para una finalidad específica. Es decir, sin un motivo legítimo, los datos personales no podrán utilizarse y el interesado conservará el anonimato apartado 1 del artículo 6 de la Directiva 95/46/CE). Este principio se denomina a veces «principio de minimización de los datos».

22. En el mismo contexto descrito en el punto 21, facilitar y promover la consulta anónima de sitios comerciales sin solicitar a los usuarios que se identifiquen mediante su nombre, apellido, dirección electrónica u otros datos.

Cuando se precise un vínculo con el usuario sin que sea necesaria su identificación completa, proponer y aceptar el uso de todo tipo de seudónimos.

En caso de no existir requisitos jurídicos de identificación, fomentar y aceptar el uso de seudónimos, incluso para determinadas transacciones. Un ejemplo es el uso de certificaciones con seudónimos para firmas electrónicas (véase el artículo 8 de la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica).

23. Definir un periodo de almacenamiento para los datos recogidos. Los datos solamente se pueden conservar durante el periodo justificado por la finalidad del tratamiento especificado y realizado (artículo 6 de la Directiva 95/46/CE y artículo 6 de la Directiva 97/66/CE).

24. Emprender las acciones necesarias para garantizar la seguridad de los datos durante el tratamiento, incluida la transmisión (por ejemplo, limitar y definir las personas a las que se autoriza el acceso a los datos, utilizar un encriptado potente, etc. Artículo 17 de la Directiva 95/46/CE).

25. Cuando participe un encargado del tratamiento, por ejemplo para alojar un sitio web, firmar un contrato en el que se exija a dicho encargado la aplicación de medidas de seguridad apropiadas de conformidad, asimismo, con la legislación del Estado miembro donde esté establecido y el tratamiento de los datos personales únicamente siguiendo las instrucciones del responsable del tratamiento.

26. Notificar a la autoridad de control según corresponda a tenor de la legislación nacional (cuando el responsable del tratamiento del sitio esté establecido en la Unión Europea o tenga un representante en territorio comunitario). El número de registro de la notificación puede aparecer en el sitio, preferentemente bajo el encabezado dedicado a la protección de datos.

27. Al transferir información a m tercer país donde no se garantice la protección de datos, asegurarse de que la transferencia de datos solamente tiene lugar si se cumple alguna de las excepciones establecidas en el artículo 26 de la Directiva 95/46/CE. En tales casos, informar al interesado sobre las garantías correspondientes para asegurar la legalidad de la transferencia.

IV. Recopilación de direcciones con fines de márketing directo por correo electrónico y envío de boletines de información

28. En lo que respecta al márketing directo por correo electrónico

- El Grupo de trabajo reitera su opinión de que no es lícito recopilar direcciones electrónicas en áreas públicas de Internet, tales como foros o grupos de debate, sin conocimiento del interesado. Por lo tanto, estas direcciones no se podrán usar para una finalidad distinta de aquella para la cual se han hecho públicas, en especial, el márketing directo'

- El uso de las direcciones electrónicas para márketing directo exclusivamente cuando se hayan recopilado de manera leal y lícita. La recogida leal y lícita implica que los interesados han recibido información sobre la posibilidad de que sus datos se utilicen con fines comerciales de márketing directo y se les ha dado la opción de aceptar dicho uso directamente en el momento de recoger la información (casilla de aceptación en línea)' El envío de mensajes electrónicos con fines promocionales

13 Véase WP 28 (5007/00): «Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico», adoptado el 3.2.2000, WP 29 (5009/00): «Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones», adoptado el 3.2.2000, y, en particular, en cuanto a la aplicación de los artículo 6 y 7 de la Directiva 95/46/CE, WP 36 (5042/00): «Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000 (COM(2000)385)», adoptado el 2.11.2000 y WP 37 (5063/00): «Documento de trabajo: Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea», adoptado el 21.11.2000.

14 Dentro de la Unión Europea, cinco Estados miembros (Alemania, Austria, Italia, Finlandia y Dinamarca) han adoptado medidas destinadas a prohibir las comunicaciones comerciales no solicitadas. En los demás Estados miembros, o bien existe un sistema de «exclusión» o bien la situación no está del todo clara. Es de observar que la propuesta de directiva de la Comisión relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (COM(2000) 385) de 12 de julio de 2000 favorece una solución armonizada basada en el enfoque de «inclusión» apoyada por unanimidad por el Grupo de trabajo en su Dictamen 7/2000 (WP 36 antes citado). Véase también el estudio de S. Gauthronet y E. Drouard (ARETE) para la Comisión «Unsolicited Cornrnercial Cornrnunications and Data Protection» enero de 2001, en http://europa.eu.

int/comm/internal_market/enlmedia/dataprot/studies/spamsum.pdf.

en estas condiciones también irá acompañado de la posibilidad de borrarse en línea de la lista de correo utilizada para ello'

29. En lo que respecta al envío de boletines de información:

- Garantizar la aceptación previa de los interesados y asegurarse de que pueden dar efectivamente de baja su suscripción en cualquier momento, lo que implica informarles de esta posibilidad en cada envío del boletín.

El Grupo de trabajo invita al Consejo, a la Comisión Europea, al Parlamento Europeo y a los Estados miembros a que tengan en cuenta la presente Recomendación.

El Grupo de trabajo se reserva la posibilidad de emitir comentarios adicionales.

Hecho en Bruselas, el 21 de mayo de 2001

Por el Grupo de trabajo

El Presidente

Stefano RODOTA

15 En la Directiva sobre comercio electrónico se establecen requisitos adicionales relativos a comunicaciones comerciales no solicitadas en los casos en que se permite la exclusión basándose en la Directiva 97/66/CE.

El tratamiento de datos personales en el contexto laboral es objeto de debate tanto a nivel comunitario como nacional. Los gobiernos y las autoridades de protección de datos de los Estados miembros han elaborado o están elaborando legislación, códigos o recomendaciones que abordan diversas cuestiones sobre protección de datos en este contexto. En el marco de su Agenda de política social, la Comisión Europea ha puesto en marcha un proceso de consultas con los interlocutores sociales sobre la protección de datos en el contexto laboral.

RESUMEN

El tratamiento de datos personales en el contexto laboral es objeto de debate tanto a nivel comunitario como nacional. Los gobiernos y las autoridades de protección de datos de los Estados miembros han elaborado o están elaborando legislación, códigos o recomendaciones que abordan diversas cuestiones sobre protección de datos en este contexto. En el marco de su Agenda de política social, la Comisión Europea ha puesto en marcha un proceso de consultas con los interlocutores sociales sobre la protección de datos en el contexto laboral.

Con el fin de contribuir a la aplicación uniforme de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE sobre protección de datos el grupo de trabajo ha creado un subgrupo para estudiar esta cuestión y ha aprobado un amplio documento que puede consultarse en Internet en la siguiente dirección http://europa.eu. mt/comrn/rnterna rnarket/efl/dataprot/wpdocs/ifldexhtlTl

Los empresarios y los trabajadores deben ser conscientes de que muchas actividades realizadas de forma rutinaria en el ámbito del empleo implican el tratamiento de datos personales de los trabajadores, a veces de información muy delicada Cualquier actividad de recopilación, uso o almacenamiento de información sobre los trabajadores por medios electrónicos entrará casi con toda seguridad en el ámbito de

1 Grupo de trabajo del artículo 29 es un grupo consultivo compuesto por representantes de las autoridades de protección de datos de los Estados miembros, que actúa de forma independiente y se ocupa, entre otras cosas, de examinar cualquier cuestión relativa a la aplicación de las medidas nacionales adoptadas en el marco de la Directiva sobre protección de datos, con el fin de contribuir a la aplicación uniforme de las mismas.

2 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas fisicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DO L 281 de 23 11.95, p. 31

Al trabajo de este subgrupo han contribuido las siguientes autoridades de supervisión: AT, BE, DE,

EL, ES, FR, IRL, IT, NL, UK.

El documento incluye un catálogo de la legislación sobre protección de datos más pertinente de los Estados miembros, con alguna repercusión en el contexto del empleo.

Ejemplos de documentos laborales que implican normalmente el tratamiento de datos personales cubiertos por la Directiva 95/46/CE: formularios de solicitud y referencias laborales, información salarial y fiscal, información sobre beneficios fiscales y prestaciones sociales, registros de enfermedad, registros de vacaciones, registros sobre permisos especiales/no remunerados, registros sobre evaluación anual, registros relativos a promociones, traslados, formación,

asuntos disciplinarios, accidentes laborales, etc.

aplicación de la legislación sobre protección de datos. Es el caso, por ejemplo, del control por parte del empresario del correo electrónico o del acceso a Internet de los trabajadores. El control del correo electrónico implica necesariamente el tratamiento de datos personales. El tratamiento de datos en forma de imagen y sonido en el contexto laboral pertenece también al ámbito de la legislación relativa a la protección de datos y la videovigilancia de los trabajadores está cubierta por las disposiciones de la Directiva y las disposiciones nacionales de aplicación.

Al tratar los datos personales de los trabajadores, los empresarios deberán tener siempre en cuenta los PRINCIPIOS FUNDAMENTALES DE LA PROTECCIÓN DE DATOS, A

SABER

• FINALIDAD Los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.

• TRANSPARENCIA Como mínimo, los trabajadores deben saber qué datos recoge el empresario sobre ellos (directamente o de otras fuentes) y cuáles son los fines de las operaciones de tratamiento previstas o realizadas con estos datos en la actualidad o en el futuro. La transparencia también puede garantizarse otorgando al interesado el derecho de acceso a los datos personales que le afectan y obligando al responsable del tratamiento a notificar a las autoridades supervisoras según lo previsto en la legislación nacional.

• LEGiTIMIDAD El tratamiento de los datos personales de los trabajadores deberá ser legítimo. El artículo 7 de la Directiva enumera los principios relativos a la legitimación del tratamiento de datos.

• PROPORCIONALIDAD Los datos personales deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. Suponiendo que se ha informado a los trabajadores sobre el tratamiento y que dicho tratamiento es legítimo y proporcionado, este tratamiento también deberá ser leal con el trabajador.

• EXACTITUD Y CONSERVACIÓN DE LOS DATOS Los registros profesionales deberán ser exactos y, cuando sea necesario, actualizados. El empresario deberá tomar 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.

• SEGURIDAD El empresario deberá implantar medidas adecuadas de carácter técnico y organizativo en el lugar de trabajo para garantizar la seguridad de los datos personales de sus trabajadores. Deberá preverse una protección especial en lo que respecta al acceso o difusión no autorizados.

• FoRMACIÓN DEL PERSONAL El personal encargado del tratamiento de datos personales de otros trabajadores o con responsabilidades en este ámbito deberá tener conocimientos sobre protección de datos y recibir una formación adecuada. Si el personal encargado del tratamiento de datos personales no recibe una formación adecuada, no podrá garantizarse el respeto de la vida privada de los trabajadores en el lugar de trabajo.

CONSENTIMIENTO El grupo de trabajo del artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.

LOS TRABAJADORES SON PARTES INTERESADAS que se benefician de los derechos que confiere la Directiva sobre protección de datos. El más importante de estos derechos es el derecho de acceso, previsto en el artículo 12 de la Directiva

INTERACCIÓN ENTRE LA LEGISLACIÓN LABORAL Y LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS El grupo de trabajo desea señalar que la legislación sobre protección de datos no se aplica de forma independiente del Derecho del trabajo y las prácticas laborales y que éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debería contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

VIGILANCIA Y CONTROL Los requisitos de protección de datos se aplican a la vigilancia y control de los trabajadores tanto en términos de utilización de correo electrónico, acceso a Internet, cámaras de vídeo o datos de localización. Cualquier control deberá ser una respuesta proporcionada del empresario ante los riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores. Cualquier dato personal que se posea o se utilice a efectos de control deberá ser adecuado, pertinente y no excesivo respecto a los fines que justifiquen dicho control. Los controles deberán implicar las menores molestias posibles.

TRANSFERENCIA DE DATOS DE TRABAJADORES A TERCEROS PAÍSES El artículo 25 de la Directiva establece que las transferencias de datos personales a un tercer país, fuera de la Unión Europea, sólo podrán efectuarse si este país garantiza un nivel de protección adecuado. Cabe recordar que, cualquiera que sea la base de la transferencia en el marco de los artículos 25 y 26, el tratamiento que se efectúe en la transferencia deberá satisfacer siempre lo dispuesto

en los artículos 6 a 8 y en las demás disposiciones de la Directiva.

6 Todos los interesados tienen derecho a obtener del responsable del tratamiento (en este caso, el empresario):

a) sin coacción, a intervalos regulares y sin retrasos o gastos excesivos:

Confirmación sobre si los datos que afectan al trabajador están siendo tratados o no, así como información relativa como mínimo a la finalidad del tratamiento, las categorías de datos a que se refiere y el destinatario o categorías de destinatarios a los que se comunican los datos.

Comunicación de forma inteligible de los datos sometidos a tratamiento y de cualquier información disponible sobre el origen de los datos.

Conocimiento de la lógica de cualquier tratamiento automático de datos que le afecten, como mínimo en caso de decisiones automatizadas.

b) En su caso, la rectificación, supresión o bloqueo de datos cuyo tratamiento no sea conforme con lo dispuesto en la legislación sobre protección de datos, en particular porque se trate de datos incompletos o inexactos.

c) La notificación a terceros a los que se han comunicado los datos de cualquier rectificación, supresión o bloqueo efectuado de conformidad con la obligación anterior, a menos que resulte imposible o implique un esfuerzo desproporcionado.

El Grupo de trabajo opina que es preferible contar con una protección adecuada en el país de destino que recurrir a las excepciones que se enumeran en el artículo 26, por ejemplo el consentimiento del trabajador. Si se recurre al consentimiento, éste deberá expresarse de forma libre e inequívoca. Los empresarios actuarían de forma poco prudente si recurrieran únicamente al consentimiento, fuera de los casos en los que la retirada posterior del consentimiento no causa problemas.

ORIENTACIONES COMPLEMENTARIAS El grupo de trabajo está considerando la posibilidad de facilitar orientaciones complementarias sobre las cuestiones en las que la aplicación de los principios generales de protección de datos plantea problemas específicos en relación con el contexto laboral, como la vigilancia y el control en el lugar de trabajo, los datos de evaluación de los trabajadores, etc.

Dictamen 9/2001 sobre la comunicación de la Comisión titulada

GRUPO DEL ARTÍCULO 29 SOBRE LA PROTECCIÓN DE DATOS PERSONALES

5074/O 1/ES/final

WP 51

Dictamen 9/2001

sobre la comunicación de la Comisión titulada

«Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos » adoptado el 5 de noviembre de 2001

El Grupo, creado por el articulo 29 de la Directiva 95/46/CE, es un órgano comunitario independiente y de carácter consultivo sobre la protección de los datos y la intimidad. Sus misiones se definen en el articulo 30 de la Directiva 95/46/CE yen el articulo 14 de la Directiva 97/66/CE. La secretaria esta a cargo de:

la Comisión Europea, Dirección General de Mercado Interior, Unidad Libre circulación de la información y protección de datos. B-1049 Bruselas- Bélgica- Despacho :C100-6/136

Dirección en Internet: www.europa.eu.int/comm/internal_market/en/dataprot/index/htm

El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales,

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos los artículos 29 y 30 de la Directiva arriba mencionada, Visto su Reglamento interno, Ha adoptado el presente Dictamen:

1. OBSERVACIONES GENERALES

En enero de 2001, la Comisión Europea dirigió al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones una comunicación sobre la creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.

De manera general, el Grupo de trabajo recibe favorablemente este texto, que tiene tendencia a integrar de manera equilibrada los distintos intereses existentes, concretamente la lucha contra la delincuencia informática (que, además, puede contribuir a mejorar la protección de los datos personales) y el respeto de los derechos y libertades fundamentales de los individuos, especialmente sus derechos a la intimidad y a la protección de sus datos. Las medidas adoptadas para responder a los intereses legítimos de la lucha contra la delincuencia informática deben ajustarse a los imperativos derivados de la protección de los derechos y libertades fundamentales'. Concretamente, toda limitación de dichos derechos y libertades debe estar debidamente justificada y ser necesaria y proporcional con respecto al objetivo perseguido. La mayor concienciación del fenómeno de la delincuencia informática no debe ser la excusa para aplicar técnicas de estrecha vigilancia de los ciudadanos sin que se hayan considerado en profundidad otras alternativas para luchar contra ese tipo de delitos.

El Grupo de trabajo constata con satisfacción que la Comunicación de la Comisión contempla la creación de un foro en el que participarán los expertos que nombre el Grupo junto con representantes de las autoridades responsables de la protección de los datos. Es importante que dicho foro pueda comenzar sus actividades tan pronto como sea posible para que toda iniciativa vinculada con la lucha contra los delitos informáticos pueda ser

1 Garantizados concretamente por las Directivas 95/46/CE y 97/66/CE, la Carta de los Derechos Fundamentales de la Unión Europea (en particular, por sus artículos 7 y 8), el Convenio Europeo de Derechos Humanos (en particular, por su artículo 8), el Convenio del Consejo de Europa n° 108 de 1981 sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, la Recomendación del Consejo de Europa R(87) 15 destinada a reglamentar la utilización de los datos de carácter personal por el sector de la policía, la Recomendación del Consejo de Europa R(95) 4 sobre la protección de los datos de carácter personal en el sector de los servicios de telecomunicaciones y, concretamente, con respecto a los servicios telefónicos.

objeto de un debate abierto, transparente y que aborde el conjunto de los temas que se plantean, y que todas las partes interesadas puedan formular sus observaciones antes de que se apliquen las medidas mencionadas en la Comunicación de la Comisión.

2. SEGURIDAD DE LOS DATOS PERSONALES

No obstante, el Grupo considera que, aunque en la Comunicación se hace referencia a las medidas preventivas, la Comisión podría haber insistido más sobre la importancia de las medidas de prevención eficaces y, concretamente, sobre las medidas de seguridad en lugar de centrarse prioritariamente en las medidas represivas Una mejora general del nivel de seguridad contribuirá a reducir el riesgo de que se atente contra la seguridad de las redes y los datos. A este respecto, el Grupo desea recordar las obligaciones derivadas de las directivas relativas a la protección de los datos.

Por una parte, en el artículo 4 de la Directiva 97/66/CE, se establece que "el proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado para el riesgo existente".

En el mismo artículo se establece que, en caso de que exista un riesgo concreto de violación de la seguridad de la red, el proveedor de un servicio público de telecomunicación debe informar a los abonados sobre dicho riesgo y sobre las posibles soluciones, incluidos los costes necesarios.

Por otra parte, en el artículo 17 de la Directiva 95/46/CE, se establece "la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, 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 conocimientos técnicos existentes 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".

Por último, el Grupo recuerda a este respecto que el artículo 24 de la Directiva arriba mencionada obliga expresamente a los Estados miembros a adoptar las medidas adecuadas para garantizar la plena aplicación de las disposiciones de dicha Directiva y a determinar, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

2 El Grupo de trabajo es consciente de la existencia de otra Comunicación de la Comisión que trata

específicamente sobre la cuestión de la seguridad titulada « Seguridad de las redes y de la información:

Propuesta para un enfoque político europeo (COM (2001) 298 de 6 de junio de 2001). El Grupo de trabajo se reserva la posibilidad de comentar este texto posteriormente

3. CONCEPTO DE DELINCUENCIA INFORMÁTICA

No existe un concepto unánimemente aceptado a nivel de la Unión Europea de las nociones comprendidas por la delincuencia informática. Puede tratarse tanto de nuevas formas de delincuencia (denegación de servicios...) como de formas tradicionales de delincuencia que se materializan utilizando las nuevas tecnologías. No obstante, el Grupo de trabajo desea recordar a la Comisión que la Comunicación utiliza una noción de delincuencia informática extremadamente amplia que engloba distintas infracciones únicamente porque, en algún momento, se ha recurrido a tecnologías de la información y la comunicación.

Sin embargo, la amplitud del concepto de delincuencia informática tiene una gran importancia. Dicho concepto servirá de base para las medidas procesales mencionadas en la Comunicación. Debería evitarse que determinados comportamientos en los que la investigación no informática no diera lugar a medidas procesales intrusivas pudieran ser objeto de dichas medidas únicamente por el empleo de las tecnologías de la información y la comunicación.

Por otro lado, el Grupo de trabajo destaca que la noción de delincuencia informática aparece recogida, por ejemplo, en el anexo del Convenio Europol o en el proyecto de decisión Eurojust para delimitar las competencias de estos organismos. Por tanto, en términos de coherencia y seguridad jurídica, procede asegurarse de que los distintos tratamientos en diferentes entidades gocen de garantías equivalentes y adecuadas Sería especialmente nocivo que los diferentes campos de competencias de estas distintas entidades pudieran permitir que los datos tratados en el contexto de la lucha contra la delincuencia informática contaran con un nivel de protección diferente.

4. CUESTIONES DE DERECHO POSITiVO

El acercamiento de las disposiciones de derecho positivo implicará la definición de infracciones comunes. A este respecto, el Grupo de trabajo desea hacer dos observaciones. Por una parte, en términos de contenido del derecho sustantivo, es necesario definir las infracciones vinculadas con la delincuencia informática (por ejemplo, el acceso ilegal o la interceptación ilegal ...) con respecto a las que podrían existir en aplicación de las legislaciones sobre la protección de la intimidad o de los datos de carácter personal (por ejemplo, el acceso ilícito a los datos de carácter personal y la violación del secreto de las comunicaciones) con objeto de evitar contradicciones y solapamientos perjudiciales en términos de seguridad jurídica. Por otra parte, los comportamientos susceptibles de ser castigados vinculados con la delincuencia informática deberán definirse necesariamente de manera precisa para así poder incriminarlos. Al definir los elementos que constituyen las infracciones, es necesario velar por una perfecta coherencia con las normas existentes en materia de protección de datos. Así, el consentimiento de una persona distinta de la persona afectada no es necesariamente un criterio válido para eliminar el carácter delictivo de un comportamiento que atente contra la seguridad de los datos personales.

Por otro lado, el Grupo de trabajo señala a la Comisión la necesidad de llevar a cabo una evaluación de los trabajos del Consejo de Europa que han culminado en el proyecto de

Lo cual legitimaría el incremento del tratamiento de datos personales por parte de dichos organismos.

Convenio sobre delincuencia en el ciberespacio. El Grupo de trabajo destaca que este texto ha recibido numerosas críticas, sobre todo sobre su falta de equilibrio . A este respecto, el Grupo de trabajo recuerda el contenido de su Dictamen 4/200 1.

Por otro lado, el Grupo de trabajo insiste en la necesidad de definir el derecho sustantivo aplicable a los comportamientos que puedan ser objeto de incriminación con un espíritu de coherencia con respecto al marco jurídico de la protección de datos.

5. CUESTIONES DE DERECHO PROCESAL

El Grupo de trabajo es especialmente sensible a las cuestiones de derecho procesal que van parejas con la recopilación de múltiples datos personales sobre los individuos sospechosos de haber cometido infracciones.

El Grupo del trabajo destaca en particular el hecho de que las medidas de derecho procesal mencionadas en la Comunicación de la Comisión podrían llegar a tener un ámbito de aplicación extremadamente amplio porque se pueden aplicar a todo tipo de delincuencia, y no sólo a la informática.

El Grupo de trabajo destaca la necesidad de definir las medidas procesales de manera que se respeten los derechos y libertades fundamentales de las personas afectadas y, en particular, de forma coherente con respecto al marco jurídico de la protección de los datos. Así, el hecho de que se pueda acceder públicamente a determinados datos personales, o de que la persona en poder de la cual se hallen éstos materialmente consienta su divulgación, no implica que dichos datos puedan utilizarse con toda libertad para luchar contra la delincuencia. Además, cuando las autoridades encargadas del cumplimiento de la ley estén autorizadas a consultar los datos relativos a las conexiones de una persona en poder de los proveedores de acceso a Internet, dichas autoridades sólo deberían poder tratar los datos de conexión relacionados con la investigación sobre un comportamiento específico (por ejemplo, se deberían poder tratar los datos de conexión relativos a una intrusión ilícita en la Intranet de una empresa, pero no los datos relativos a las costumbres de navegación del autor de la intrusión que no tengan relación con la infracción investigada). De la misma forma, el hecho de que los individuos dejen señales de su presencia en las redes y de que se conserven sus datos personales (a veces sin que la persona interesada lo sepa) no implica que todos estos datos puedan utilizarse automáticamente para una investigación concreta. De manera más general, el Grupo es consciente de que, a la hora de incautarse de datos informáticos, puede ser dificil determinar directamente cuáles son los datos pertinentes y los que no lo son, pero, en cualquier caso, es fundamental que sólo se conserven los primeros.

La adopción de cada medida procesal y de mecanismos de cooperación internacional debería ir acompañada de condiciones y cláusulas de salvaguardia.

A título de ejemplo, véase la posición común del Grupo de trabajo internacional sobre la protección de los datos en las telecomunicaciones relativa a los aspectos de protección de los datos del proyecto de Convenio del Consejo de Europa sobre delincuencia en el ciberespacio de 13 y 14 de septiembre de 2000: « Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating

Computer-related Crime», disponible en la siguiente dirección de Internet: http://www.datenschutz berlinde /doc/int/iwgdpt/cy-en.htm , así como el Informe del Parlamento Europeo de 17 de julio de 2001 sobre la Estrategia para la Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.

El Grupo de trabajo estima que deberían tenerse en cuenta los siguientes puntos:

- debe establecerse con antelación el fundamento jurídico que autoriza cada medida de manera no arbitraria, accesible y previsible en cuanto a sus efectos;

- la necesidad de cada medida en una sociedad democrática, lo que implica la justificación de la medida por una necesidad social imperiosa, la falta de medios alternativos menos intrusivos para comprobar los hechos y excluye toda medida de vigilancia general o exploratoria;

- las medidas sólo deberían poder aplicarse si existieran indicios que permitieran sospechar que alguien intenta proyectar, materializar o haber materializado determinados comportamientos delictivos específicos; se debería realizar una prueba de proporcionalidad en cada caso que comprendiera la naturaleza, las circunstancias y la gravedad de la infracción;

- toda medida debería ser limitada en el tiempo y en el espacio, ser suficientemente específica (persona determinada, categorías de datos que pueden incautarse, ordenador particular, datos específicos) y pertenecer a una investigación penal determinada;

- para cada uno de los casos, se deberían establecer una motivación de la aplicación de la medida procesal, así como una indicación sobre las razones por las que otros medios menos intrusivos no permitirían demostrar los hechos;

- para los casos en los que se obtengan datos que no sean pertinentes (datos relativos a terceros, datos no pertinentes para la infracción investigada, etc.) mediante las medidas procesales, deberían establecerse garantías específicas y, concretamente, medidas de borrado de tales datos;

- debería contemplarse la posibilidad de informar a la persona afectada sobre la aplicación de la medida procesal a partir del momento en que tal información no perjudique o deje de perjudicar a la investigación;

- debería aplicarse de manera efectiva la transparencia democrática de las medidas procesales, por ejemplo, mediante la elaboración de informes sobre política delictiva;

- la aplicación de la medida debe ser objeto de autorización por parte de una autoridad judicial o equivalente con competencias en la materia y sometida a un control independiente;

- las personas afectadas por las medidas deben disponer de un derecho de recurso judicial 5;

- deben adoptarse garantías específicas para las profesiones reguladas (abogados, médicos, etc.).

Véase el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea.

6 A este respecto, véase la jurisprudencia del Tribunal Europeo de Derechos Humanos, que exige que los locales que albergan documentos cubiertos por el secreto profesional gocen de una mayor protección y que toda inspección domiciliaria en la materia sea proporcional y concreta para evitar el acceso a documentos cubiertos por el secreto profesional ajenos a la investigación.

Por otro lado, el Grupo de trabajo recomienda consultar sus trabajos precedentes sobre determinadas cuestiones específicas, a saber, la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones y, en particular, sobre la necesidad de que el derecho nacional defina de forma rigurosa y respetando todas las disposiciones anteriormente mencionadas las condiciones de interceptación de las comunicaciones, la Recomendación 3/99 sobre la conservación de datos sobre tráfico y la Recomendación 3/97 sobre el anonimato en Internet

6. Códigos de conducta

La Comunicación de la Comisión hace referencia a códigos de conducta en varias ocasiones. El Grupo de trabajo desea señalar a la Comisión que toda limitación de los derechos fundamentales de los individuos debe basarse en un fundamento jurídico por razones de control democrático

Conclusiones

El Grupo de trabajo destaca el carácter equilibrado de la Comunicación de la Comisión.

El Grupo de trabajo recomienda la mayor vigilancia para que el conjunto de medidas concretas destinadas a luchar contra la delincuencia informática integre los imperativos de protección de los derechos y libertades fundamentales y, concretamente, los derechos a la protección de los datos y a la intimidad.

El Grupo de trabajo insiste en la necesidad de mantener un debate público y transparente que dé comienzo lo más rápidamente posible en el que intervengan todas las partes interesadas y, en particular, expertos en protección de datos.

El Grupo de trabajo sugiere a la Comisión que evalúe si es verdaderamente oportuno inspirarse en los trabajos que se han llevado a cabo en el Consejo de Europa y que han culminado en el proyecto de Convenio sobre delincuencia en el ciberespacio.

El Grupo de trabajo invita a la Comisión, los Estados miembros y el Parlamento Europeo a tener en cuenta el presente Dictamen.

El Grupo se reserva la posibilidad de formular sus observaciones sobre las iniciativas concretas que se tomen en el ámbito de la lucha contra la delincuencia informática.

Hecho en Bruselas, el 5 de noviembre de 2001

Por el Grupo

El Presidente

Stefano RODOTA

Véase asimismo la Resolución de los Comisarios Europeos para la protección de datos sobre el mismo tema emitida en Estocolmo en la primavera de 2000.

Véase el párrafo segundo del apartado 2 del artículo 2 de la Recomendación del Consejo de Europa n° R (95)4.

De conformidad con la interpretación del Tribunal Europeo de Derechos Humanos.

Decisión 1/2001 sobre la participación de representantes de las autoridades de control de la protección de datos de los países candidatos en las reuniones del Grupo de trabajo del artículo 29 sobre protección de datos

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

5080/01/ES/Final

WP 52

DECISIÓN 1/2001

sobre la participación de representantes de las autoridades de control de la protección de datos de los países candidatos en las reuniones del Grupo de trabajo del artículo 29 sobre protección de datos

Aprobado el 13 de diciembre de 2001

El Grupo de trabajo se creó en virtud del articulo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el articulo 30 de la Directiva 95/46/CE yen el articulo 14 de la Directiva 97/66/CE. La secretaria encargada es la siguiente:

Comisión Europea, DG Mercado Interior, Dirección de libre circulación de la información y protección de datos.

B-1049 Bruselas- Belgium - Despacho: C100-6/136
Teléfono: directo (32-2) 299.27.19. central: 299.11.11 .Telefax: (32-2)296.80.10.
Dirección Internet: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

DECISIÓN

sobre la participación de representantes de las autoridades de control de la protección de datos de los países candidatos en las reuniones del Grupo de trabajo del artículo 29 sobre protección de datos

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS

PERSONALES,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas fisicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos', y, en particular, su artículo 29 y la letra a) del apartado 1 y el apartado 3 de su artículo 30, Visto el reglamento interno del Grupo de trabajo y, en particular, el apartado 1 de su artículo 9, Considerando lo siguiente:

(1) La ampliación de la Unión Europea es uno de los proyectos más ambiciosos de su historia. La perspectiva de una Unión que se extienda a todo el continente es mucho más real desde el Tratado de Niza, que determina las modificaciones institucionales necesarias para permitir que la UE acoja a los países candidatos que estén preparados al final de 2002. El proceso de ampliación abarca actualmente a los siguientes trece países candidatos: Bulgaria, Chipre, la República Checa, Estonia, Hungría, Letonia, Lituania, Malta, Polonia, Rumanía, la República Eslovaca, Eslovenia y Turquía.

La estrategia comunitaria para la ampliación comprende, por una parte, las negociaciones de adhesión, basadas en el principio de que el acervo comunitario (acquis communautaire) — incluida la Directiva 95/46/CE - debe incorporarse con la adhesión; y por otra, una estrategia de preadhesión reforzada cuya finalidad es garantizar que los países candidatos adoptan y aplican en la mayor medida posible el acervo comunitario antes de su ingreso en la UE. Uno de los objetivos de la estrategia de preadhesión es familiarizar a los candidatos con las políticas y procedimientos de la Unión, mediante la posibilidad participar en programas comunitarios Este objetivo, confirmado por el Consejo Europeo de Luxemburgo de diciembre de 1997 fue mejor especificado por la Comisión más adelante en su Comunicación al Consejo sobre la participación de países candidatos en

1 DO L 281 de 23.11.1995, p. 31, disponible en:

http://europa.euint/comm/privacy

2 Adoptado por el Grupo de trabajo en su tercera reunión, celebrada el 11 de septiembre de 1996.

Comunicación de la Comisión al Consejo, de 15 de julio de 1997 'Agenda 2000: Fo, a stronger a,,d wide, Unjo,,', COM(97) 2000.

Consejo Europeo de Luxemburgo, 12 y 13 de diciembre de 1997, Conclusiones de la Presidencia, punto 20.

programas, agencias y comités comunitarios A pesar de que la Comisión reconoce en dicha Comunicación que los países que aún no son miembros de la Unión Europea no deben participar en ningún mecanismo de toma de decisiones, insiste, no obstante, en el interés para la Unión Europea de que los países candidatos se impliquen en los mecanismos que desarrollan el acervo comunitario, con el fin de garantizar una aplicación más eficaz en dichos países y familiarizarlos con los procedimientos comunitarios. El Grupo de trabajo comparte plenamente la postura de la Comisión.

(2) El Grupo de trabajo del artículo 29 es un órgano consultivo e independiente. Entre sus tareas se incluye el estudio de todas las cuestiones relacionadas con la aplicación de las medidas nacionales adoptadas en virtud de la Directiva 95/46/CE para contribuir a que dichas medidas se apliquen de modo uniforme. A este respecto, la oportunidad de que disponen los representantes de los países candidatos de asistir a las reuniones del Grupo de trabajo como observadores y así seguir sus deliberaciones podría ser uno de los medios más eficaces para alcanzar el objetivo mencionado.

(3) El Grupo de trabajo del artículo 29 está compuesto por representantes de la autoridad o autoridades de control, designados por cada Estado miembro, por un representante de una autoridad o autoridades establecidas para las instituciones y órganos comunitarios y por un representante de la Comisión. Por consiguiente, la participación de países candidatos en las reuniones del Grupo de trabajo debe limitarse a aquellos países donde exista una autoridad de control responsable del seguimiento de la aplicación de la normativa sobre protección de datos.

(4) Es conveniente que los representantes de las autoridades de control encargadas de la protección de datos en los países candidatos tengan la posibilidad de intervenir en las reuniones del Grupo de trabajo con comentarios o preguntas, aunque sin participar en las votaciones. Deben estar sujetos a las normas del reglamento interno del Grupo de trabajo, si son de aplicación, y, en particular, al artículo 11 del mismo.

(5) Deben adoptarse las disposiciones necesarias para garantizar que el Grupo de trabajo continúa realizando sus tareas de forma eficaz. Es preciso, sobre todo, que el Presidente conserve la facultad de determinar los puntos del orden del día de la reunión a la que podrán ser invitados los observadores de países candidatos.

(6) Los recursos financieros y humanos de las autoridades de control de los Estados miembros y de la Comisión destinados a compartir los gastos de asistencia y de organización de reuniones son limitados. La participación de representantes de países candidatos debe organizarse de forma que no afecte a dichos recursos y de modo que el Grupo de trabajo pueda continuar trabajando a su ritmo actual.

(7) La participación de representantes de países candidatos en las reuniones del Grupo de trabajo se entiende sin peijuicio de las negociaciones de adhesión y, en particular, del examen de la legislación de los países candidatos, efectuada por la Comisión.

Comunicación de la Comisión al Consejo, de 20 de diciembre de 1999, sobre la participación de países candidatos en programas, agencias y comités comunitarios, COM(99) 710.

HA ADOPTADO LA SIGUIENTE DECISIÓN:

Artículo 1

El Presidente del Grupo de trabajo podrá invitar a representantes de las autoridades de control de la protección de datos de los trece países candidatos a la adhesión a la Unión Europea a participar en las reuniones del Grupo de trabajo. Las disposiciones necesarias a tal efecto serán adoptadas por la Secretaría

Artículo 2

Los representantes de las autoridades de control de la protección de datos de los países candidatos asistirán a las reuniones del Grupo de trabajo en calidad de observadores. Podrán participar en los debates del Grupo de trabajo pero no estarán autorizados a participar en las votaciones.

Artículo 3

Cuando se apruebe el proyecto de orden del día, el Presidente del Grupo de trabajo indicará los puntos del mismo donde los representantes de las autoridades de control de la protección de datos de los países candidatos podrán estar presentes.

Hecho en Bruselas, 13 de diciembre de 2001

Por el Grupo de trabajo

El Presidente

Stefano RODOTA

Dictamen 10/2001 relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo aprobado el 14 de diciembre de 2001

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

0901/02/ES/Final

WP 53

Dictamen 10/2001

relativo a la necesidad de un enfoque equilibrado en la lucha contra el terrorismo aprobado el 14 de diciembre de 2001

El Grupo de Trabajo se creó en virtud del articulo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el articulo 30 de la Directiva 95/46/CE y en el articulo 14 de la Directiva 97/66/CE. La secretaria encargada es la siguiente:

Comisión Europea, DG Mercado Interior, Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de

Datos.

B-1049 Bruselas - Bélgica - Despacho: Ci 00-6/1 36
Dirección Internet: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm:
http://eu ropa eu nt/cornm/privac

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995', Vistos el artículo 29 y los apartados 1, letra a), y 3 del artículo 30 de dicha Directiva,

Visto su Reglamento interno y, en particular, sus artículos 12 y 14,

Ha adoptado el siguiente DICTAMEN:

Los trágicos ataques terroristas perpetrados contra los Estados Unidos han puesto de manifiesto la necesidad de que las sociedades democráticas inicien una lucha contra el terrorismo. Este objetivo constituye un elemento tanto necesario como valioso de las sociedades democráticas. En esta lucha deben respetarse determinadas principios que constituyen también el fundamento de nuestras sociedades democráticas.

En este especial contexto se están debatiendo en la actualidad distintas medidas a escala tanto de la Unión Europea

como de los Estados miembros. Algunas de estas medidas son innovadoras, mientras que otras no son realmente nuevas, sino que constituyen sencillamente una actualización de proyectos ya existentes que cobran un nuevo interés. Estas medidas cubren en muchos casos varios ámbitos y no sólo la lucha contra el terrorismo. Se puede observar cierta proliferación de la utilización de medios de identificación de las personas y, en términos generales, de medios de recopilación de datos personales a través de la utilización, por ejemplo, de la biometría. Se observa además un aumento de la penalización de determinados comportamientos relacionados con la sociedad de la información — ' - como intrusión en sistemas de información, así como la reproducción de obras protegidas por derechos de autor . Las definiciones de estas infracciones son a menudo bastante amplias, por lo que plantean la cuestión del respeto de los principios fundamentales de la seguridad jurídica y de la legalidad de las infracciones y de las sanciones Al mismo tiempo, se refuerzan las medidas procesales ya existentes que legitiman la intrusión de las autoridades públicas en la vida privada de las personas y se debaten o incluso se adoptan medidas nuevas, aunque discutibles. Se trata no sólo de las escuchas telefónicas, sino también de la conservación previa y generalizada de datos sobre telecomunicaciones por parte de los prestatarios y operadores de comunicaciones electrónicas, la adopción de medidas que permitan la vigilancia «en tiempo real» de los ciudadanos, el abandono del principio de doble tipicidad como condición necesaria para el intercambio de determinados datos personales sobre los delincuentes, el intercambio de datos personales para distintos fines tales como la

1 Oficial n° L 281 de 23.11.1995, p. 31, que puede consultarse en:

http://europa.eu.int/commlinternal_market/en/dataprot/index.htm.

2 Véanse en particular las conclusiones de la cumbre de Justicia e Interior de la UE de 20 de septiembre de 2001 y el "mapa de carreteras" de la Unión Europea tras los ataques en los Estados Unidos (13880/1) de 15 de noviembre de 2001.

En los Estados Unidos, la " Recording Industry Association of America (RIAA)" intentó conseguir, con motivo de los debates en tomo al "Patriot Act", la adopción de una enmienda que hubiese autorizado legalmente a este sector para introducirse en sistemas de información a fin de identificar a los infractores de la legislación sobre derechos de autor.

Véase el Convenio del Consejo de Europa sobre la delincuencia en el ciberespacio, firmado en Budapest el 23 de noviembre de 2001.

Lucha contra la delincuencia, la inmigración y el contraespionaje exterior y la comunicación prematura de datos personales a terceros países. Tal comunicación puede resultar especialmente arriesgada si los países receptores no ofrecen garantías suficientes en materia de protección de datos.

Todas estas medidas tienen un incidencia directa o indirecta en la protección de los datos personales. El Grupo de Trabajo ha presentado varios dictámenes sobre temas afines , siendo al mismo tiempo plenamente consciente de la gravedad del problema del terrorismo, un fenómeno que Europa conoce lamentablemente desde hace bastante tiempo.

En este contexto, el Grupo de Trabajo recuerda el compromiso de las sociedades democráticas de respetar los derechos y las libertades fundamentales de las personas. El derecho de las personas a la protección de los datos personales forma parte de esos derechos y libertades fundamentales Las Directivas comunitarias sobre la protección de los datos personales (Directivas 95/46/CE y 97/66/CE) forman parte integrante de dicho compromiso Estas Directivas tienen como objetivo garantizar el respeto de los derechos y las libertades fundamentales y, en particular, el derecho a la vida privada en el tratamiento de los datos personales, así como contribuir al respeto de los derechos protegidos por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y, en particular, su artículo 8. Todas estas disposiciones establecen excepciones en la lucha contra la delincuencia, siempre que se cumplan determinadas condiciones.

El Grupo de Trabajo subraya concretamente la necesidad de tener en cuenta la incidencia a largo plazo de políticas que se están aplicando rápidamente con carácter urgente o que se están proyectando en la actualidad. Esta reflexión a largo plazo es necesaria, máxime teniendo en cuenta que el terrorismo no es un fenómeno nuevo y que no se puede calificar de fenómeno temporal. El Grupo de Trabajo subraya también la obligación de respetar el principio de proporcionalidad en relación con toda medida de restricción del derecho fundamental del respeto a la vida privada

Véanse en particular el documento de trabajo titulado 'Tratamiento de los datos personales en Internet" de 23 de febrero de 1999, las Recomendaciones 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones y 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, el documento de trabajo titulado 'Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea, de 21 de noviembre de 2000, el Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones y el Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2000 — COM(2000)385, el Dictamen 4/2001 acerca del proyecto de Convenio del Consejo de Europa sobre el ciberdelito y el Dictamen 9/200 1 sobre la Comunicación de la Comisión titulada 'creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" Todos estos documentos pueden consultarse en:

http://europa.eu.int/conmilinternal_market/en/dataprot/index.htm.

6 Véase en particular el el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y la jurisprudencia del Tribunal Europeo de Derechos Humanos en los recientes asuntos Aman de 16 de febrero de 2000 y Rotaru de 4 de mayo de 2000.

Véanse los considerandos 1, 2, 10 y 11 de la Directiva 95/46/CE y el segundo considerando de la Directiva 97/66/CE.

Establecido en el artículo 8 del Convenio Europeo sobre Derechos Humanos y la jurisprudencia correspondiente, lo que supone, entre otras cosas, la obligación de demostrar que toda medida adoptada responde a una « exigencia social imperativa ». Las medidas simplemente «útiles » o «convenientes» no pueden restringir los derechos y las libertades fundamentales. El Grupo de Trabajo subraya por lo tanto la necesidad de entablar un amplio debate sobre las medidas destinadas a luchar contra el terrorismo, analizando todas sus consecuencias en materia de derechos y libertades fundamentales de las personas, rechazando la confusión entre la lucha contra el terrorismo real y la lucha contra la delincuencia en general y limitando asimismo las medidas procesales que interfieren en la vida privada a las estrictamente necesarias.

El Grupo de Trabajo recuerda además que las disposiciones legislativas que limitan el derecho de las personas al respeto de su vida privada han de ser accesibles y previsibles en cuanto a sus consecuencias para las personas afectadas. A tal efecto la legislación debe ser suficientemente clara en su definición de las circunstancias, el ámbito y las modalidades del ejercicio de las medidas de interferencia. Las disposiciones deben ser claras e indicar de forma pormenorizada en qué circunstancias las autoridades públicas están autorizadas para adoptar medidas que limitan los derechos fundamentales. Concretamente deben especificar dónde pueden aplicarse tales medidas, excluir toda vigilancia general o preliminar y ofrecer protección contra los ataques arbitrarios de las autoridades públicas 8

Por último, el Grupo de Trabajo se preocupa de que la protección de los datos personales se presente cada vez más como un obstáculo a la lucha eficaz contra el terrorismo y desea recordar, por un lado, que los textos sobre protección de datos (que incluyen las Directivas 95/46/CE y 97/66/CEE, así como el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea) tienen como objetivo proteger los derechos fundamentales del ciudadano y, por otro, que dichos textos contemplan las excepciones necesarias para la lucha contra la delincuencia dentro de los límites autorizados por el Convenio Europeo sobre Derechos Humanos.

Las medidas contra el terrorismo no deben reducir los niveles de protección de los derechos fundamentales que caracterizan a las sociedades democráticas. Uno de los elementos clave de la lucha contra el terrorismo es la necesidad de preservar los valores fundamentales que constituyen el fundamento de nuestras sociedades democráticas y los valores que precisamente intentan destruir los que abogan por el recurso a la violencia.

Hecho en Bruselas, el 14 de diciembre de 2001

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA

Véase en particular la jurisprudencia del Tribunal Europeo de Derechos Humanos en los asuntos Chappell (30 de marzo de 1989, n° 152, punto 56), Malone (2 de agosto de 1984, puntos 67 y 68), Sunday Times (26 de abril de 1979, punto 49), Valenzuela Contreras (30 de julio de 1998, punto 46) y Lambert (24 de agosto de 1998).